CONTRIBUȚII PRIVIND UTILIZAREA STEGANOGRAFIEI ÎN PROTECȚIA ŞI TRANSMITEREA DATELOR

Teză destinată obţinerii
titlului ştiinţific de doctor inginer
la
Universitatea "Politehnica" din Timişoara
în domeniul ŞTIINŢA CALCULATOARELOR
de către

Ing. Daniela Natalia Stănescu

Conducător ştiinţific: prof.univ.dr.ing. Mircea STRATULAT

Referenţi ştiinţifici: prof.dr.ing. Daniela POPESCU
prof.dr. Alexandru CICORTAŞ
prof.dr.ing. Ştefan HOLBAN

Ziua susţinerii tezei: 05.05.2010

Seriile Teze de doctorat ale UPT sunt:

1. Automatică
2. Chimie
3. Energetică
4. Ingineria Chimică
5. Inginerie Civilă
6. Inginerie Electrică
7. Inginerie Electronică şi Telecomunicaţii
8. Inginerie Industrială
9. Inginerie Mecanică
10. Ştiinţa Calculatoarelor
11. Ştiinţa şi Ingineria Materialelor
12. Ingineria sistemelor

Universitatea „Politehnica” din Timişoara a iniţiat seriile de mai sus în scopul diseminării expertizei, cunoştinţelor şi rezultatelor cercetărilor întreprinse în cadrul şcolii doctorale a universităţii. Seriile conţin, potrivit H.B.Ex.S Nr. 14 / 14.07.2006, tezele de doctorat susţinute în universitate începând cu 1 octombrie 2006.

România, 300159 Timişoara, Bd. Republicii 9,
tel. 0256 403823, fax. 0256 403221
e-mail: editura@edipol.upt.ro

Cuvânt înainte

Teza de doctorat a fost elaborată pe parcursul activităţii mele în cadrul Departamentului de Calculatoare, din cadrul Universităţii „Politehnica” din Timişoara.

Cele mai alese gânduri de recunoştinţă şi mulţumire se îndreaptă spre conducătorul ştiinţific, domnul profesor dr. ing. Mircea Stratulat, care m-a sprijinit constant în activitatea mea didactică, doctorală şi ştiinţifică, şi căruia îi datorez în bună măsură formarea mea de cercetător şi pedagog. De asemenea, doresc să evidenţiez efortul enorm depus şi răbdarea de care acesta a dat dovadă în îndrumarea competentă şi permanentă pe parcursul elaborării acestei lucrări.

Mulţumesc domnului profesor dr. ing. Ştefan Holban care cu generozitate, răbdare şi profesionalism, a îmbogăţit permanent conţinutul ideatic şi ştiinţific al cercetărilor mele, dând consistenţă tezei, precum şi pentru sprijinul personal şi încrederea pe care mi le-a acordat în întreaga mea carieră universitară.

De asemenea, doresc să mulţumesc doamnei profesor dr. ing. Daniela Popescu (Universitatea Oradea) şi domnului profesor dr. Alexandru Cicortaş (Universitatea de Vest Timişoara), care au răspuns solicitării de a face parte din comisia de analiză a tezei pentru răbdarea de a evalua prezenta teză şi pentru aprecierile exprimate asupra acesteia.

Aduc de asemenea mulţumiri tuturor colegilor din laboratorul B425 şi B513 pentru sprijinul permanent acordat şi pentru întreaga colaborare de peste 12 ani, concretizată printr-o listă de realizări comune, atât pe plan didactic, cât şi ştiinţific, multe dintre ele fiind puncte de referinţă pentru teza elaborată.

Mulţumesc întregului colectiv al Departamentului de Calculatoare, din cadrul Universităţii „Politehnica” din Timişoara, care a contribuit la formarea mea profesională şi colegilor care mi-au oferit sprijinul şi prietenia lor.

Doresc de asemenea să adresez mulţumirile cuvenite tuturor celor care, direct sau indirect, prin sugestiile oferite au contribuit la şlefuirea acestui demers ştiinţific şi m-au susţinut în finalizarea lui.

Nu în ultimul rând, doresc să mulţumesc întregii familii, în special soţului meu Manuel şi fiului Raul pentru înţelegerea, răbdarea şi sprijinul acordat în tot intervalul de timp alocat elaborării tezei. De asemenea mulţumesc părinţilor şi socrilor pentru încurajările şi ajutorul acordat în toată această perioadă.

Timişoara, mai 2010 Daniela Natalia Stănescu

Stănescu, Daniela Natalia

Contribuţii privind utilizarea steganografiei în protecţia şi transmiterea datelor

Teze de doctorat ale UPT, Seria 10, Nr. 28, Editura Politehnica, 2010, 222 pagini, 71 figuri, 15 tabele.

ISSN: 1842-7707

ISBN: 978-606-554-088-0

Cuvinte cheie: steganografie, model steganografic, algoritm steganografic, domeniul spaţial, domeniul vectorial,microprocesor

Rezumat,

Teza se încadrează în domeniul protecţiei şi transmiterii datelor cu ajutorul steganografiei prin ascunderea informaţiilor în mesaje care să nu trezească suspiciuni. Aspecte abordate: Conceperea unui model steganografic ce permite creşterea gradului de siguranţă a sistemelor steganografice. Dezvoltarea, conceperea şi verificarea unor algoritmi steganografici care să satisfacă modelul propus. Implementarea unor algoritmi steganografici pe două microprocesoare cu arhitecturi interne diferite în vederea testării capacităţii acestora de a prelucra astfel de date în scopul dezvoltării unor aplicaţii steganografice pentru telefonia mobilă.

CUPRINS

1 INTRODUCERE

1.1 *Preliminarii*

Dorinţa oamenilor de a păstra o informaţie confidenţială sau de a trimite mesaje secrete care să nu fie descoperite s-a manifestat încă din cele mai vechi timpuri. Pentru a putea realiza ceea ce-şi doresc oamenii au fost nevoiţi să inventeze cu abilitate diferite metode de ascundere în funcţie de necesităţile ce le aveau de îndeplinit la acea vreme. Prima condiţie ca un mesaj să poată fi ascuns în aşa fel încât să nu fie nici măcar bănuită existenţa lui era găsirea unui mediu prielnic care să pară cât mai inofensiv pentru un observator întâmplător sau chiar rău voitor. În general în acele timpuri erau transmise doar mesajele importante, cu un scop precis de la o persoana la alta, dar astăzi este cunoscut faptul că oamenii sunt inundaţi cu informaţii ce le pot fi necesare sau nu. Un astfel de exemplu ar putea fi reclamele publicitare ce pot fi transmise prin intermediul televiziunii, radioului, Internet-ului, telefoniei etc. Este important de remarcat faptul că informaţiile transmise în aceste moduri pot fi inofonsive sau nu, iar procesul de ascundere a acestora constituie o adevărată artă, numită steganografie.

Aşadar, steganografia este o artă veche de ascundere a unor mesaje secrete în mesaje care par inofensive la prima vedere. Pe de altă parte, steganografia reprezintă un tip de comunicare între două persoane care au cunoştinţă de existenţa mesajelor secrete şi de metoda aplicată în acest sens. Informaţiile secrete sunt astfel ascunse încât nu pot fi detectate deoarece nu este conştientizată existenţa lor de către o altă persoană.

Comunicarea secretă este întâlnită pretutindeni în ziua de azi şi este folosită de diferite persoane pentru numeroase motive, cum ar fi: protejarea afacerilor prin schimburi secrete de informaţii între companii, ascunderea datelor importante sub formă audio, video, imagini digitale faţă de persoane care nu ar trebui sa aibă acces la ele, protecţia intelectuală, semnătura digitală, etc.

Cuvântul *steganografie* provine din grecescul *steganos* (secret) şi *graphein* (reprezentare grafică - scriere) şi a avut un rol important în comunicarea secretă pe parcursul întregii istorii. De-a lungul timpului au fost folosite diferite tehnici de ascundere a informaţiilor precum: tatuarea unui mesaj secret pe capul unui sclav trimis ca mesager, scrierea pe tăbliţe de lemn acoperite cu ceară, folosirea cernelii invizibile creată din diferite substanţe, etc. [JOH01]. Odată cu trecerea timpului au fost generate noi metode de ascundere în funcţie de evoluţia dezvoltării tehnologiei.

În prezent steganografia modernă se bazează în mare parte pe comunicarea electronică facilitată de apariţia Internet-ului şi a telefoniei mobile. Astfel un mesaj text, imagine sau sunet poate fi încorporat într-un alt mesaj text, imagine sau sunet cu ajutorul unui algoritm implementat în aşa fel încât procesul de ascundere să nu fie bănuit sau detectat nici de ochiul uman dar nici de un program specializat în acest sens.

În procesul de ascundere se evidenţiază două părţi: încorporarea mesajului ce se doreşte a fi secret într-o informaţie oarecare şi extragerea acestuia din informaţia în care a fost ascuns. De asemenea este foarte important ca informaţia să fie astfel ascunsă, încât să nu fie detectată, pentru ca eventualii interceptori să nu realizeze existenţa acesteia. Scopul steganografiei este transmiterea unei informaţii secrete într-o manieră în care să se evite apariţia suspiciunilor din partea unor potenţiali atacatori.

Pentru comunicarea secretă a informaţiilor poate fi utilizată şi criptografia, în care mesajele sunt codificate astfel încât să poată fi citite doar de către cineva care deţine cheia de codare folosită în acest scop. Spre deosebire de criptografie, steganografia ascunde mesajele astfel încât existenţa lor nu este detectabilă.

Cele două domenii de securizare a informaţiilor nu se exclud, ci doar se complementează existând posibilitatea de a le utiliza simultan pentru a creşte siguranţa transmiterii informaţiei.

O problemă importantă întâlnită la ora actuală o constituie protejarea împotriva copierii în cazul înregistrărilor de imagini sau sunete. În acest sens se poate apela la o tehnică numită watermarking digital, ce asigură un mod de protejare a drepturilor unui proprietar asupra propriei creaţii. Un watermark electronic reprezintă un semn sau o imprimare asupra unui document şi este folosit cu scopul de a dovedi autentificarea şi pentru a minimiza şansele ca o persoană neautorizată să altereze respectivul document. În acest mod se poate demonstra dreptul de proprietate în cazul în care un anumit material este copiat sau modificat puţin.

Aşadar, watermarking-ul digital ascunde informaţie într-un anumit obiect de acoperire, şi aceasta îl face să devină o aplicaţie a steganografiei. Este o formă limitată, deoarece este încorporată o cantitate destul de mică de informaţie şi în principiu este adecvată doar pentru protejare şi demonstrare a proprietarului , nu şi pentru transmiterea informaţiei.

În prezent steganografia se bazează în bună parte pe noile evoluţii ale tehnologiei informaţiei, care prezintă pe lângă avantajele legate de puterea de calcul, mobilitatea şi simplitatea în comunicare şi o serie de efecte secundare în ceea ce priveşte furturile intelectuale, atacuri la informaţie, precum şi lipsa de confidenţialitate. Într-un raport înaintat Uniunii Europene [SCH01] se menţionează dorinţa de păstrare a confidenţialităţii comunicaţiilor personale şi având în vedere că în unele ţări europene, criptarea personală a datelor nu mai este permisă, impunându-se doar standardele existente se simte necesitatea identificării unor noi moduri de protejare a informaţiilor. O cale preconizată în acest sens o poate avea steganografia, care prezintă o alternativă în găsirea unor soluţii în ceea ce priveşte transmiterea şi protecţia datelor. Aceasta a condus în ultimii ani la necesitatea dezvoltării unor sisteme steganografice cât mai sigure.

Prima conferinţă în domeniul steganografiei a avut loc în 1996, iar în septembrie 2001 la o conferinţă pe teme de securitate a informaţiei susţinută la Londra s-a pus pentru prima dată problema unei securităţi globale pe Internet. Aşadar, steganografiei îi revine un rol şi o alternativă în domeniul protecţiei datelor.

Consider ca în acest domeniu atât de vast al steganografiei, pot să aduc o contribuţie proprie în vederea creşterii securizării datelor, prin găsirea unor soluţii mai eficiente sau alternative pentru ascunderea informaţiilor secrete.

1.2 *Oportunitatea şi motivarea lucrării*

Această lucrare îşi propune să dezvolte găsirea unor noi modalităţi de îmbunătăţire a modelelor steganografice specifice domeniului, cât şi dezvoltarea unor algoritmi steganografici cu posibilitatea de implementare pe microprocesoare folosite sau în curs de utilizare în telefonia mobilă. Oportunitatea acestor cercetări

este dată de găsirea unor soluţii mai eficiente sau alternative pentru asigurarea confidenţialităţii comunicaţiilor mobile.

Motivaţia unei astfel de cercetări a plecat de la dorinţa de mobilitate a transmiterii datelor în tehnologia calculatoarelor ce a fost propusă de către dr. George H. Heilmeier în octombrie 1992 în [HEI92]. Acesta preciza că "*Oamenii şi maşinile lor ar trebui să poată accesa informaţia şi comunicarea uşor cu ceilalţi într-un mod simplu şi sigur, într-un mediu sau o combinaţie de medii precum, media-voce, imagine sau video, oricând şi oriunde în timp real*".

În prezent în era mobilităţii aproape oricine poate utiliza un calculator mobil sau un telefon mobil pentru a comunica prin intermediul acestora simplu şi rapid. Din acest motiv nu este nici un secret că au loc cercetări în domeniul translatării aplicaţiilor în era mobilităţii. Lucrarea de faţă se situează în acest domeniu, aducând mobilitate steganografiei în această direcţie.

Se constată o tendinţă tot mai pronunţată de a se trece de la comunicarea prin intermediul unor echipamente fixe spre o evoluţie a utilizării unor echipamente mobile sau utilizarea Internet-ului. În [1] se prezintă evoluţia numărului de utilizatori de Internet (figura 1.1.) şi de telefoane mobile (figura 1.2).

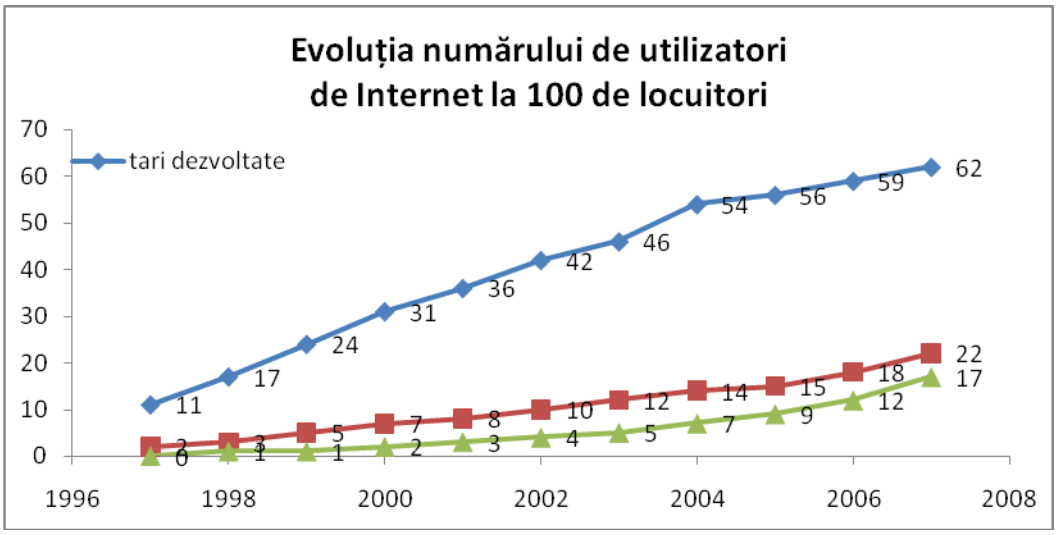


Figura 1.1. Evoluţia numărului de utilizatori de Internet la 100 de locuitori [1]

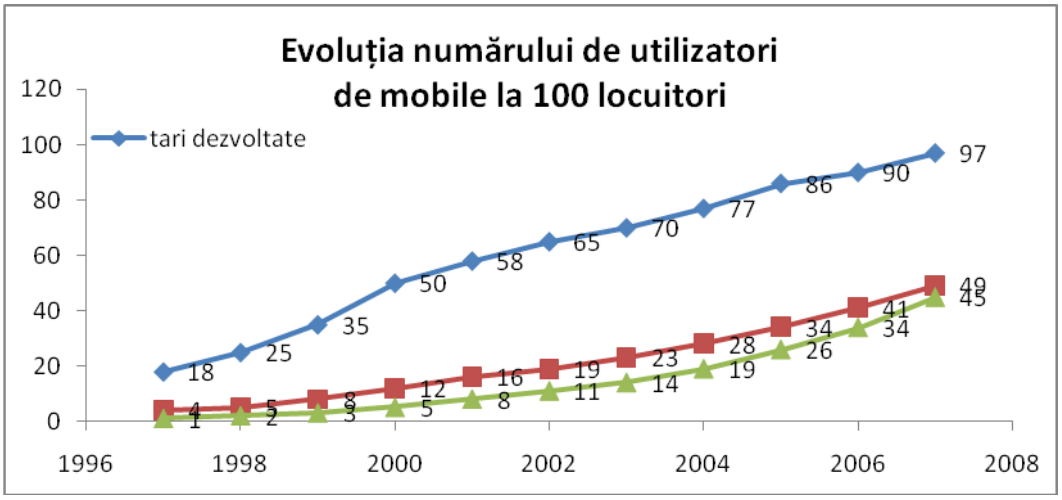


Figura 1.2. Evoluţia numărului de utilizatori de telefoane mobile la 100 de locuitori [1]

După cum se vede din cele prezentate evoluţia numărului de utilizatori de Internet a crescut în ultimii 10 ani de la 11 la 62 de utilizatori/100 de locuitori (figura 1.1). Pe de altă parte, statisticile din 2007 arată că 97% din populaţie deţine cel puţin un telefon/locuitor în ţările dezvoltate (figura 1.2).

Totodată pe baza aceloraşi statistici [1] se constată că numărul de telefoane mobile vândute anual depăşeşte de aproximativ 3 ori numărul de calculatoare vândute în aceeaşi perioadă (figura 1.3), în schimb numărul de programatori specializaţi pe dezvoltarea aplicaţiilor în telefonia mobilă este infim comparativ cu numărul de programatori de dezvoltare a aplicaţiilor pentru sistemele clasice de calcul (figura 1.4).

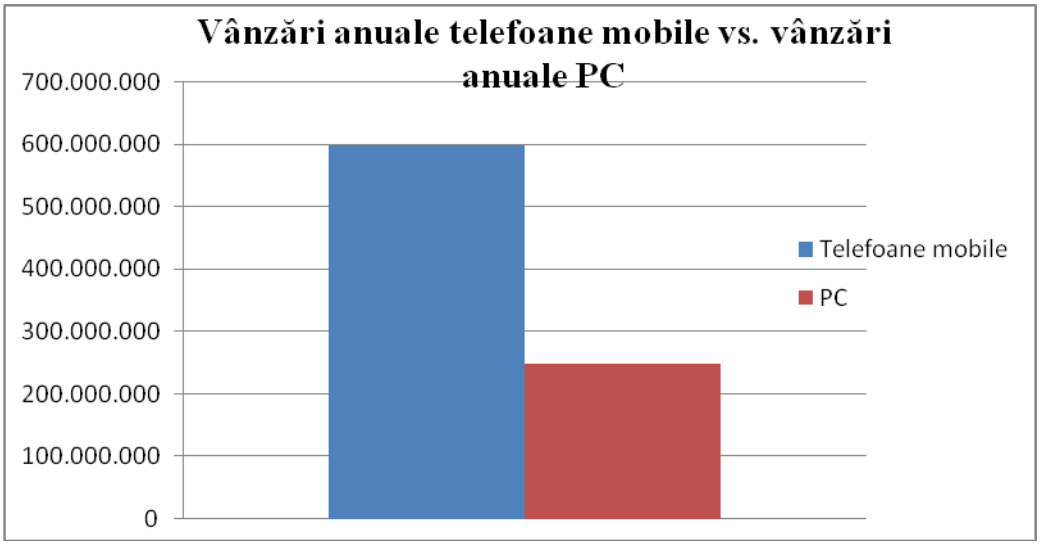


Figura 1.3. Vânzările anuale de telefonie mobilă în comparaţie cu vânzări de calculatoare personale [1]

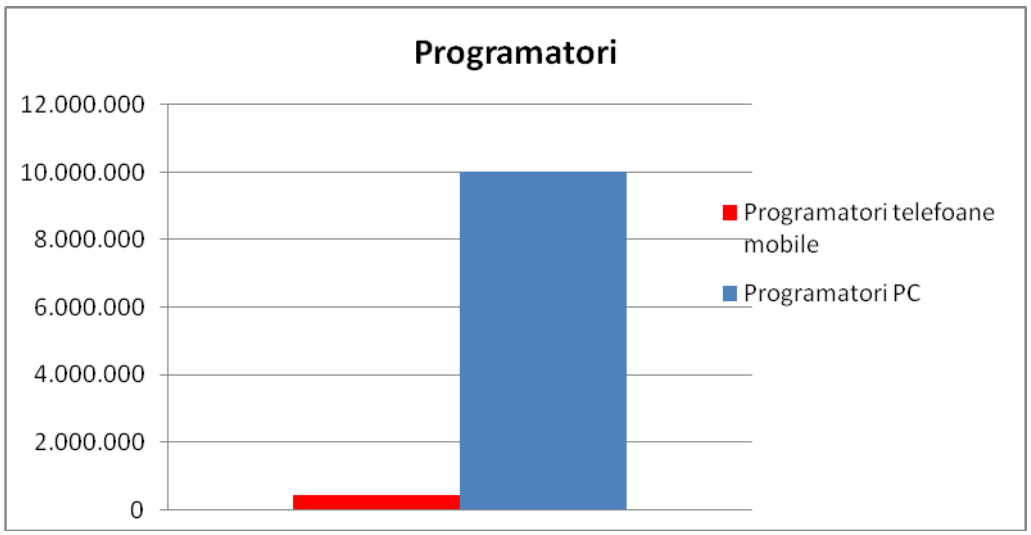


Figura 1.4. Numărul de programatori pentru calculatoare personale şi telefoane mobile [1]

În ultima perioadă pe lângă mobilitatea în comunicare s-a dorit şi o creştere a puterii de calcul, astfel că s-a impus ideea ca noua tehnologie să asigure o comunicare oricând şi oriunde dublată de o putere de calcul care să atingă caracteristicile unui calculator portabil.

De asemenea s-a constatat o tendinţă în ceea ce priveşte integrarea unui calculator personal într-un telefon mobil. Această dorinţă a dus la apariţia SmartPhone-urilor şi a iPhon-urilor. Vânzările de iPhone-uri în al doilea trimestru al anului 2009 [2] arată 20,73 milioane de unităţi vândute la nivel mondial faţă de 0,27 milioane de unităţi vândute la mijlocul anului 2007 constatându-se o creştere de aproximativ 78,41 ori, aşa cum arată în figura (figura 1.5).

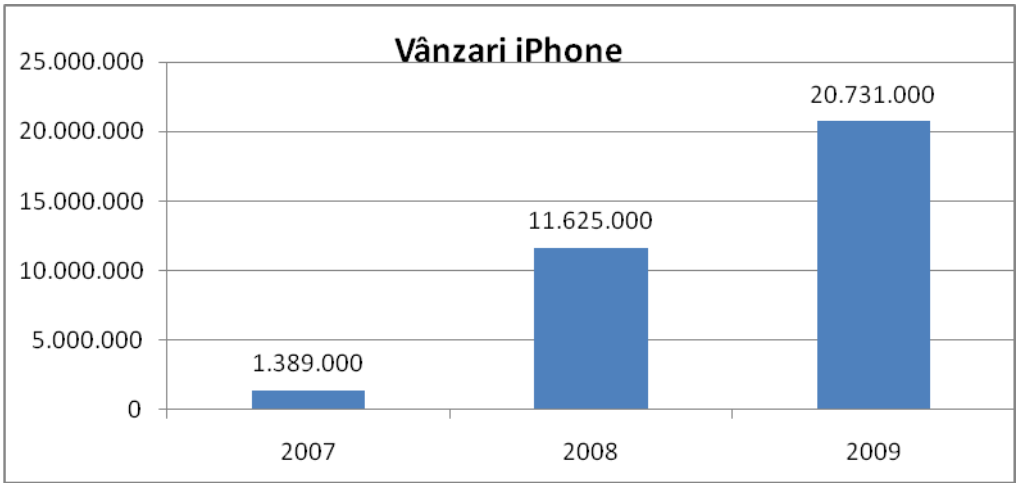


Figura 1.5. Vânzări iPhone [2]

Elementele care au favorizat dezvoltarea dispozitivelor mobile se caracterizează în primul rând prin dezvoltarea tehnologiilor pentru comunicaţii cu un grad mare de flexibilitate personală, miniaturizarea, dezvoltarea unui număr tot mai mare de funcţionalităţi şi interfeţe, uşurinţa de utilizare şi nu în ultimul rând creşterea puterii de calcul prin trecerea de la calculatoare personale statice sau portabile spre SmartPhon-uri, respectiv iPhon-uri. Pe de altă parte se impune crearea unor medii de dezvoltare pentru dispozitivele mobile care să permită facilităţi suplimentare privind funcţionalitatea şi comunicarea.

O caracteristică importantă a sistemelor mobile actuale este mobilitatea şi puterea de calcul din ce în ce mai evoluată a acestora, ca urmare a folosirii unor procesoare tot mai performante, cu o capacitate de memorie din ce în ce mai mare şi cu posibilitatea de conexiune tot mai rapidă atât în reţeaua mobilă, cât şi pe Internet. Toate acestea implică utilizarea telefoanelor mobile de către un număr foarte mare de persoane. Modelele noi apărute prezintă posibilităţi de programare din ce în ce mai complexe, ce permit integrarea unor funcţionalităţi multiple, cum ar fi: încorporarea camerelor de luat vederi, camere video, sisteme de afişare cu o rezoluţie din ce în ce mai mare, utilizarea ecranelor tactile, încorporarea de senzori şi a unor sisteme de localizare GPS.

Pe lângă aceste facilităţi, dispozitivele mobile prezintă şi unele constrângeri specifice acestor sisteme, cum ar fi: un număr mare de modele existente pe piaţă, un număr limitat de periferice de intrare-ieşire (tastatură, ecran tactil), dimensiunea mică a ecranului, energia stocată limitată, existenţa unui număr redus de aplicaţii. Este de aşteptat ca pe măsură ce performanţele telefoanelor mobile evoluează, să sporească şi numărul de aplicaţii specifice acestora. Astfel, se poate imagina încorporarea telefonului mobil într-un sistem de tip "casă inteligentă" sau în sisteme de monitorizare şi control ale traficului pe baza datelor obţinute direct din mediu [3]. Totodată se poate încadra ca o potenţială aplicaţie şi asigurarea confidenţialităţii comunicaţiilor prin utilizarea steganografiei. În prezent firmele producătoare de microprocesoare utilizate în telefonia mobilă şi-au propus, ca urmare a cererilor tot mai mari din partea beneficiarilor să includă şi funcţii de protecţie a transmiterii informaţiilor prin utilizarea steganografiei.

1.3 *Obiectivele lucrării*

În cadrul tezei sunt urmărite câteva problematici importante legate de dezvoltarea unor sisteme steganografice implementate pe microprocesoare utilizate în telefonia mobilă. În acest sens obiectivele urmărite în lucrarea de faţă sunt:

- Găsirea mediului steganografic adecvat problematicii propuse . În urma studierii unei game largi de posibile medii steganografice ce pot fi utilizate în ascunderea informaţiilor s-a constatat că imaginile digitale constituie mediul steganografic cel mai potrivit datorită faptului că satisfac toate cerinţele specifice sistemelor steganografice.
- Analiza comparativă a principalelor domenii de reprezentare a imaginilor digitale în privinţa găsirii acelor domenii adecvate pentru dezvoltarea unor algoritmi steganografici.
- Studiu privind stadiul actual al modelelor steganografice prezentate în literatura de specialitate şi determinarea deficienţelor referitoare la posibilitatea de implementare reală a acestora în practică.
- Dezvoltarea, demonstrarea teoretică şi verificarea practică a unor noi modele steganografice care să conducă la îmbunătăţirea procesului

steganografic atât din punctul de vedere al calităţii obiectului steganografic transmis, cât şi al mesajului recuperat.
- Studierea particularităţilor arhitecturilor microprocesoarelor tipice utilizate în telefonia mobilă şi exploatarea acestora în vederea dezvoltării de algoritmi steganografici specifici unor astfel de aplicaţii, care trebuie să îmbine aspectele legate de timpi de execuţie, cantitate de informaţie posibil ascunsă şi de extragere a mesajului secret în timp real.
- Adaptarea şi dezvoltarea unor algoritmi steganografici ce prezintă posibilităţi de a fi implementaţi pe microprocesoarele utilizate în telefonia mobilă, care să satisfacă caracteristicile legate de obţinerea unei imagini steganografice de o calitate indiscutabilă astfel încât să nu trezească nici un fel de suspiciune unui eventual atacator.

1.4 *Prezentarea conţinutului lucrării*

Conţinutul lucrării este dezvoltat pe parcursul a zece capitole.

În primul capitol este prezentată o scurtă descriere a tematicii legate de steganografie, oportunitatea cercetării în domeniul menţionat, motivarea direcţionării cercetării spre aplicaţii specifice microprocesoarelor utilizate în telefonia mobilă, descrierea principalelor obiective ale lucrării, respectiv modul de structurare a acesteia în funcţie de obiectivele propuse.

În capitolul 2 este prezentată o analiză comparativă a principalelor medii de ascundere, raportată la necesităţile sistemelor steganografice legate de vizibilitate, detecţie, robusteţe şi capacitate de încorporare. Concluzia ce se desprinde pe baza analizei menţionate constă în faptul că imaginile digitale pot satisface în totalitate toate aceste cerinţe. Ca atare în continuarea cercetării prezente am folosit imaginile digitale ca suport în dezvoltarea algoritmilor steganografici.

În continuare am scos în evidenţă în capitolul 3 câteva caracteristici esenţiale ale imaginilor digitale plecând de la captarea acestora din imagini reale până la reprezentarea lor în sistemele de calcul. Sunt de asemenea descrise principalele tipuri de imagini folosite în lucrare atât ca şi obiecte de acoperire, cât şi ca mesaje secrete.

În capitolul 4 sunt descrise cele trei domenii de reprezentare ale imaginilor digitale: spaţial, frecvenţă, respectiv vectorial. Din punct de vedere al percepţiei ochiului uman, respectiv al selecţiei culorilor, domeniul spaţial poate fi regăsit în diferite reprezentări, cum ar fi: RGB, YUV etc. Pentru fiecare domeniu se prezintă suportul matematic ce stă la baza transpunerii imaginii în unul dintre cele trei domenii.

În capitolul 5 după o trecere în revistă a evoluţiei stadiului actual a aplicaţiilor steganografice bazate pe implementare hardware, respectiv arii programabile, circuite integrate, microprocesoare sunt prezentate câteva aplicaţii ce utilizează facilităţile oferite de serviciile telefoniei mobile şi a reţelelor fără fir. Pe baza constatărilor rezultate în urma aplicaţiilor descrise se desprinde ca o soluţie posibilă, implementarea directă sau chiar cablarea algoritmilor în microprocesoarele ce urmează a fi utilizate în telefonia mobilă. În continuare se face analiza principalelor caracteristici arhitecturale pentru un microprocesor ARM ce se bazează

pe o arhitectură de tip RISC a cărui punct forte îl reprezintă banda de asamblare. De asemenea se analizează avantajele microprocesorului ISAAC ce se bazează pe o arhitectură constituită din mai multe nuclee. Pe baza acestor caracteristici au fost verificaţi practic mai mulţi algoritmi scoţându-se în evidenţă performanţele lor de timp.

În capitolul 6 după o scurtă prezentare a modelului clasic, respectiv a modelului de bază steganografic s-a făcut o analiză din punctul de vedere al siguranţei sistemelor steganografice a celor mai frecvent citate modele în literatura de specialitate, scoţând în evidenţă aspecte legate de dificultatea utilizării acestora în practică sau punerea în evidenţă a unor aspecte ce nu fost luate în considerare. În vederea îmbunătăţirii siguranţei unui sistem steganografic, în urma acestor analize am propus un model steganografic în două variante de lucru: prima o constituie modelul denumit MPOA şi presupune procesarea obiectelor de acoperire înaintea generării obiectului steganografic, iar a doua variantă o constituie modelul denumit MPOAM, ce presupune în plus pe lângă procesarea obiectului de acoperire şi procesarea mesajului secret. Pentru validarea primului model s-a demonstrat pe baza distribuţiei de probabilitate că o procesare a obiectelor steganografice poate conduce la îmbunătăţirea acestora. Rezultatele practice obţinute în urma unor seturi de experimente conduc la aceeaşi concluzie, în sensul că procesarea asupra obiectelor steganografice şi asupra mesajelor secrete înainte de a fi încorporate permite o îmbunătăţire semnificativă atât a claritătii obiectului steganografic, cât şi a mesajului secret recuperat rezultând astfel un sistem steganografic cu un grad mai mare de siguranţă.

Capitolul 7 descrie un set de algoritmi dezvoltaţi în domeniul spaţial. Pentru analiza performanţelor privind comportarea în timp au fost dezvoltate trei variante de algoritmi bazate pe ascunderea informaţiilor în biţii cei mai puţini semnificativi în spaţiul RGB, respectiv un algoritm ce se bazează pe prelucrarea obiectului de acoperire cu ajutorul transformatei YUV. Cei patru algoritmi au fost dezvoltaţi pentru a fi implementaţi pe un calculator personal, respectiv pe două microprocesoare, dintre care unul este bazat pe arhitecturi de tip bandă de asamblare, iar celălalt pe o arhitectură constituită din mai multe nuclee. În urma testelor efectuate pe un set de imagini de dimensiuni diferite sunt prezentate rezultatele timpului de execuţie. Pentru compararea cantităţii de informaţie ce poate fi ascunsă, respectiv a calităţii obiectului steganografic a fost implementat un algoritm bazat pe complexitatea planurilor de biţi care din punct de vedere al calităţii asigură performanţe foarte bune, dar din punctul de vedere al cantităţii informaţiei ascunse este inferior în comparaţie cu algoritmii bazaţi pe ascunderea în cei mai puţini semnificativi biţi.

În capitolul 8 s-a dezvoltat un algoritm în domeniul frecvenţei bazat pe transformata cosinus discretă prin care mesajul secret este încorporat într-o imagine video în format MPEG-2. Scopul acestui algoritm a constat în verificarea robusteţii obiectului steganografic, dar care conduce la ascunderea unei cantităţi relativ mici de informaţii. Astfel de algoritmi realizaţi în domeniul frecvenţei ar putea face obiectul îmbunătăţirii robusteţii sistemelor steganografice prin combinarea cu alţi algoritmi mai performanţi din punct de vedere al cantităţii de informaţii, cum ar fi cei din domeniul spaţial.

În capitolul 9 au fost concepuţi un set de algoritmi prin care s-a urmărit îmbunătăţirea performanţelor unuia dintre parametrii sistemelor steganografice. În acest sens pentru a obţine o cantitate maximă de informaţii ce poate fi ascunsă, am conceput un algoritm steganografic denumit $ASAC$ bazat pe comprimarea mesajului secret fără pierderi semnificative de informaţii şi ascunderea acestuia în biţii cei mai puţini semnificativi ai obiectului de acoperire. Cele trei variante ale algoritmului

confirmă cantitatea extrem de mare a informaţiei (100%) ce poate fi ascunsă fără degradarea obiectului steganografic a cărui calitate este de necontestat, iar recuperarea mesajului secret se face în condiţii foarte bune.

Un al doilea algoritm denumit $ASAZ$ dezvoltat în acest capitol se bazează pe îmbunătăţirea robusteţii sistemului steganografic. Astfel, mesajul secret este ascuns în zgomotele generate în mod pseudoaleator şi de aşa manieră încât ele să nu conducă la degradarea imaginii obiectului steganografic. În acest fel un eventual atacator ar putea interpreta obiectul steganografic ca fiind afectat de zgomotele induse pe canalul de transmisie.

Al treilea algoritm realizat şi denumit $ASAC_{MS}$ constă în ascunderea mesajului secret prin codarea acestuia cu ajutorul unei chei secrete, ceea ce face imposibilă descifrarea mesajului de către un eventual atacator fără cunoaşterea acestei chei. Algoritmul s-a realizat în două variante de ascundere a mesajului secret, respectiv două variante de extragere a acestuia independente de modul de ascundere. Toate variantele acestui algoritm conduc la obţinerea unui obiect steganografic de o calitate foarte bună, în schimb recuperarea mesajului este nuanţată de modul în care acesta este extras.

În finalul lucrării sunt prezentate concluziile, contribuţiile personale şi posibilele direcţii de cercetare în opinia autorului. Teza se întinde pe 219 de pagini, conţine 70 de figuri, 15 tabele, un număr de 184 de titluri bibliografice. O mare parte din contribuţii au fost validate prin publicarea a 6 lucrări ştiinţifice la care autorul tezei este prim autor, după cum urmează:

- 3 lucrări publicate în volumele unor conferinţe indexate ISI Proceedings,
- 3 lucrări publicate în volumele unor conferinţe indexate Inspec şi IEEExplore.

2 MEDII FOLOSITE PENTRU APLICAREA STEGANOGRAFIEI

Steganografia exploatează comunicarea ce pare inofensivă la prima vedere pentru un observator întâmplător, utilizând diferite medii în care poate ascunde datele secrete. Mediile de ascundere pot fi de diferite forme: text, imagine, sunet etc. Pentru ca procesul steganografic să fie realizat cu succes este foarte important ca mediul ales pentru ascunderea informaţiilor secrete să nu atragă atenţia asupra lui, şi anume să pară cât mai inofensiv. De asemenea este necesar ca acesta să conţină suficiente informaţii astfel încât mesajul ce urmează a fi ascuns să nu devină vizibil.

Multimedia reprezintă capacitatea unui sistem de a comunica prin intermediul mai multor medii de prezentare, cum ar fi text, grafică, fotografii, animaţie, sunet etc. În plus, multimedia implică şi noţiunea de interactivitate, deoarece utilizatorul nu este un simplu spectator. Se pot deosebi diferite metode de ascundere a informaţiilor secrete, în funcţie de mediul prin care acestea sunt transmise. În capitolul de faţă se descriu cele mai utilizate medii în care este aplicată steganografia.

2.1 *Steganografia în text*

Ascunderea mesajelor secrete în interiorul unui text este una din metodele steganografice aplicate încă din cele mai vechi timpuri. De-a lungul timpului a avut loc o evoluţie în domeniul comunicării prin dezvoltarea unor noi tehnologii în care un rol semnificativ îl constituie utilizarea calculatoarelor.

În ceea ce priveşte documentele tip text, acestea pot fi modificate în vederea ascunderii unei informaþii secrete prin manipularea poziþiilor liniilor ºi cuvintelor. În acest sens pot fi amintite o serie de metode care utilizează ca suport pentru ascunderea unei informaţii secrete obiecte de tip text. În [JOH01] se prezintă câteva soluţii utilizate de-a lungul timpului pentru ascunderea informaţiilor secrete în texte prin diferite artificii efectuate în cadrul acestora, cum ar fi: exploatarea spaţiilor adăugate în plus în documente între cuvinte, fraze, rânduri; folosirea metodelor semantice prin schimbarea unor cuvinte sinonime; generarea de obiecte steganografice noi prin care eventualul atacator să nu sesizeze existenţa unei informaţii ascunse.

În [CAS07] se propune un sistem steganografic pentru ascunderea datelor în documente Microsoft Office, iar [GAR04] prezintã câteva experimente fãcute în vederea determinării problemelor care apar în urma aplicării steganografiei în documente Word. În lucrare se propun soluþii care sã rezolve aceste probleme. În sistemele tip bibliotecã digitalã, documentele sunt disponibile în formã digitalã, iar în acest mod, pot fi uºor copiate ºi identitatea lor poate fi supusã riscului unui eventual atac. Acest fapt duce la descurajarea celor ce publicã documente ce conþin

informaþii de valoare, deoarece există posibilitatea pierderii titlul de autor. În [SER95] se

propune un sistem pentru înregistrarea documentelor existente într-o librărie digitală, după care este realizat un serviciu ce detectează copiile făcute. În acest sens, pot fi identificate copiile făcute parţial sau complete la documentele în cauză. În lucrare se descriu algoritmii folosiţi pentru astfel de detecţii şi totodată sunt prezentate metricile necesare în vederea evaluării metodelor de detecţie.

O altă aplicaţie interesantă de securizare a informaţiei constă în stabilirea unor comunicări ascunse bazate pe steganografie prin intermediul telefoniei mobile în cazul folosirii serviciului SMS, ce a fost primit cu mare căldurã de oamenii din întreaga lume. Folosind acest serviciu oamenii pot comunica uºor prin scrierea ºi trimiterea de mesaje scurte de la unul la altul. De asemenea, pot fi trimise ºi poze alb-negru sau color prin intermediul acestui serviciu. La orice tip de comunicare este indicat să se þinã seama de aspectul securitãþii informaþiei. Deoarece se manifestã un tot mai mare interes pentru stabilirea comunicării ascunse se dezvoltã tehnici steganografice ºi în cazul folosirii serviciului SMS.

Astfel, în [SHA07b, SHA08b] se prezintã douã metode utilizate pentru schimbul secret de informaþii prin ascunderea acestora în mesaje SMS sau prin intermediul unui joc transmis tot prin serviciul SMS. În [SHA06a] se propune o metodã pentru schimbul ascuns de date secrete prin realizarea unui proces steganografic în care obiectul de acoperire folosit este o imagine, iar aceasta este încorporatã într-un mesaj SMS. Ideea de bazã urmãritã constã în aplicarea steganografiei în imagini alb-negru ºi realizarea acestui proces prin intermediul telefoniei mobile. Trebuie avut în vedere faptul cã utilizarea mesajelor SMS prezintã anumite limitări.

O altã aplicaþie privind folosirea steganografiei în telefonia mobilã prin intermediul serviciului MMS (Multimedia Messaging Service) este dezvoltat în [SHA08a] unde tehnologia MMS este folositã pentru transmiterea unor mesaje ce includ obiecte multimedia printre care ºi imagini. Pentru protecþia imaginii care este transmisã prin MMS se foloseºte o metodã de marcare a acesteia. La extragerea mesajului din MMS se poate constata dacã aceasta a fost duplicatã sau nu.

Deoarece la ora actualã foarte multã lume foloseºte Internet-ul, există multe posibilitãþi de a transmite date ascunse pe această cale. În acest sens pot fi alese ca obiecte de acoperire documente în format HTML. Pentru a ascunde mesaje secrete este necesar să fie luate în considerare informaþiile ce pot fi ignorate de browser**.** Există site-uri de comerþ electronic care folosesc cãsuþe ascunse pentru a indica starea. Acestea pot fi folosite pentru a ascunde informaþie, dar devin vizibile în cazul în care se consultã codul sursã. În acest sens inserarea spaþiilor în paginile HTML este o modalitate de aplicare a steganografiei. În general, un simplu observator nu verificã sursa HTML, ca urmare, poate fi aplicatã steganografia prin inserarea informaþiilor ascunse folosind spaþiile ramase libere. În vederea protecþiei aplicaþiilor Java contra copierii, [SHA06c] prezintã o metodã ce aplicã o tehnicã steganograficã pentru pagini web în format HTML. Mesajul secret, format dintr-un ºir de 8 caractere, este ascuns cu ajutorul unei chei secrete într-o paginã HTML, aleasã ca ºi obiect de acoperire pentru realizarea procesului steganografic. Proiectul propus este implementat prin aplicarea limbajului de programare Java, prin intermediul cãruia, informaþia ºi cheia secretã sunt încorporate în obiectul de acoperire ales. Dupã execuþia programului, aplicaþia Java extrage datele din pagina HTML folosind cheia secretã.

În concluzie, metoda steganograficã ce are ca suport de ascundere un text este consideratã una dintre cele mai vechi metode, iar pânã la apariþia noilor

tehnologii audio-video, era printre puþinele metode cu rezultate satisfãcãtoare. În prezent modalitatea de ascundere a datelor în text ºi-a pierdut în mare parte interesul, având în vedere posibilitãþile reduse de ascundere. Procesele steganografice care folosesc ca ºi mediu de transmitere a datelor secrete textul, prezintã ºi dezavantajul cã din punct de vedere cantitativ se poate remarca un procent destul de mic de informaþii ce pot fi ascunse. În ultimul timp, în urma apariþiei telefoniei mobile ºi utilizarea destul de largã a transmiterii mesajelor prin SMS, s-a încercat revigorarea metodelor de ascundere având ca suport un text SMS, dar bineînþeles ºi în aceastã situaþie limita acestui suport de ascundere îºi spune cuvântul permiþând astfel doar ascunderea unor informaþii reduse cantitativ.

2.2 *Steganografia în fiºiere executabile*

Multimedia este în primul rând perceputã de simþurile umane care sunt de multe ori imperfecte. De aceea conþine o cantitate de date redundante ce pot fi suprascrise cu mesaje secrete. Mai mult, acestea pot conþine o serie de zgomote datorate anumitor procese, cum ar fi:scanare, înregistrare. Prin contrast fiºierele executabile sunt rareori percepute vizual. Ele simt prezenþa prin sarcina pe care trebuie sã o îndeplinească. În teorie douã executabile sunt echivalente dacã produc acelaºi rezultat pentru date de intrare identice. În practicã, însã existã ºi alte constrângeri, cum ar fi: spaþiu, timp de execuþie, încãrcarea pe procesorul pe care-l comandã. Chiar ºi aºa, existã un numãr mare de fiºiere executabile echivalente, lucru ce poate fi folosit în optimizare, semnare digitalã, watermarking, steganografie, etc.

Una din modalitãþile aplicate pentru ascunderea datelor într-un program executabil ar putea consta în încorporarea mesajului secret dupã apariþia marcajului de sfârºit de fiºier (EOF). În acest caz, programul rulează fãrã nici o problemã, deoarece informaþia scrisã dupã sfârºitul de fiºier este ignoratã.

În [BER05] se cercetează o parte din domeniul steganografiei aplicatã programelor executabile. Este cunoscut faptul cã steganografia ascunde un mesaj secret într-un obiect de acoperire, iar în lucrare se identificã 3 tipuri de obiecte de acoperire cu redundanþã utilizabilã în programe executabile. Se prezintã de asemenea tehnici steganografice pentru cercetarea acestor redundanþe.

Utilizarea fişierelor executabile ca mediu purtător prezintă dezavantajul că nu toate formatele oferă redundanţă suficientă pentru steganografie, ceea ce conduce la reducerea posibilităţilor de ascundere a mesajelor secrete. Încercările de utilizare ale fişierelor în acest sens sunt cu precădere destinate protecţiei anumitor aplicaţii.

2.3 *Steganografia aplicatã mediilor de stocare*

Steganografia poate fi aplicatã în diferite medii de stocare ale calculatorului, cum ar fi: spaþiile neutilizate de pe discul calculatorului, partiþii ascunse, discuri optice, etc.

Ascunderea informaþiilor în spaþiile de pe disc este o metodã steganograficã ce se bazeazã pe descoperirea spaþiilor neutilizate de pe discul calculatorului, deoarece acestea nu sunt vizibile pentru un observator.

Crearea de partiþii ascunse este o altã modalitate de ascundere a datelor secrete. Cu ajutorul acestei metode pot fi ascunse cantitãþi mari de informaþie, dar în multe cazuri, prin rularea unui program de configurare a discului se descoperã partiþia ascunsã. Aºadar, aceastã metodã dã rezultate bune, doar dacã utilizatorii calculatorului respectiv nu au o pregãtire bunã în acest domeniu.

Contestarea plauzibilã poate fi de asemenea utilizatã în steganografie în situaþia în care un atacator doreºte sã obþinã de la posesorul unui calculator în mod forþat o informaþie secretã ascunsã. Acestuia i se poate furniza de cãtre proprietar o parolã falsã cu ajutorul cãreia atacatorul crede cã obþine ceea ce cautã, deºi adevãrata informaþie secretã este ascunsã ºi criptatã cu o altã parolã, dar a cãrei existenþã nu poate fi demonstratã.

Codarea contestabilã a informaþiilor poate fi utilizatã în criptografie pentru a descrie tehnici steganografice, în care existenþa unui mesaj sau fiºier codat este contestabilã, în ideea cã atacatorul nu poate demonstra aceastã existenþã. În acest sens existã sisteme, cum ar fi TrueCrypt, ce au ca principiu de bazã ascunderea datelor criptate. Astfel, proprietarul datelor criptate poate avea mai multe chei ce pot fi folosite pentru decriptarea mai multor informaþii, dar acesta poate nega în faþa unui eventual atacator cã existã aceste chei, rezultând astfel o afirmaþie care nu poate fi contrazisã fãrã cunoaºterea tuturor cheilor de criptare implicate. În acest fel, existenþa unor date ascunse în datele criptate este contestabilã, în sensul cã aceasta nu poate fi demonstratã [FRU05].

Ascunderea informaþiilor pe dischete ºi discuri optice prezintã de asemenea o posibilitate de ascundere a unor informaþii secrete. Este cunoscut faptul cã atât pe dischete cât ºi pe discurile optice existã o serie de spaþii neutilizate [BAR00] care pot fi exploatate ca ºi obiecte de acoperire într-un proces steganografic. Datele binare nefolosite pot fi utilizate chiar la protecþia clonãrii discului sau copierii ilegale a datelor existente. Acest lucru este cu atât mai valabil în ultimul timp la discurile optice de mare capacitate, cum sunt: DVD, BLUE RAY, HDVD pe care marile firme producãtoare de filme inscripþionează ultimele producþii ºi din acest motiv iau toate mãsurile de protecþie împotriva clonãrilor, avându-se în vedere investiþiile masive care se fac în producþiile de filme.

În concluzie, ascunderea datelor secrete în diferite medii de stocare chiar dacã prezintã unele avantaje legate de cantitatea de informaþie ascunsã posibilã, prezintã ºi dezavantaje, în sensul cã, prin rularea unor programe de configurare este posibilã descoperirea datelor mascate. În general aceste medii de ascundere pot da rezultate bune cu precãdere în cazul unor aplicaþii particulare, cum ar fi: protecþia unor date confidenþiale aflate în partiþii ascunse sau a proprietãþii intelectuale .

2.4 ***Steganografia aplicatã în reþele de calculatoare***

Se poate spune că în urma extinderii comunicării prin Internet s-au dezvoltat şi metode steganografice de ascundere sau de protecţie a datelor. Încercările cele mai numeroase au fost direcţionate mai puţin în domeniul ascunderii

datelor şi mai mult în direcţia protejării acestora ca o măsură suplimentară pentru a asigura securitatea datelor transmise. Din acest motiv comunicările prin Internet utilizează cu precădere pentru protecţia datelor, instalarea şi configurarea unor softuri de securitate, cum ar fi: Antivirus, Anti-Spyware, Anti-Malware, Firewall, etc. Utilizarea acestor programe necesită actualizări periodice deoarece zilnic apar noi ameninţări, noi atacuri, noi viruşi şi se descoperă noi vulnerabilităţi în programele existente. Din acest motiv sunt necesare a fi luate în considerare măsuri suplimentare de protecţie, iar steganografia poate avea un rol suplimentar în acest sens. Astfel, ascunderea informaþiilor în ceea ce priveºte comunicarea prin reþelele de calculatoare poate fi realizatã în: ataºamente, antetul protocoalelor de reþea, protocoale în timp real, protocoale publice ºi reþele fãrã fir.

2.4.1 Ascunderea informaþiilor în ataºamente

O posibilitate de acoperire a comunicării ascunse între un emiþător ºi un anumit receptor, o constituie transmiterea de mesaje aparent inofensive, sub forma unor ataºamente tip text, imagine etc. În [COL03] sunt prezentate o parte dintre metodele folosite pentru transmiterea informaþiilor ascunse prin intermediul Internet-ului:

Email - ul – Poate constitui o soluþie facilã de trimitere a unei informaþii secrete în texte, sunete sau imagini, în special dacã între emiþător ºi receptor existã un transfer real de informaþii care sã mascheze adevãratul scop al comunicării secrete. O altã metodã folositã în acest sens este trimiterea unui email la mai mulþi destinatari sub forma cunoscutã de spam. În această situaþie, doar persoana vizatã ºtie sã caute datele ascunse.

Transfer de fiºiere sau FTP (File Transfer Protocol) – Această metodă presupune publicarea unui fiºier cu un conþinut ascuns, care de fapt constituie obiectul steganografic. În acest caz numai o persoanã avizatã va ºti ce sã caute. Eficienþa acestui tip de transmisie o constituie faptul cã nu existã o dovadã a celui care a publicat informaþia ºi nici a celui care este interesat de ea.

Publicarea pe Internet – este o tehnicã ce constã în publicarea unui fiºier cu date ascunse, ales ca obiect de acoperire, la vedere pe Internet pe un anumit site. Spre exemplu, pot fi încorporate date ascunse în poze create pe calculator, ce pot fi postate pe un site dedicat în acest sens. ªi această metodă ascunde identitatea destinatarului ºi a emiþătorului.

2.4.2 Ascunderea informaþiilor în antetul protocoalelor de reþea

Caracteristicile esenþiale ale protocoalelor de reþea pot fi considerate un avantaj în ascunderea informaþiilor. Zilnic sunt transmise prin intermediul Internet-ului un numãr extrem de mare de pachete de date, ceea ce reprezintã o modalitate bunã pentru comunicarea secretã. Spre exemplu, pachetele TCP/IP (Transmission Control Protocol/Internet Protocol) pot fi utilizate în scop steganografic, prin transferul informaþiilor secrete prin intermediul Internet-ului. În acest sens, pot fi

exploatate ca obiecte de acoperire, antetele care au spaþii nefolosite ºi alte caracteristici ce pot fi manipulate pentru ascunderea informaþiilor.

Multe dintre protocoale existente au fost create în urmã cu mulþi ani, chiar de la apariþia Internet-ului. Ele conþin informaþii care acum nu mai sunt necesare ºi din acest motiv pot fi înlocuite cu date secrete ºi pot fi utilizate ca ºi obiecte de acoperire în procesul steganografic.

Pentru realizarea procesului steganografic este necesarã stabilirea obiectelor de acoperire ce urmeazã a fi folosite în vederea ascunderii datelor secrete. Trebuie identificate câmpurile ce ar putea fi suprascrise fãrã a afecta transmiterea informaþiilor în nici un fel. Anumite câmpuri din antetul protocolului IP trebuie sã conþinã informaþii specifice, cum ar fi, lungimea antetului. În cazul în care nu se respectã aceastã condiþie, procesul de comunicare va eºua. În schimb, existã un câmp în antetul protocolului IP numit Pachet Identificare, care poate fi exploatat. Acesta este folosit pentru a detecta pachetele care au fost fragmentate, astfel, dacã un pachet este prea mare, el este împãrþit în mai multe pachete. Receptorul ºtie sã le reconstituie dupã identificatorul pachetului. De obicei, identificatorul pachetului este incrementat cu 1 pentru fiecare pachet care este trimis, iar pentru identificarea pachetului poate fi folosit orice numãr.

[XUB07] prezintã o nouã cale de comunicare ascunsã între diferite puncte de pe Internet. În lucrare se propune o schemã ce foloseºte o parte dintr-un sistem creat haotic numit Chebâshev. Acest sistem generează aleator diferite secvenþe ce sunt utilizate ca ºi obiecte de acoperire în vederea încorporării de mesaje secrete, dupã care ascunde mesajele secrete în câmpuri identificate, cum ar fi antetul protocolului IP.

Steganografia aplicatã pe Internet reprezintã exploatarea elementelor Internet ºi a protocoalelor cu scopul de a ascunde date suplimentare în procesul de comunicare [DEE03]. În acest sens, fiecare schemã realizatã presupune stabilirea unei interacþiuni între principiile steganografice fundamentale cu mediile de securitate ale reþelelor existente. Scopul urmãrit este de a crea o legãturã între zonele unde sunt ascunse datele, protocoalele de reþea utilizate ºi securitate. În [DEE03] se prezintã douã canale ascunse, folosite ca obiecte de acoperire în procesul steganografic, legate de Protocoale de Internet (IP) ce exploatează redundanþele rezultate în reprezentarea informaþiei.

Antetul protocolului TCP foloseºte numere de confirmare pentru a ºti câte date au fost trimise ºi câte au fost recepþionate. În timpul primei faze de comunicare, sunt alese numere aleatorii de confirmare, generate atât de către emiþător , cât ºi de receptor. Aºadar, datele pot fi ascunse în primul pachet trimis, deoarece numerele sunt oricum generate aleator ºi nu împiedicã transmiterea informaþiilor cu nimic. Dupã ce este stabilit canalul de comunicare, aceste valori devin critice, ele fiind absolut necesare realizãrii procesului de comunicare. Este necesar de subliniat faptul cã datele pot fi ascunse doar în timpul secvenþei iniþiale.

În steganografie nu poate fi utilizat orice protocol pentru ascunderea datelor, datoritã caracteristicilor acestora legate de mãrimea antetului foarte micã ce nu permite încorporarea unor date secrete suplimentare. În aceastã situaþie se gãsesc spre exemplu protocoalele UDP (User Datagram Protocol) ºi ICMP (Internet Control Message Protocol).

Multe dintre protocoalele utilizate ca şi mediu de ascundere pot crea dificultăţi în implementarea unor algoritmi steganografici. În această categorie intră acele metode care folosesc ca loc de ascundere antetul protocoalelor, deoarece spaţiul disponibil este foarte mic.

În concluzie, ascunderea datelor secrete în diferite protocoale utilizate în reţelele de calculatoare poate prezenta avantaje legate de flexibilitatea şi posibilităţile foarte largi de ascundere a datelor, dar prezintă şi dezavantaje legate de cantitatea mică de date ascunse şi de atacurile frecvente întâlnite în astfel de medii. Respingerea unui eventual atac, nu asigură şi recuperarea în totalitate a mesajului ascuns.

2.4.3 Ascunderea informaþiilor în protocoale în timp real

În ultimii ani se remarcã o creºtere continuã pentru ascunderea, trimiterea ºi afiºarea informaþiilor în timp real, în special în locuri publice. Acest proces a întâmpinat mari provocări ºi a atras atenþia multor cercetători.

Unul dintre cele mai populare servicii utilizat în ziua de azi în reþele, îl constituie VoIP Voice over Internet Protocol, ce a apărut pe piaþa telecomunicaþiilor schimbând-o în întregime. Deoarece este utilizat din ce în ce mai mult în întreaga lume, implicã totodatã ºi creºterea traficului pe canalele de comunicare. VoIP este un serviciu în timp real care permite comunicarea audio în reþelele IP.

[MAZ06, MAZ08] prezintã protocoale utilizate în vederea securitãþii ºi controlului pentru serviciul VoIP RTCP (Voice over Internet Protocol – Real Time Control Protocol) în situaþia transferului de informaþie în timp real. Protocolul RTP (Real Time Protocol) este cel mai important protocol de transport pentru transmisii audio în timp real, iar RTCP este un protocol de control pentru RTP. În plus, se oferã soluþii de autentificare ºi integritate pentru mesajele tip voce, care sunt capabile sã schimbe ºi sã verifice calitatea serviciului ºi parametrii de securitate. Protocolul propus foloseºte douã tehnici de ascundere a informaþiei secrete: steganografia pentru a putea crea un canal ascuns prin care sã fie transmiºi biþii de control ºi watermarking-ul digital pentru a transmite valorile parametrilor utilizaþi pentru emisia de voce. Procesul steganografic ce utilizează un astfel de protocol prezintă avantajul cã transmiterea informaþiei se realizează în mod continuu în timp, rata biþilor de transfer pe secundã este destul de înaltă, iar cantitatea de date ascunsă este destul de mare.

O altă tehnică folosită în vederea ascunderii datelor în timp real este prezentată în [SHA06d]. Metoda propusă se bazează pe ascunderea mesajului secret în timp real în ecrane de ieºire similare cu cele arătate prin intermediul monitorului. Procesul steganografic astfel realizat este foarte asemănător cu două procedee foarte populare, ºi anume: steganografia în imagini ºi steganografia în video.

E bine de remarcat faptul că algoritmii steganografici utilizaţi în comunicarea prin intermediul reţelelor de calculatoare trebuie implementaţi astfel încât să facă faţă unui eventual atac în timp real.

2.4.4 Ascunderea informaþiilor în protocoale publice ºi reþele fãrã fir

Ascunderea datelor în protocoale publice poate fi numită ºi camuflarea datelor [COL03]. Aceastã tehnicã constã în transmiterea datelor prin reþea ca ºi cum ar exista un protocol deschis sau public. Un exemplu îl constituie Protocolul

HTTP, deoarece foarte multe reþele au trafic mare pe portul 80, corespunzător acestui protocol. Datele secrete pot fi trimise pe acest port, dar dacă o persoană interesată ar examina traficul, ar descoperi că datele trimise nu reprezintă trafic Web. În cazul în care se adaugă documente în format HTML la datele transmise, atunci acestea ar semăna cu traficul web ºi ar trece nedetectate.

Creºterea continuă a comunicaþiilor ce au loc pe calea Internet-ului a dus la producerea mai multor programe software ce pot fi lansate pe Internet fără a fi nevoie să fie instalate anterior pe calculator. Programele sunt aplicate în funcþie de domeniul dorit, cum ar fi: divertisment (jocuri), financiar, comercial etc.

Spre exemplu în [SHA08b] se utilizează pentru ascunderea informaþiilor un joc de puzzle foarte popular pentru ascunderea unor mesaje ce pot fi transmise prin telefonia mobilă. Utilizarea acestei căi nu atrage atenþia existenþei informaþiei ascunse pentru un posibil atacator. O mare parte din programele de ascundere folosesc limbajul de programare Java ºi pot fi găsite pe pagini de web ca ºi Aplicaþii Java. Autorul Shahreza descrie în [SHA06b] o procedură de conectare la Internet prin telefonia mobilă folosind protocolul WAP (Wireless Application Protocol) prin care mesajul ascuns este plasat în paginile WML (Wireless Markup Language).

În [LEP07] se prezintă un model de protocol de ascundere a mesajului în care toate acþiunile sunt publice, în ideea generării unei soluþii steganografice folosind ºi protocoale criptografice prin care mesajul ascuns permite legitimarea traficului de informaþii.

Telefoanele mobile, precum ºi tehnologiile aplicate pe Internet au avut o creºtere continuă în ultimii ani. Legătura dintre acestea a dus la inventarea de noi tehnologii de comunicare, cum ar fi stabilirea de conexiuni fără fir (wireless) pe Internet prin telefoane mobile, cunoscute sub denumirea de Protocoale de Aplicaþii Wireless (WAP).

O reţea denumită wireless (Wi-Fi) WLAN este o reţea fără fir locală, extinsă pe arii limitate în funcţie de echipamentele folosite şi de puterea acestora, prin care se poate face transfer de date şi Internet folosind undele radio. O constrângere legată de utilizarea reţelelor wireless ar putea fi lăţimea de bandă (mediul fizic de comunicare este partajat şi are oricine acces la el), rata de eroare, mobilitatea şi nu în ultimul rând securitatea.

Steganografia este o metodă relativ nouă, aplicată în vederea creşterii securităţii datelor şi în special a stabilirii de comunicări ascunse prin intermediul protocoalelor de reţea fără fir.

[SHA06b] prezintă o metodă ce permite transmiterea unor date secrete sub o formă ascunsă, prin aplicarea unui proces steganografic la pagini web WML. Aceste pagini sunt create special pentru a facilita comunicarea prin reţele fără fir (WAP). Programul de codare a fost implementat folosind limbajul Java, iar programul de decodare utilizează o versiune a limbajului Java aplicată în cazul dispozitivelor de dimensiune mai mică, numită J2ME (Java 2 Micro Edition). S-a apelat la această versiune pentru ca programul să poată fi implementat pe telefoane mobile.

În [CHR06] sunt descrise şi discutate rezultate privind siguranţa, nedetectarea şi capacitatea a două modele diferite propuse pentru construirea unui canal steganografic. Cele două modele sunt prezentate sub forma unor prototipuri WLAN ce au fost implementate şi testate.

Transmiterea multimedia prin reţele fără fir are tendinţa de a fi deosebit de populară, deoarece multe telefoane mobile sunt deja echipate cu ecrane cu o varietate de culori şi prezintă multe aplicaţii multimedia. Din acest motiv în [HON04] este făcută o analiză a posibilităţilor de transmitere şi accesare a datelor multimedia

pe canalele de comunicaţii fără fir. Astfel de comunicaţie devine provocatoare datorită mobilităţii aparaturii. În schimb se ridică o serie de restricţii legate de puterea limitată a telefoanelor mobile, banda de transmitere impusă şi influenţa mediului înconjurător. Toate acestea pot genera erori de transmisie ce pot afecta integritatea mesajului transmis, dar şi securitatea comunicării. În articol se propune ca în procesul de transmitere să fie încorporate informaţii de detecţie şi corecţie a erorilor. Astfel de metode pot asigura şi o transmitere sigură a mesajului steganografic [BEE08].

Multe din aplicaţiile steganografiei sunt utilizate pentru marcarea proprietăţii intelectuale a datelor audio, video, text. Ca urmare, în [PET05, DUT05] sunt prezentate studii privind posibilitatea ascunderii unor informaţii secrete în videoclipuri transmise spre terminale mobile în reţele fără fir a unor mărci privind protecţia proprietăţii cu rezultate mulţumitoare din punctul de vedere al rezistenţei la atacuri clasice pentru protejare fie a coloanei sonore transmisă, fie a reclamei în cauză.

În concluzie, în ceea ce priveşte securitatea reţelelor fără fir se poate spune că acestea sunt relativ mai puţin sigure decât cele cablate, datorită accesului mai facil la reţea al persoanelor neautorizate aflate în zonele de acoperire ale punctelor de acces. Există în implementarea reţelelor fără fir, diferite obstacole ce formează aşa numita securitate de bază a reţelelor fără fir, care împiedică accesul neintenţionat al persoanelor străine de reţea, aflate în aria de acoperire a unui punct de acces. Pentru persoane rău intenţionate cu o bună pregătire în domeniul calculatoarelor, securitatea acestor reţele este discutabilă.

2.5 *Steganografia în audio*

Dintre toate mediile de comunicare, imaginile poartă cea mai mare cantitate de informaţie, iar sunetul are calitatea de a fi cea mai subtilă cale de a transmite informaţie. Efectele sonore pot fi incluse într-o aplicaţie multimedia pentru a îmbogăţi conţinutul. În acest sens, sunetul este un mediu eficient pentru a atrage atenţia utilizatorului, deoarece prin vorbire se poate aborda un aspect particular într-o manieră directă. Având acces direct la sufletul uman, spre deosebire de imagini şi text, sunetul poate induce în modul cel mai rapid şi direct o paletă largă de stări sufleteşti.

În situaţiile în care se ascund date într-un obiect de acoperire tip sunet, trebuie să fie luat în vedere sistemul auditiv uman, ţinând cont de cele mai importante caracteristici fizice ale sunetelor: înălţimea, intensitatea, respectiv timbrul sunetului [STA99].

Sistemul auditiv uman este foarte perceptibil la diferite zgomote de fond, în schimb nu poate diferenţia variaţii subtile în frecvenţă. Înălţimea unui sunet se referă la frecvenţa acestuia. Sunetele cu frecvenţă ridicată sunt percepute ca fiind mai înalte. De aici rezultă şi una din calităţile sunetului, de a fi mai grav sau ascuţit.

Intensitatea sau amplitudinea unui sunet este o caracteristică a sunetului ce poate fi percepută de urechea umană în mod obiectiv, ca şi intensitate sonoră (acustică) sau subiectiv ca şi intensitate auditivă într-o scară logaritmică.

Timbrul sunetului este una din caracteristicile sunetului ce permite diferenţierea între două sunete de aceeaşi intensitate şi frecvenţă, dar emise de două surse diferite. Sunetul emis de o sursă sonoră este format din mai multe

sunete cu frecvenţe diferite, iar timbrul sunetului este determinat de numărul acestor sunete şi de distribuţia energiei dintre ele, deoarece aceasta diferă de la o sursă la alta.

În cazul în care un sistem steganografic optează ca obiectul de acoperire să fie sunetul trebuie luate în considerare două aspecte importante: modalitatea de stocare sau reprezentarea digitală a sunetului, respectiv mediul de transmisie al acestuia.

Spre exemplu, [BAO04] descrie o schemă steganografică pentru un sistem audio în care sunt încorporate date ascunse ce sunt transportate prin intermediul unei melodii. În [KES04] este prezentată o altă soluţie posibilă de ascundere a informaţiei în sunet unde în urma încorporării mesajului secret rezultă obiectul steganografic tot sub formă de sunet, eventual perceput de către urechea umană ca fiind mai zgomotos.

Ascunderea informaţiilor în imagini sau audio nu are un impact virtual în sistemul senzorial uman. În cazul imaginilor ascunderea informaţiilor se poate realiza prin modificarea luminozităţii, contrastului sau culorilor. În audio pot fi adăugate ecouri, întârzieri mici sau pot fi mascate semnale corespunzătoare mesajului secret prin sunete de amplitudine înaltă.

Algoritmii folosiţi pentru ascunderea informaţiilor secrete în sistemele audio în general se bazează pe aceleaşi tehnici ca cele utilizate şi în imagini, cum ar fi: ascunderea în cei mai puţini semnificativi biţi, metode bazate pe transformate în domeniul frecvenţă.

O soluţie privind ascunderea unui mesaj secret într-un obiect de acoperire tip sunet este prezentată în [NED04]. În acest sens algoritmul steganografic propus se bazează pe metoda inserţiei în biţii cei mai puţini semnificativi.

În [POO07] este realizată o metodă steganografică în care obiectul de acoperire ales este un semnal audio digital. Astfel, datele ascunse sunt încorporate în coeficienţii de undă ai semnalului audio folosit ca şi obiect de acoperire. Pentru evitarea erorilor la extragerea mesajului ascuns se aplică diferite permutări între coeficienţii transformatei de undă. În vederea folosirii capacităţii maxime a unui semnal audio, se calculează pragul de auz în domeniul undă. Ţinând cont de acest prag, biţii cu date sunt încorporaţi în cei mai puţin semnificativi biţi ai coeficienţilor permutaţi de undă. Permutarea inversă a transformărilor de undă se aplică în vederea modificării coeficienţilor pentru construirea semnalului audio steganografic rezultat în domeniul timp.

[MAT06] prezintă o metodă de ascundere a datelor prin distribuirea acestora în spectrul audio. În acest sens se introduc mutări de faze în semnale audio pentru a reduce corelaţia cu semnalele pseudo-aleatoare pentru fiecare sub-bandă.

Pe lângă metodele de ascundere comune folosite atât în sunet, cât şi în imagini pot fi desprinse şi soluţii specifice pentru steganografia în audio, cum ar fi: adăugarea ecoului sau alte acorduri muzicale ce pot fi folosite la ascunderea mesajului fără a fi interpretat de un eventual atacator în acest sens. Un astfel de sistem steganografic cu o robusteţe ridicată se prezintă în [ERF09] unde datele secrete sunt adăugate în ecoul unui semnal audio.

În concluzie, folosirea sunetelor digitale ca şi medii purtătoare pentru transmiterea informaţiilor ascunse prezintă dezavantajul existenţei unei bande de frecvenţă relativ redusă, în care datele secrete pot fi ascunse. Aceasta implică în mod evident şi o cantitate destul de mică de informaţii ce pot fi transmise pentru a fi protejate pe această cale. Cu toate acestea sunt de menţionat câteva rezultate în acest domeniu, inclusiv încercări de realizare a unor emiţătoare – receptoare audio care să permită generarea unor informaţii care să nu fie recepţionate voit sau

accidental de alte persoane. Mai mult, dacă aceste informaţii nu pot fi detectate în timp real, ele ar putea fi detectate ulterior prin înregistrare şi spargere a algoritmilor de ascundere, cu atât mai mult cu cât aceşti algoritmi folosesc în general metode mai puţin sofisticate.

2.6 *Steganografia în video*

Steganografia în video presupune folosirea obiectelor video digitale ca şi obiecte de acoperire pentru a transmite informaţii secrete. Ascunderea datelor în imagini şi video este de obicei realizată prin intermediul modificărilor de neperceput asupra datelor vizuale.

Un obiect video digital este alcătuit dintr-o serie de imagini sau cadre care presupun o prelucrare în prealabil pentru a putea fi transmise. Digitizarea secvenţelor audio şi video solicită resurse considerabile de memorie, iar aceasta necesită soluţii de compresie a acestor medii. Pe baza recomandărilor ISO (International Standardization Organization) şi IEC (International Electrotechnical Commision) a fost creată şi publicată compresia obiectelor video digitale de aproximativ 200:1, recunoscută sub denumirea MPEG-1[BUR08]. La ora actuală sunt cunoscute mai multe astfel de metode de compresie, cum ar fi: MPEG, AVI, DivX, Xvid etc.

În principiu, compresia se bazează pe existenţa unui cadru de referinţă care la rândul lui este supus unui proces de compresie, în general cu algoritmi asemănători folosiţi la imaginile digitale în format JPEG şi o serie de cadre ce conţin doar diferenţele ce apar în timp între acestea şi cadrul de referinţă. Din acest motiv, procesul de compresie este diferit de la cadru la cadru, existând astfel cadre în care compresia este maximă. De multe ori într-un proces steganografic ascunderea mesajului este posibilă doar în cadrul ce prezintă o compresie minimă. Compresia video este considerată de obicei cu pierderi, deoarece codarea unui cadru cu ajutorul predecesorului său poate presupune apariţia unor distorsiuni, ceea ce implică o posibilă degradare a imaginii finale.

În legătură cu acest tip de codificare se propun în [BUD06] câteva metode de detectare a unor semne watermark ascunse. Acestea sunt realizate prin analize şi simulări aplicate unor secvenţe video digitale bazate pe interacţiunea dintre cadre.

Trebuie remarcat faptul că ordinea de transmitere a cadrelor nu respectă ordinea lor normală de afişare. La codificarea imaginilor ce urmează imaginii de referinţă, sistemul compară macro-blocurile acestora cu macro-blocurile corespunzătoare imaginii de referinţă, şi astfel numai macro-blocurile care prezintă diferenţe sunt luate în considerare la codificare. De exemplu, pentru un interviu fundalul este mereu acelaşi şi va fi codificat ca atare, iar pentru imaginile următoare se pot lua în calcul numai diferenţele [SHA01].

În [CHA06a] se propune un algoritm steganografic ce foloseşte ca mediu de ascundere imagini video în format MPEG. Informaţia ascunsă este încorporată în vectorii de mişcare a macro-blocurilor în care este împărţită imaginea de referinţă. Pentru a face mai uşor procesul de extragere a datelor ascunse, informaţia de control a fost încorporată în cadrul imaginii de tip I, P respectiv B. Avantajele algoritmului propus sunt menţinerea robusteţii în timpul procesării video şi

posibilitatea încorporării unei cantităţi destul de mari de informaţie, dar totodată se remarcă şi dezavantajul degradării virtuale a imaginilor transmise.

După câţiva ani de la apariţia algoritmului de compresie MPEG – 1 s-a dezvoltat un nou algoritm MPEG – 2 văzut ca şi o extensie a acestuia, deşi au în comun aceleaşi proprietăţi de bază. O caracteristică a acestui nou format o reprezintă posibilităţile de transmisie în timp real. Pornind de la principiul de funcţionare al algoritmului MPEG – 2 am propus în [STA07b] un decodor ce utilizează ascunderea de date pentru a transmite date adiţionale fără a necesita o lărgime de bandă suplimentară obţinându-se astfel o degradare aproape de neperceput a imaginii. Datele adiţionale transmise pot fi subtitrări, semnale de corecţie sau watermarking.

De cele mai multe ori, ascunderea în fluxuri video digitale implică aceleaşi tehnici utilizate ca şi la imaginile digitale. O parte din metodele utilizate în steganografia video folosesc transformarea cosinus discretă (DCT), deoarece există posibilitatea ascunderii datelor în acele componente ale imaginii care au frecvenţă înaltă şi care influenţează mai puţin calitatea imaginii. [OGI96] prezintă o astfel de metodă prin care datele secrete sunt încorporate şi ascunse în cadrele care formează un flux video. O posibilă aplicaţie a steganografiei în fişiere video este ascunderea unui mesaj în timpul unei videoconferinţe.

Ca şi o concluzie, datorită faptului că o imagine video este compusă din mai multe cadre, poate conduce la ideea că şi cantitatea de informaţii ascunse este foarte mare. Însă, în realitate de cele mai multe ori cadrele nu se transmit ca imagini independente unul faţă de celălalt şi modificarea unui cadru rezultă automat în modificarea cadrelor următoare. Aceasta poate duce la degenerarea vizibilă a imaginii video, ceea ce poate atrage atenţia asupra faptului că transmisia este de proastă calitate sau că imaginea video conţine date ascunse. Acest fapt încalcă multe din proprietăţile sistemelor steganografice (vizibilitatea, robusteţea etc.). De asemenea, se pune problema timpului de prelucrare a informaţiei care nu poate fi întotdeauna realizată în timp real. Prelucrarea celor 20 de cadre pentru o secundă de transmitere necesită un timp relativ mare pentru comprimarea datelor, la care se va adăuga timpul de încorporare a informaţiei ce urmează să fie ascunsă. Din motivele enumerate mai sus, apreciez că obiectele video digitale nu sunt întotdeauna cele mai adecvate medii de transmitere a unui mesaj secret.

2.7 *Steganografia în imagini digitale*

În general steganografia se bazează pe alegerea unui anumit „purtător” a informaţiei secrete ce urmează a fi ascunsă. În procesul steganografic acest "purtător" este numit obiect de acoperire. În ultimii ani, imaginile digitale au devenit poate cele mai populare purtătoare. Informaţia secretă poate fi înglobată într-o imagine digitală într-o manieră în care imaginea rămâne neschimbată ochiului uman, iar dimensiunea fişierului imaginii rezultate rămâne nemodificată faţă de cea originală. Pentru a reface informaţia încorporată trebuie folosit un algoritm adecvat.

O imagine digitală poate conţine diferite informaţii, cum ar fi: un desen, o hartă, un text şi este formată dintr-un număr fix de linii şi coloane de pixeli. În esenţă, steganografia în imagini explorează limitele sistemului vizual uman. Aşadar, un text, o imagine sau orice altceva ce poate fi încorporat într-un flux de biţi poate fi astfel ascuns. Imaginile digitale pot fi reprezentate în urmãtoarele domenii: spaþial, vectorial ºi frecvenþã.

În domeniul spaţial fiecare pixel este reprezentat într-un sistem de trei axe de coordonate reprezentative pentru cele trei culori de bază: R (roşu), G (verde), B (albastru). Culoarea unui pixel este rezultată ca o sumă ponderată a celor trei culori. O prezentare amănunţită a acestui domeniu se va face în capitolul 4.1.

Domeniul frecvenţă se bazează pe transformata Fourier prin descompunerea semnalului ce reprezintă imaginea în funcţii de sin şi cos ce sunt cunoscute ca funcţii armonice. Acest domeniu prezintă avantajul unei îmbunătăţiri a operaţiilor de procesare a imaginilor. Totodată este permisă realizarea compresiei imaginilor printr-un suport matematic bine definit [GUI99]. O analizã în detaliu a acestui domeniu se face în capitolul 4.2.

În domeniul vectorial imaginea este reprezentată ca o matrice de vectori de pixeli spre deosebire de domeniul spaţial în care imaginea este reprezentată printr-o matrice de pixeli. Imaginea digitală reprezentată în domeniul vectorial necesită ocuparea unui spaţiu de memorie mai mic în calculator, iar dimensiunea vectorilor se poate mări sau micşora fără a se pierde din rezoluţia imaginii. Acest proces duce la schimbarea parametrilor unor funcţii matematice fără a implica numărul elementelor imaginii. În capitolul 4.3 va fi descris mai pe larg acest domeniu de reprezentare.

Imaginile digitale prezintă o serie de caracteristici ce le pot face astfel deosebit de atractive şi în domeniul steganografiei, deoarece au un impact foarte mare asupra oamenilor fiind percepute vizual. Utilizând camere digitale sau video, scanere, calculatoare, telefonie celulară, imaginile pot fi regăsite în filme, reclame, poze personale sau din vacanţe, artă, pictură, etc. Din punctul de vedere al clasificării, imaginile digitale sunt : de tip binar, alb-negru şi color. Indiferent de tipul imaginii acestea prezintă diferite proprietăţi ce permit o dimensionare a acestora în funcţie de aplicaţia ce urmează a fi executată şi în funcţie de capacitatea mesajului ce urmează a fi încorporat. Din acest motiv se poate spune că îndeplinesc una din cerinţele importante ale steganografiei şi anume, ascunderea unei cantităţi cât mai mare de informaţie. Totodată, în cazul în care se doreşte o creştere a robusteţii mesajului ascuns, imaginile digitale prezintă o flexibilitate în ceea ce priveşte poziţia în care este plasat mesajul, respectiv introducerea unor date redundante pentru a spori gradul de detecţie şi corecţie a erorilor pe durata transmiterii mesajului steganografic.

O altă caracteristică a imaginilor digitale constă în faptul că mesajul încorporat este greu de detectat vizual, în special dacă algoritmul steganografic ales nu degradează în mod sensibil obiectul de acoperire folosit ca purtător de mesaj secret.

Imaginile alese ca şi obiecte de acoperire în vederea ascunderii unor informaţii secrete trebuie să nu fie comune şi cunoscute. Astfel de imagini nu sunt recomandate a fi folosite, deoarece pot fi uşor comparate cu imaginea de acoperire aleasă pentru procesul steganografic. După o simplă verificare a mărimii imaginii pot apărea suspiciuni. Imaginile alese cu succes ca şi obiecte de acoperire sunt cele cu multe detalii, care nu conţin porţiuni mari cu aceeaşi culoare şi dacă se poate să fie cât mai noi, spre exemplu, imagini capturate în cea mai recentă vacanţă. Este important să se ţină cont de faptul că în cazul în care este schimbat un bit într-o imagine, aceasta poate însemna trecerea de la o nuanţă de roşu la o cu totul altă nuanţă de roşu. O astfel de schimbare ar fi imediat observată în imaginea afişată. Se recomandă schimbări graduale ale tonurilor de culoare, în acest fel crescând posibilităţile imaginii în sensul ascunderii de informaţii secrete. Aşadar, după ce s-a stabilit imaginea folosită ca şi obiect de acoperire este necesar sa se aleagă şi o tehnică sau un algoritm de ascundere a datelor.

În literatura de specialitate [BAR98], [CHU01], [PIY04] se constată că frecvent imaginile digitale sunt utilizate ca obiecte de acoperire. Din punctul de vedere al algoritmilor steganografici utilizaţi se constată că aceştia sunt axaţi în general pe una dintre caracteristicile steganografiei, cum ar fi: robusteţea mesajului ascuns, dificultatea de detecţie a acestuia, vizibilitatea obiectului steganografic şi mai rar pe cantitatea de informaţii ce poate fi ascunsă. În funcţie de tehnica sau algoritmul utilizat în literatura de specialitate există o varietate mare de soluţii propuse ce urmăresc îmbunătăţirea uneia dintre caracteristicile steganografiei menţionate mai sus. Spre exemplu, în [YUA07] este prezentată o metodă steganografică pentru încorporarea unei imagini alb-negru într-o imagine color, iar pentru a îngreuna posibilitatea detecţiei mesajului secret, autorul din [CHE08a] utilizează un cod Gray pentru încorporarea informaţiei secrete în cei mai puţini semnificativi biţi ai unei imagini utilizată ca şi obiect de acoperire.

Pentru ascunderea unor mesaje de lungime mai mare decât cea permisă prin încorporarea simplă în cei mai puţini semnificativi biţi , în [ZHA07b] este propusă o metodă prin care are loc adăugarea sau scăderea unei valori la valoarea curentă a pixelilor. Practic mesajul este ascuns în planul primar şi secundar al pixelilor existenţi, obţinându-se astfel o eficienţă mai mare a algoritmului de ascundere.

În funcţie de numărul de biţi folosit obiectul steganografic poate deveni granulat la vedere pe măsură ce este încorporată o cantitate mai mare de informaţie. Pentru a rezolva această problemă se aplică tehnici cum ar fi BPCS (Bit-Plane Complexity Segmentation Steganography) în care se recurge la limitarea încorporării informaţiilor secrete în biţii de nivel superior în favoarea încorporării în regiunile cele mai complexe ale imaginii.

În [KAW98] este descrisă o tehnică numită BPCS care profită de această proprietate a sistemului vizual uman. Tehnica presupune divizarea imaginii în regiuni, determinarea complexităţii acestora şi încorporarea datelor secrete în acestea.

Compresia imaginilor reprezintă o soluþie foarte bună în cazul în care se transmit imagini mari. [DOR04] prezintă două tehnici pentru ascunderea informaţiilor folosind compresia JPEG pentru imagini. Cunoscând faptul că anumite tipuri de compresii ale imaginilor conduc la pierderi de informaţii, în [JIA04] este prezentată o metodă steganografică aplicată imaginilor prin care se îmbunătăţeşte robusteţea acestora împotriva compresiei JPEG. În cazul utilizării compresiilor cu pierderi asupra imaginilor în [CHI08] se prezintă o metodă steganografică în care este realizată ascunderea mesajelor secrete, cu recuperarea acestora în condiþii optime.

O altă soluţie pentru compresia imaginilor constă în utilizarea proprietăților transformatei Karhunen Loeve (KLT). O astfel de metodă este considerată a fi optimă din punct de vedere statistic conducând la obţinerea unor rezultate superioare de compactare a energiei medii şi permite totodată decorelarea completă a datelor [EFF03]. În general metoda prezintă avantajul reducerii numărului setului de date ceea ce ar putea conduce la obţinerea unor rezultate într-un timp mai scurt. Această afirmaţie nu este împărtăşită de majoritatea autorilor. Transformata KLT este utilizată în foarte multe domenii, cum ar fi: prelucrări statistice ale semnalelor seismografice, electrocardiografice, în procesarea semnalelor digitale, compresia semnalelor, analiza şi procesarea datelor, dar există posibilitatea de a fi folosite şi în procesul de ascundere a datelor. Această proprietate va fi exploatată în lucrarea de faţă în capitolul 9 pentru generarea unor noi algoritmi steganografici.

Aşadar, tehnicile pentru încorporarea informaţiei secrete într-un obiect de acoperire ce are ca mediu o imagine digitală pot fi dezvoltate corespunzător cu domeniile de reprezentare ale acesteia. În acest sens am conceput diferiţi algoritmi pentru fiecare domeniu în parte: spaţial, frecvenţă, vectorial, algoritmi ce vor fi descrişi în capitolele 7, 8, respectiv 9.

Având în vedere cele menţionate mai sus în ultimii ani m-am axat pe cercetări în domeniul steganografiei [STA07a], [STA07b], [STA07c], [STA08a], [STA08b], [STA09] şi am utilizat ca şi obiect de acoperire, respectiv mesaj ascuns imaginile digitale. Direcţiile de cercetare au urmărit toate cele trei caracteristici principale ale steganografiei: cantitate, detecţie, robusteţe. Trebuie menţionat că în literatura de specialitate nu se specifică sub nici o formă timpul de execuţie al algoritmilor. Din acest motiv am încercat să realizez algoritmi steganografici care să poată fi executaţi într-un timp cât mai scurt în scopul utilizării acestora chiar şi în timp real pentru a putea rula pe microprocesoarele utilizate în telefonia mobilă.

Ca şi o concluzie, pe baza datelor din literatura de specialitate [CHO06], [CHO08], [JAE08], [CAW86], [RAJ05], [SHI93], [STA07c] din punct de vedere teoretic acest mediu de ascundere generează cele mai mari avantaje, ceea ce implică totodată şi dezvoltarea unor algoritmi steganografici cu o complexitate ridicată şi cu un grad mare de prelucrare. Acest ultim aspect în general nu constituie un impediment major avându-se în vedere că în marea majoritate a cazurilor prelucrările steganografice nu implică prelucrări în timp real pentru a obţine imaginea steganografică. În acest caz prin procesul steganografic se poate genera o imagine steganografică robustă, ce presupune rezistenţă la eventuale atacuri, în aşa fel încât informaţia ascunsă nu poate fi distrusă sau modificată. Se poate spune că ascunderea unei informaţii având ca obiect de acoperire o imagine digitală prezintă o serie de avantaje, în special cele legate de cantitatea mare de date ce pot fi ascunse, cât şi de posibilitatea introducerii de informaţii redundante care ar putea fi folosite eventual la detecţia şi corecţia unor erori ce se pot manifesta în procesul de transmitere.

2.8 *Concluzii referitoare la mediile folosite în steganografie*

În capitolul de faţă s-au prezentat cele mai utilizate medii pentru ascunderea informaţiilor secrete în vederea realizării unui proces steganografic. Pentru stabilirea gradului de reuşită a unui astfel de proces sunt luate în considerare cele trei criterii de bază specifice steganografiei, şi anume : cantitatea de informaţii ce poate fi ascunsă (de preferat să fie cât mai mare posibil), dificultatea de detecţie a mesajului secret, respectiv robusteţea mesajului ascuns. Un sistem steganografic poate încorpora unul, două sau toate cele trei criterii în funcţie de scopul şi aplicaţia urmărită. E posibil ca pe lângă cele trei proprietăţi de bază steganografia să mai fie caracterizată si de alţi factori, cum ar fi: confidenţialitate (maximă), vizibilitate (minimă), flexibilitate în alegerea algoritmilor ce pot fi implementaţi în procesul de ascundere.

În steganografia ce foloseºte ca mediu purtãtor un format text algoritmii sunt relativ simpli, posibilitãþile de ascundere reduse, iar interceptarea mesajului permite destul de uºor posibilitatea extragerii informaþiei utile. Þinând cont de metodele de ascundere prezentate, este de remarcat faptul cã sistemele steganografice, care folosesc formatele text pentru a transmite informaþie, ar putea fi uºor distruse prin rescrierea documentelor.

Cu toate acestea se poate considera cã în eventualitatea dezvoltãrii telefoniei mobile, a creºterii ratei de transfer, a îmbinãrii textului cu imagini digitale sau video ºi combinând diferitele metode de ascundere este posibilã generarea unor noi categorii de algoritmi care sã îmbine caracteristicile tuturor tipurilor de medii purtãtoare.

O necesitate importantã de realizat în timpul unui proces steganografic este cantitatea de date ascunsã ºi transmisã în condiþii cât mai bune astfel încât aceasta sã nu fie detectatã ºi chiar distrusã de un posibil atacator. Din acest punct de vedere o mare parte din mediile folosite în steganografie ºi prezentate în acest capitol nu oferã posibilitatea transmiterii unei cantitãþi mari de informaþie secretã. Acest dezavantaj se poate regãsi la aplicarea steganografiei în format text, SMS, HTML, fiºiere executabile, protocoale de reþea. În majoritatea din aceste potenþiale medii purtãtoare, mesajul secret se poate ascunde în zone cu limitãri specifice fiecãrui format în parte, cum ar fi anumite câmpuri, spaþii libere ce pot fi ignorate , însã toate acestea conduc la douã mari dezavantaje, cum ar fi: un grad scãzut de robusteþe, respectiv posibilitatea ascunderii unei cantitãþi mici de informaþie secretã.

Faptul cã majoritatea mediilor amintite anterior permit ca informaþia secretã sã fie ascunsã într-un loc bine stabilit face ca acest gen de ascundere sã prezinte anumite dezavantaje, în sensul cã în realitate nu este realizat un proces steganografic în adevăratul sens, ci doar o mascare a unor informaţii.

Diferite modalităţi de ascundere în ceea ce priveşte steganografia modernă pot fi regăsite cel mai uºor în mediile audio,video şi imagini digitale, iar din acest motiv direcţiile cele mai multe de cercetare se îndreaptă spre cele trei medii menţionate.

Steganografia în audio prezintã dezavantajul cã mesajele ascunse au dimensiuni mai mici deoarece banda de frecvenþã existentã pentru realizarea unui proces steganografic este relativ redusã. În acest fel ºi posibilitãþile de detecþie pot avea ºanse mai mari de reuºitã, deoarece domeniul de cãutare este mai restrâns. Sunetul poate fi captat mai uşor prin aparatură mai puţin sofisticată, mai ieftină ce se poate procura de mai multe persoane, deci există riscul unor interceptări cu probabilitate mai mare, chiar de un atacator pasiv (nu răuvoitor).

Obiectele video digitale au avantajele imaginilor digitale, dar prezintă şi un mare dezavantaj, dată fiind cantitatea mare de informaţii ce se transmit, necesită în mod obligatoriu folosirea unor metode de compactare, cum ar fi MPEG (Moving Picture Expert Group) care poate asigura o rată de compactare de 1/200. Datorită faptului că nu toate cadrele se compactează la fel mesajul ar putea fi distrus în urma acestui proces. În general la imaginile video digitale se execută mai multe tipuri de compactări. La recepţie practic imaginea video se reface din datele ce s-au recepţionat, ceea ce face dificilă găsirea unor metode adecvate de ascundere. Un exemplu în acest sens este imaginea video transmisă pe Internet care şi în condiţiile fără ascundere este de proastă calitate.

Imaginile digitale ca mediu purtător prezintă în primul rând posibilitatea ascunderii unei capacităţi mari de informaţie, datorită faptului că aceasta poate fi dispersată cu ajutorul unor algoritmi implementaţi în toată imaginea corespunzătoare obiectului de acoperire şi nu doar într-un anumit loc disponibil ca şi la celelalte medii.

O a doua proprietate importantă a imaginilor digitale o constituie faptul că detecţia informaţiei ascunse se face cu şansă mai mică de reuşită şi aceasta se întâmplă numai dacă obiectul steganografic la care are acces un atacator poate fi analizat cu un sistem de calcul care să conţină algoritmi de detecţie.

Din punct de vedere al robusteţii, imaginile digitale se caracterizează printr-o probabilitate maximă ca atunci când mesajul este ascuns şi emis într-un mediu printr-un canal de transmitere să poată fi recuperat cât mai fidel de către receptor.

Pentru a realiza procese steganografice în care obiectele de acoperire sunt imagini digitale se pot imagina diferite metode de ascundere ce utilizează algoritmi în vederea creşterii gradului de robusteţe şi siguranţă a informaţiilor transmise astfel.

Se apreciază că din punct de vedere teoretic, gradul de ascundere exprimat procentual în imagini digitale poate atinge valori de până la 100% cu condiţia de a utiliza algoritmi de procesare steganografică performanţi şi o imagine purtătoare care să permită un grad mare de ascundere fără degradarea vizibilă a imaginii iniţiale.

În figura 2.1 se prezintă în sinteză diferitele caracteristici ale mediilor purtătoare de informaţii în care se pot ascunde date. Se poate constata că atât imaginile digitale, cât şi imaginile video îndeplinesc toate cele trei criterii de bază ce caracterizează mediile de ascundere. Imaginile video din punct de vedere tehnic pot fi tratate ca imagini digitale, ceea ce implică utilizarea aceloraşi tehnici.

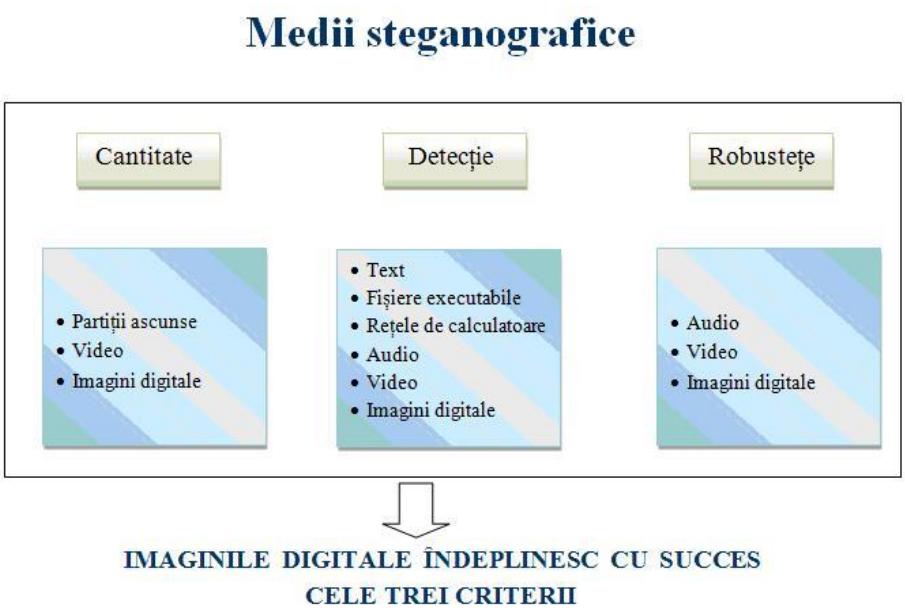


Figura 2.1 Medii steganografice - Caracteristici de bază

În urma celor prezentate se poate desprinde concluzia că imaginile digitale, sub diferite forme: alb negru sau color permit ascunderea unor cantităţi mari de informaţii, cu un grad mare de robusteţe şi dificultate sporită în observarea informaţiilor ascunse. În schimb, gradul de vizibilitate al mesajelor ascunse este scăzut. Toate aceste caracteristici sunt posibile datorită aplicării unor algoritmi steganografici specifici, ceea ce a condus la îndreptarea eforturilor mele spre acest mediu steganografic. Din acest motiv consider că un candidat important ce ar putea fi folosit ca obiect de acoperire în studiul realizării unui proces steganografic este imaginea digitală. Pentru a o mai bună înţelegere a modului în care un mesaj secret se poate ascunde într-o imagine oarecare se va prezenta în continuare o descriere

mai în amănunt a imaginilor digitale.

3 IMAGINI DIGITALE UTILIZATE ÎN STEGANOGRAFIE

3.1 *Descrierea imaginilor digitale*

Lumea înconjurătoare este formată din imagini ce pot fi regăsite prin aproape orice mijloc de comunicare. Pentru ca o imagine reală vizualizată de o persoana să fie transmisă şi altei persoane trebuie ca aceasta să treacă printr-un proces de digitizare astfel încât aceasta să devină o imagine digitală. Imaginile astfel transformate pot fi utilizate în calculatoare, camere digitale, video, scanere, telefonie celulară, etc.

Datorită dezvoltării fără precedent în domeniul hard şi soft în prezent orice amator poate manipula o imagine digitală sau video la fel de simplu ca un profesionist. Indiferent de domeniul de aplicaţie şi de tipul acesteia color sau alb negru, imaginea digitală este constituită dintr-un element de bază numit pixel.

În mod practic fiecare imagine digitală este formată dintr-un număr fix de linii şi coloane de pixeli formând astfel o matrice de $M \times N$ pixeli, dar care luaţi ca atare nu pot fi percepuţi de ochiul uman. Un pixel este caracterizat printr-unul sau mai multe canale de culoare, cu valori cuprinse între 0 şi 255. Fiecare valoare în parte reprezintă luminozitatea pixel-ului respectiv. In acest sens, imaginea digitală este un vector de numere ce reprezintă intensitatea luminii în diferite puncte sau pixeli. Din acest punct de vedere, imaginile sunt de trei tipuri: binare, alb-negru şi color.

3.2 *Stocarea imaginilor digitale*

În principiu pixelii regăsiţi într-o imagine sunt doar înşiruiri de numere, iar memorarea lor în mod teoretic poate fi realizată prin notarea şirului de numere pe o hârtie. Această metodă prezintă un dezavantaj important deoarece necesită stocarea unei cantităţi mari de informaţii datorită lungimii mari a şirului de numere. Pentru a ocupa mai puţin spaţiu în memoria calculatorului, imaginile digitale pot fi atât stocate cât şi transmise sub forme comprimate urmând a fi decomprimate la destinaţie.

În acest sens, culoarea fiecărui pixel regăsit într-o imagine este stocată printr-un număr (pentru imaginile monocrome, aşa zise imagini alb-negru) sau 3 numere pentru formatele color (câte un număr pentru fiecare culoare primară: roşu, verde şi albastru). Numerele care se folosesc pentru stocarea culorilor sunt reprezentate uzual pe 8 biţi, ceea ce oferă imaginilor alb-negru o plajă de 256 de culori (2^8 culori), iar celor color de 16 milioane de culori (2^{24} culori).

Numărul de pixeli dintr-o imagine este dat de rezoluţia imaginii (numărul de pixeli pe verticală şi orizontală) şi determină direct: claritatea imaginii (cu cât

numărul de pixeli e mai mare, cu atât imaginea va fi mai clară), respectiv dimensiunea fişierului în care imaginea va fi stocată. Stocarea imaginilor în formă iniţială (fără a comprima informaţia în nici un fel) necesită o cantitate mare de spaţiu de stocare, ceea ce conduce în mod evident la tendinţa reducerii acestei dimensiuni cât mai mult posibil, fără a se pierde prea mult din calitatea imaginii

Pentru rezolvarea acestor probleme se aplică diferite metode de compresie asupra imaginilor digitale, ce se împart la rândul lor în două mari categorii [HOG06, JAI89]

- fără pierdere de informaţie - compresia imaginii este relativ mică, dar imaginea nu pierde deloc din calitate. Acest tip de compresie se pretează atunci când se doreşte păstrarea calităţii imaginii, mai mult decât a spaţiului pe care aceasta îl ocupă.

- cu pierdere de informaţie - compresia imaginii este mare (ex: 10-15 ori mai mică pentru o compresie normală JPEG), dar imaginea astfel prelucrată pierde din informaţia originală şi implicit din calitate.

Cele mai multe metode de compresie permit o selectare a compresiei dorite, în funcţie de priorităţile aplicaţiei: dimensiunea informaţiei sau calitatea imaginii. Formatele care folosesc compresia cu pierdere de informaţie duc în mod evident la o degradare progresivă a imaginii în urma procesului de prelucrare. Aceasta se întâmplă deoarece la deschiderea unui fişier astfel comprimat, informaţia din el este convertită în matrice de pixeli (aşa cum a fost imaginea originală) pentru a putea fi afişată. Dacă fişierul este resalvat, compresia se va aplica din nou. În schimb, formatele cu compresie fără pierdere de informaţie nu prezintă astfel de probleme, deoarece în aceste cazuri se pune accent pe păstrarea calităţii imaginii (din acest motiv aceste tipuri de compresii sunt mai des utilizate la prelucrarea de imagini sau în fotografia profesionistă).

3.3 *Generarea imaginilor digitale*

Orice obiect în spaţiu poate fi caracterizat prin intermediul a trei axe de coordonate notate de obicei cu (X, Y, Z) [HOG06, JAI89]. Cele trei dimensiuni reprezintă lungimea, lăţimea şi adâncimea sau înălţimea obiectului astfel exprimat. Pentru a transforma o imagine reală într-una digitală este necesară achiziţia imaginii sub formă tridimensională exprimată într-un sistem de coordonate (X, Y, Z). Aceasta se realizează prin proiecţia imaginii captate într-un plan având un sistem de coordonate (x, y) reprezentată în figura 3.1. şi descrisă de ecuaţiile următoare:

$$y = -f\frac{y}{z} \quad \text{şi} \quad x = -f\frac{x}{z} \tag{3.1}$$

f poartă numele de distanţă focală şi Z este axa optică.

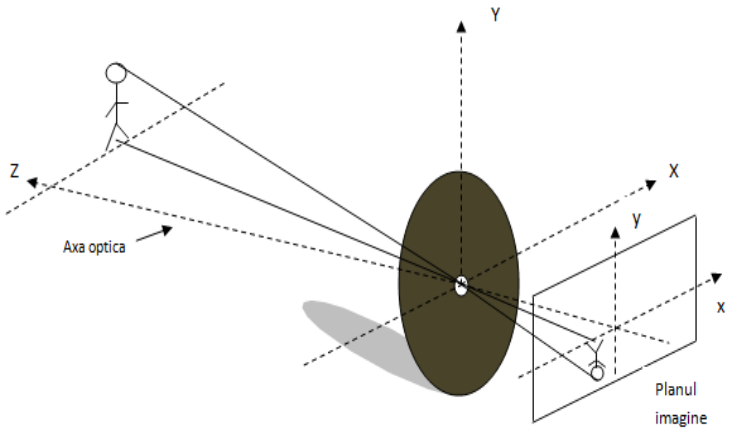


Figura 3.1. Proiecţia imaginii captată într-un plan de coordonate (x, y)

În acest mod imaginea în spaţiu 3D devine plană şi este exprimată în spaţiul 2D. Imaginea astfel rezultată este la rândul ei captată de senzori dispuşi într-un plan 2D notat în general cu (u, v). Aşadar, imaginea reală, originală este transpusă într-o imagine plană datorită dispunerii senzorilor pe o suprafaţă plană. Senzorii sunt practic dispuşi pe două axe de coordonate u şi v, iar pe fiecare axă pot fi regăsiţi un număr de n senzori.

Pentru a putea vizualiza şi prelucra imagini în calculator acestea trebuiesc digitalizate, adică împărţite în elemente de dimensiuni foarte mici numite pixeli. Fiecare pixel este practic un eşantion extras din imaginea iniţială. Cu cât este mai mare numărul de pixeli cu atât imaginea va fi mai aproape de cea reală. Pixelii sunt codificaţi la rândul lor în parte, primind fiecare câte o valoare binară exprimată zecimal. De exemplu, dacă un pixel este reprezentat pe 8 biţi, valoarea acestuia este cuprinsă între 0 şi (2^8 – 1), respectiv 255. Convenţia general adoptată este faptul că valoarea cea mai mică ”0” pe care o poate lua un pixel exprimă culoarea negru, iar valoarea cea mai mare 255 reprezintă culoarea alb. Intensitatea luminoasă a unei imagini este transpusă prin codificare binară în valori binare în funcţie de rezoluţia acesteia care reprezintă de fapt numărul de biţi prin care fiecare pixel din imagine este codificat.

Pentru a converti imaginea captată într-o imagine digitală urmează procese de eşantionare spaţială, respectiv de eşantionare temporală a imaginii [GUI99, JAI89]. Prin eşantionare spaţială imaginea plană este descompusă într-o matrice de pixeli de M linii şi N coloane. Fiecare element al matricii reprezintă un pixel, iar fiecare pixel este cuantificat în urma procesului de eşantionare în valori cuprinse între 0 şi 256, dacă rezoluţia imaginii este pe 8 biţi.

Imaginile pot fi reprezentate în diferite moduri în funcţie de necesitatea aplicaţiilor care le utilizează. În acest fel se pot regăsi imagini binare, alb-negru sau color.

3.4 *Imagini binare*

Imaginile binare sunt semnale discrete, bidimensionale şi datorită reprezentării lor foarte simple, sunt folosite doar în câteva aplicaţii ce pot fi întâlnite în practică sub formă de pagini tipărite, scrisori, documente, ziare, hărţi geografice, hărţi meteorologice, etc. De asemenea pot fi regăsite la rezultatele obţinute în urma utilizării imprimantelor. Transmisia şi stocarea imaginilor binare poate fi întâlnită în diverse domenii de activitate, cum ar fi: transmisia prin fax sau baze de date de amprente utilizate în criminalistică.

Intensitatea unei imagini binare este exprimată doar prin două valori, alb sau negru ale fiecărui pixel component. Pentru a stoca o imagine binară este necesar un volum mare de memorie şi din acest motiv sunt binevenite aplicarea metodelor de compresie ce reduc practic timpul de transmisie, lărgimea de bandă necesară transmisiei şi necesarul de capacitate de stocare.

Cele două valori, alb sau negru sunt reprezentate prin utilizarea unui singur bit (0/1) pentru fiecare pixel. Ca atare imaginea binară conţine şiruri de 0 şi 1 în funcţie de modul cum sunt distribuiţi pixelii albi şi negri. În funcţie de imaginea reprezentată, şirul poate fi constituit dintr-un număr variabil de 0, urmat de un număr oarecare de 1. Din acest motiv, imaginile binare pot deveni susceptibile în cazul aplicării unei metode de substituţie unor astfel de pixeli redundanţi ceea ce conferă unor astfel de imagini un grad scăzut de robusteţe.

Un mod de ascundere a unui mesaj secret într-o imagine binarã a fost prezentat în [KOC95]. În lucrare informaþia secretã este încorporatã în pixelii ai cãror vecini au culoarea opusã.

În imaginile binare în care există diferenţe mari de contrast, modificările se fac la graniţa dintre pixelii albi şi negrii. În vederea creşterii robusteţii se apelează la adaptarea procesului de încorporare în funcţie de diferiţi parametrii ce specifică procentajul de pixeli ce îşi pot schimba culoarea.

Matsui si Tanaka prezintã în [MAT94] o altã metodã de ascundere ce utilizeazã un sistem de comprimare fãrã pierderi folosit pentru a codifica informaþia. Tehnicile aplicate þin cont de faptul cã în imaginile binare existã o probabilitate mare ca pixelii succesivi sã aibã aceeaºi culoare, astfel cã în aceste cazuri nu este codificatã culoarea fiecãrui pixel în mod explicit, ci poziþiile schimbãrilor de culoare împreunã cu numãrul de pixeli succesivi de aceeaºi culoare.

3.5 *Imaginea alb-negru*

Componentele unei imagini alb – negru sunt reprezentate printr-un singur canal de culoare ce reprezintă practic intensitatea, luminanţa sau densitatea imaginii. Fiecare pixel este reprezentat pe 8 biţi (1 byte) şi astfel poate lua valori între 0 şi $2^8 - 1$, respectiv (0, 255). Valoarea 0 reprezintă intensitatea luminoasă minimă, respectiv cea mai închisă culoare (negru), iar 255 intensitatea luminoasă maximă, adică cea mai deschisă culoare (alb).

[YUC06] propune o metodă pentru ascunderea imaginilor alb-negru ce permite diferitor utilizatori să poată extrage imagini secrete în funcţie de cheia

secretă pe care ei o cunosc. Pentru a reduce dimensiunea informaţiilor ce urmează a fi încorporate, fiecare dintre imaginile secrete este mai întâi comprimată după care este ascunsă.

Pentru aplicaţiile profesionale, cum ar fi: poze artistice din diferite domenii, imaginea alb – negru nu este foarte sugestivă. Ca atare, utilizatorul apelează la altă reprezentare a imaginii în care fiecare pixel este exprimat pe mai mult de 8 biţi, cum ar fi spre exemplu utilizarea imaginilor color.

3.6 *Imagini color*

Datorită faptului că imaginile color au cel mai mare impact vizual asupra ochiului uman sunt şi cele mai utilizate în aplicaţiile profesionale, cum ar fi televiziune, foto, imprimare, etc. Fenomenul de percepţie a culorilor este complex şi foarte interesant în acelaşi timp şi din acest motiv, de sute de ani a fost o ţintă de cercetare a oamenilor de ştiinţă, psihologilor, filozofilor, artiştilor. Pentru a putea lucra cu imaginile digitale color este necesar ca utilizatorii să aibă cunoştinţe despre diferitele tehnici şi aspecte mai importante în ceea ce priveşte reprezentarea acestora.

O imagine color necesită, spre deosebire de una alb-negru, trei octeţi pentru fiecare pixel. Percepţia culorii este foarte importantă pentru oameni şi depinde în principal de caracteristicile luminii şi de procesul complex ce are loc între creier şi ochi. Astfel, oamenii folosesc informaţia de culoare pentru a distinge mai bine obiectele, în mod practic, aceasta ajută la stabilirea unor detalii, contururile fiind practic aceleaşi. În imaginile color fiecare pixel este exprimat prin combinarea a trei culori de bază numite culori primare RGB.

Imaginile color reprezintă un suport atractiv pentru a fi utilizate în steganografie şi permit încorporarea unei cantităţi mari de informaţii, cum se sugerează în [CHO08] în care se propune introducerea în mod dinamic a datelor secrete în culoarea albastră a imaginilor RGB şi YUV, deoarece aceasta este insensibilă ochiului uman. În plus sunt luate o serie de măsuri steganalitice în vederea protejării datelor ascunse.

În [PIY04] se prezintă o metodă de încorporare a unei imagini color bazată pe tehnici de cuantizare în vederea protejării dreptului de autor. Rezultatele obţinute permit utilizarea algoritmului şi în alte aplicaţii multimedia ce se bazează pe tehnica de cuantizare a imaginilor color.

O altă aplicaţie steganografică ce utilizează imaginile color ca şi suport de ascundere se prezintă în [CHO06]. Scopul lucrării constă în încorporarea unei cantităţi cât mai mare de informaţie menţinând calitatea obiectului steganografic rezultat. Acest lucru se realizează prin manipularea imaginilor color în domeniul spaţial şi inserarea datelor secrete în bitul cel mai puţin semnificativ al imaginii suport. De asemenea se iau în considerare efectul vizual al ochiului uman. Metoda propusă permite ascunderea unei cantităţi de informaţie egală cu 60% din capacitatea obiectului de acoperire.

3.7 *Concluzii*

Imaginile digitale ca mediu purtător a unui mesaj secret constituie cea mai bună soluţie pentru a genera un obiect steganografic. Este mediul ce permite ascunderea celor mai mari cantităţi de informaţie fără a genera suspiciuni că ar conţine un mesaj secret.

Proprietatea de bază pe care se bazează steganografia utilizând imaginile digitale ca mediu steganografic constă în caracteristicile ochiului uman, ce are tendinţa de a integra informaţia primită. Din acest motiv, ochiul uman nu poate desluşi aspectele legate de detaliile foarte fine. Chiar în situaţiile în care ar putea să facă distincţie de faptul că imaginea nu este foarte clară este nevoie de o referinţă (imaginea originală) pe care în schimb nu are cum să o deţină. Tocmai pe acest principiu se bazează steganografia, şi anume faptul că atacatorul nu cunoaşte imaginea purtătoare, nu cunoaşte metoda de ascundere (algoritmul), nu cunoaşte ce procesări s-au făcut asupra mesajului iniţial şi nu are cunoştinţă de eventualele metode de secretizare introduse. Pentru a parcurge toate etapele menţionate mai sus este necesară o putere de calcul semnificativă şi timp suficient pentru a ajunge la mesajul ascuns.

Având în vedere caracteristicile imaginilor digitale menţionate mai sus, am ales ca principala mea direcţie de cercetare să fie utilizarea acestora ca suport de bază pentru dezvoltarea unor noi sisteme steganografice. Algoritmii steganografici dezvoltaţi de mine au tendinţa de a exploata toate caracteristicile imaginilor digitale reprezentate în domeniul spaţial, frecvenţă, respectiv vectorial. Încercările multiple de a crea şi adapta algoritmi în cele trei domenii de reprezentare a imaginilor digitale au avut drept scop identificarea acelui algoritm care se pretează cel mai bine pentru a fi implementat pe un microprocesor utilizat în telefonia mobilă, cunoscând faptul că astfel de aplicaţii implică furnizarea mesajului într-un timp cât mai scurt.

4 DOMENII DE REPREZENTARE ALE IMAGINILOR DIGITALE

Pentru a aduce spaţiul culorilor mai aproape de ochiul uman au fost generate sisteme de reprezentare a imaginilor în trei mari domenii, şi anume: *spaţial, frecvenţă*, *vectorial.*

Domeniul spaţial constituie rezultanta firească a exprimării imaginii rezultate în urma eşantionării spaţiale a acesteia în care fiecare culoare a unui pixel este reprezentată într-un sistem de 3 coordonate color. Fiecare culoare reprezintă o axă a sistemului de coordonate ce este cunoscut sub denumirea de domeniu spaţial. Acesta poate fi reprezentat în diferite forme geometrice, dintre care cele mai cunoscute sunt cele cubice şi piramidale.

Domeniul frecvenţă se bazează pe descompunerea semnalelor asociate imaginilor digitale într-o sumă de armonici având ca bază de plecare transformata Fourier (FT). Fiecare pixel a unei imagini la rândul lui poate să fie exprimat sub forma unui vector de o anumită valoare, ceea ce face ca orice imagine să poată fi exprimată şi vectorial, într-un domeniu corespunzător.

4.1 *Domeniul spaţial*

4.1.1 Domeniul spaţial – RGB

Imaginea color RGB este una dintre cele mai utilizate reprezentări. Pixelii componenţi ai unei astfel de imagini sunt codaţi după o schemă ce constă în combinarea a trei culori primare: roşu (R), verde (G) şi albastru (B) pentru fiecare pixel în parte. Cele trei culori sunt folosite pentru reprezentarea, memorarea şi transmiterea imaginii color fie sub formă analogică pentru a fi utilizată în televiziune, fie sub formă numerică pentru a fi utilizată în calculatoare, camere digitale, imprimante, scanere. Datorită aplicaţiilor vaste, reprezentarea RGB este des întâlnită în procesări de imagini, programe grafice, biblioteci ce includ astfel de procesări, etc.

Realizarea diferitelor culori într-o imagine necesită modificarea intensităţii fiecărui pixel component. RGB este un sistem color aditiv, ceea ce înseamnă că toate culorile pornesc de la una singură, cum ar fi negru, iar diferitele nuanţe se creează prin adăugarea de culori primare. Fiecare pixel captează o anumită rază de lumină ce poate fi roşie, verde, albastră, iar pentru crearea diferitelor culori trebuie modificată intensitatea fiecăreia din cele trei culori în mod independent. Astfel că, intensităţile diferite a fiecărei culori primare controlează nuanţa şi luminozitatea culorii realizate. Pe monitoarele calculatoarelor sau ecranului TV color pot fi vizualizate imagini create prin executarea unor operaţii ce presupun mixarea celor trei culori primare la intensităţi diferite. Astfel pot fi create culorile alb şi gri, iar punctele roşu, verde şi albastru sunt stimulate simultan de către radiaţiile de electroni la nivele de energie diferită (intensităţi) formând astfel o imagine color

continuă. Este cunoscut faptul că ochiul uman este astfel conceput încât integrează culorile. Spre exemplu, dacă într-o imagine există 10 pixeli vecini de culoare verde deschis şi în interiorul lor există intercalat un pixel alb, practic acesta va fi nesesizat. Pentru a exprima rezultanta culorilor formate s-a generat aşa numitul sistem a imaginii color RGB [HOG06, GUI99, JAI89]. Spaţiul RGB color poate fi vizualizat sub forma a trei dimensiuni ce reprezintă un cub în care cele trei culori primare formează cele trei axe de coordonate şi este cunoscut sub denumirea de *domeniu spaţial RGB.*

O culoare formată C poate fi exprimată în funcţie de ponderile celor trei culori primare, notate cu p_1, p_2, p_3 după următoarea relaţie matematică:

$$C = p_1 \times R + p_2 \times G + p_3 \times B \quad (4.1)$$

Ponderile pot fi exprimate ca numere subunitare, procente sau numere întregi cuprinse în intervalul [0,255] în cazul în care o culoare este codificată pe 8 biţi. Valorile celor trei culori primare RGB sunt pozitive şi sunt cuprinse în intervalul $[0, c_{max}]$, unde $c_{max} = 255 = 2^8 - 1$ şi sunt reprezentate în figura 4.1. Fiecare culoare posibilă c_i corespunde unui punct în cubul RGB şi poate fi exprimată astfel:

$$c_i = (R_i, G_i, B_i) \quad ; \quad 0 \leq R_i, G_i, B_i \leq c_{max} \quad (4.2)$$

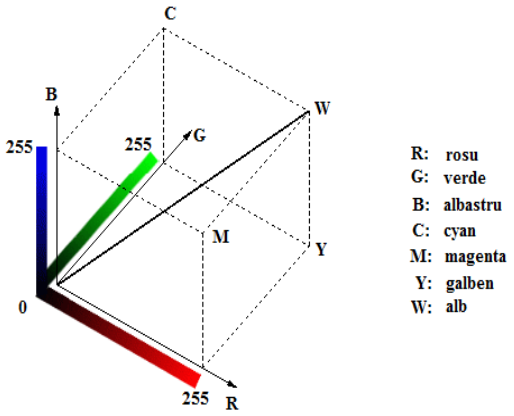


Figura 4.1 Distribuţia culorilor în domeniul spaţial RGB [JAI89].

Deoarece de cele mai multe ori valorile RGB sunt normalizate în intervalul [0,1] pot fi vizualizate sub forma unui cub unitar, ca în figura 4.1. Punctul din originea sistemului de coordonate astfel format în care R=G=B=0 reprezintă culoarea negru, în timp ce punctul opus acestuia R=G=B=1 reprezintă culoarea alb. Segmentul ce leagă cele două puncte reprezintă diferite nivele de gri formate din egalarea culorilor R=G=B.

Fiecare pixel dintr-o imagine color poate fi reprezentat printr-o culoare anume rezultată din combinarea culorilor de bază în diferite proporţii. Pentru a obţine rezultate cât mai profesionale în care imaginea constituită să fie cât mai apropiată de imaginea reală este indicat ca diferenţele dintre culorile folosite să fie cât mai mici. În acest sens se ţine cont de ordonarea componentelor unei imagini color şi ordinea de împachetare a acestora.

O imagine $I = (I_R, I_G, I_B)$ poate fi alcătuită dintr-un grup de imagini I_R, I_G, I_B reprezentat ca în figura 4.2

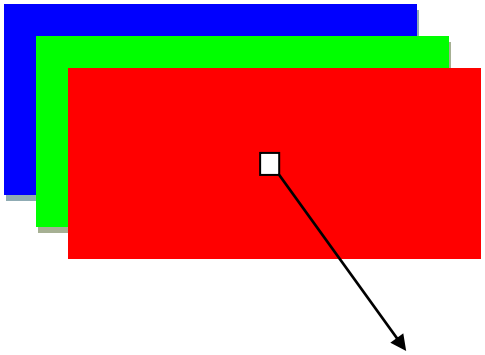


Figura 4.2. Grup de imagini I_R, I_G, I_B

Astfel că, valoarea unei componente de culoare RGB a imaginii în funcţie de poziţia în planul senzorilor (u, v) se obţine prin accesarea celor 3 imagini în felul următor:

$$\begin{bmatrix} R \\ G \\ B \end{bmatrix} = \begin{bmatrix} I_R(u,v) \\ I_G(u,v) \\ I_B(u,v) \end{bmatrix} \quad (4.3)$$

Ordinea de împachetare pentru fiecare valoare RGB a unei imagini $I(u,v) = (R, G, B)$ se obţine accesând individual componentele pixelilor color în felul următor :

$$\begin{bmatrix} R \\ G \\ B \end{bmatrix} = \begin{bmatrix} Red(I(u,v)) \\ Green(I(u,v)) \\ Blue(I(u,v)) \end{bmatrix} \quad (4.4)$$

$$I(u,v) = (I\downarrow R\ (u,v), I\downarrow G\ (u,v\ ), I\downarrow B\ (u,v)) \quad (4.5)$$

Sistemul de culori RGB este utilizat, programat, manipulat pe diferite dispozitive hardware. În cazul în care este modificată o culoare în spaţiul RGB este important de remarcat faptul că metrica sau măsura distanţei în acest spaţiu al culorii nu este proporţională cu percepţia ochiului uman asupra respectivei culori. Modificarea diferitelor culori a unui punct dintr-un spaţiu de culoare în aceeaşi cantitate poate cauza modificări sesizabile în imagine. În plus, schimbarea luminozităţii în spaţiul de culoare RGB este percepută ca o transformare neliniară. Deoarece orice modificare a unei coordonate modifică tonul culorii, saturarea şi strălucirea corespunzătoare acesteia, face ca selectarea spaţiului culorii RGB să fie un proces destul de dificil şi neintuitiv. S-a constatat în urma efectuării mai multor experimente că ochiul uman este mai sensibil la intensitatea luminoasă a culorii decât la nuanţă. Pornind de la această observaţie s-a dezvoltat o altă modalitate de reprezentare a culorilor cunoscută sub numele YUV.

Domeniul spaţial stă la bază multor algoritmi implementaţi pentru ascunderea datelor secrete. [JAE08] propune o metoda steganografică bazată pe imagini, care este un fel de tehnică a domeniului spaţial. Astfel, pentru a ascunde datele secrete în imaginea de acoperire, se foloseşte tehnica diferenţelor notabile şi metoda senzitivităţii funcţiei de contrast.

4.1.2 Domeniul spaţial – YUV

YUV este un spaţiu de culoare ce codifică o imagine colorată ţinând seama de percepţia umană, care permite reducerea lăţimii de bandă pentru componentele cromatice şi permite transmiterea de erori mai eficient mascate de percepţia umană decât cu ajutorul unei simple reprezentări RGB [JAI89].În acest caz, fiecărui pixel dintr-o imagine reprezentată într-un spaţiu RGB i se aplică o funcţie pentru a face trecerea în spaţiul YUV. La această nouă reprezentare se utilizează în locul celor trei componente primare R,G,B alte trei mărimi derivate din acestea şi anume:

$$\begin{aligned} Y &= 0.30R + 0.59G + 0.11B \\ U &= R - Y = 0.70R - 0.59G - 0.11B \\ V &= B - Y = -0.30R - 0.59G - 0.89B \end{aligned} \tag{4.6}$$

Astfel, fiecare culoare exprimată în domeniul spaţial YUV are intensitatea luminoasă definită prin componenta Y întâlnită şi sub numele de luminanţă, iar coeficienţii 0.30, 0.59 si 0.11 reprezintă strălucirile relative la alb ale celor trei culori primare roşu, verde şi albastru. Celelalte două componente U şi V definesc nuanţa culorii şi sunt denumite componente de crominanţă. Ele sunt date de diferenţa dintre componenta roşie, respectiv albastră şi cea de luminanţă.

Reprezentarea imaginilor în spaţiul YUV are ca utilizare practică domeniul televiziunii în culori ca urmare a compatibilităţii cu televiziunea alb-negru ce a fost utilizată deja pe scară largă. YUV este utilizat pentru codificarea culorilor în sisteme analogice, cum ar fi: PAL (Phase Alternate Line) şi NTSC (National Television System Committee). Avantajul principal al unei astfel de reprezentări îl constituie separarea componentei de luminanţă pentru care ochiul este foarte sensibil la detalii de componentele de nuanţă pentru care sensibilitatea este mai redusă. Aceasta permite în cazul televiziunii în culori să aplice diferite compresii ce duc la limitarea benzii de frecvenţă alocată semnalelor de crominanţă.

Metodele de ascundere a datelor secrete pot fi aplicate atât sistemelor color RGB, cât şi YUV. [CHO08] propune o metodă de încorporare a unei cantităţi relative mari de date pentru imaginile color. Aceasta presupune să fie modificată valoarea albastră a pixelilor cu scopul de a ascunde datele secrete, deoarece valoarea albastră este o culoare insensibilă pentru ochiul uman.

4.1.3 Alte domenii spaţiale

Ca urmare, selecţia culorii este mai intuitivă în alte spaţii de culoare cum ar fi spaţiul HSV (hue, saturation, value) deoarece din punct de vedere perceptual una din caracteristicile culorii, respectiv saturarea poate fi reprezentată individual şi totodată poate fi şi modificată individual [JAI89].

Din punctul de vedere al capacităţii de percepere a detaliilor, s-a constat, în urma diferitelor experimente făcute de-a lungul timpului că, ochiul uman este mai sensibil la intensitatea luminoasă a culorii decât la nuanţă. Reprezentarea culorilor în spaţiu RGB ţine seama mai mult de modalităţile tehnice de captare şi reproducere a imaginii, decât de mecanismul fiziologic de percepere a culorii, ca atare un vector în spaţiul RGB descrie intensitatea luminoasă a celor trei culori primare folosite.

Din această cauză, s-a apelat la o altă modalitate de reprezentare a culorilor care să ţină cont de această observaţie. În acest sens, se descrie un alt spaţiu, cunoscut sub numele de YC_bC_r ce se distinge între luminozitatea Y şi alte două componente cromatice C_b ,C_r . Astfel, Y reflectă strălucirea culorii, iar C_b si C_r realizează distincţia între gradele culorii. Un vector culoare în RGB poate fi convertit în vector YC_bC_r folosind următoarea transformată [KAT00]:

$$Y = 0.299R + 0.587G + 0.114B \tag{4.7}$$

$$C_b = 0.5 + \frac{(B - Y)}{2}$$

$$C_r = 0.5 + \frac{(R - Y)}{1.6}$$

Alternativele la spaţiul culorilor RGB sunt la rândul lor folosite în diferite aplicaţii. Un exemplu ar fi, separarea automată a obiectelor din planurile îndepărtate (blue box tehnic in TV) sau codificarea semnalelor TV pentru transmisie sau imprimare. Aşadar, distribuţia culorilor unei imagini poate fi reprezentată în spaţii de culoare diferite, acestea urmând a fi alese în funcţie de cerinţele aplicaţiei aflate în lucru. Cele mai des utilizate domenii spaţiale de culoare sunt: RGB, HSV, HLS, YUV.

În [LIU08] sunt prezentate câteva domenii spaţiale de culoare derivate din domeniul spaţiul de culoar RGB ce sunt utilizate pentru recunoaşterea facială, cum ar fi: domeniul spaţial de culoare necorelat (UCS), domeniul spaţial de culoare independent (ICS) şi domeniul spaţial culoare discriminator (DCS).

Pentru a se face trecerea dintr-un spaţiu de culoare în altul există metode specifice de conversie ce pot fi regăsite în literatura de specialitate. [JAI89]

În concluzie, au fost generate diferite sisteme color reprezentate în domeniul spaţial pentru a reprezenta culorile într-un mod mai prietenos faţă de ochiul uman. Sistemul imaginilor color RGB prezintă avantajul că reprezentarea culorilor în spaţiu RGB ţine seama mai mult de modalităţile tehnice de captare şi reproducere a imaginii, în schimb are dezavantajul că nu ţine cont de mecanismul fiziologic de percepere a culorii de către ochiul uman şi de faptul că mărimea sau valoarea fiecărei culori de bază nu exprimă întotdeauna şi culoarea reală, percepută de către ochiul uman. De exemplu, o creştere semnificativă a valorii unei culori primare nu conduce întotdeauna şi la o modificare semnificativă a culorii. Din acest motiv au fost create şi alte sisteme de reprezentare a culorilor în domeniul spaţial plecându-se în schimb tot de la sistemul de bază RGB. Astfel, celelalte sisteme de reprezentare în domeniul spaţial au fost dezvoltate de aşa manieră încât imaginea să ţină seama şi de percepţia umană pentru a genera o imagine color cât mai apropiată de realitate.

Domeniul spaţial este deosebit de favorabil pentru a fi utilizat în steganografie deoarece permite încorporarea unei cantităţi mari de informaţii care poate permite efectuarea unor prelucrări multiple atât asupra obiectului de

acoperire, cât şi a mesajului secret într-o aşa manieră încât acesta din urmă să poată fi atât ascuns, cât şi mascat prin algoritmi specifici sau proceduri de dispersie în diferite locuri ale obiectului de acoperire. Aceste aspecte pot conduce la realizarea unei imagini steganografice de o calitate extrem de bună şi care în mod normal nu prezintă nici un fel de suspiciune.

Mai mult, algoritmii dezvoltaţi în domeniul spaţial pot fi combinaţi cu metode de compresie, de criptare suplimentare care pot mări şi mai mult performanţele sistemelor steganografice concepute pentru acest domeniu. Totodată algoritmii dezvoltaţi în acest domeniu pot prezenta anumite proprietăți ce permit adaptarea acestora pentru orice fel de arhitectură de procesoare, cum ar fi cele ce utilizează arhitecturi bazate pe banda de asamblare sau arhitecturi concepute pe mai multe nuclee, ceea ce poate conduce la scăderea costurilor, respectiv micşorarea semnificativă a timpului de execuţie.

4.2 ***Domeniul frecvenţei***

În ultimul timp a avut loc o dezvoltare foarte rapidă a telecomunicaţiilor şi ca atare şi cercetările în acest domeniu au dus la modificări multiple şi importante în tehnologiile de telecomunicaţii. Televiziunea este unul dintre sistemele de telecomunicaţii ce poate fi regăsit în cele mai diversificate domenii de activitate: economie, industrie, medicină, etc.

Sistemele de televiziune actuale pot fi împărţite în funcţie de modul în care imaginile sunt captate, prelucrate, transmise şi reproduse în trei categorii: analogice, analog-digitale şi digitale. Pe monitoarele calculatoarelor sau ecranului TV color pot fi vizualizate imagini create prin executarea unor operaţii ce presupun mixarea celor trei culori primare R,G,B la intensităţi diferite. Astfel pot fi create culorile alb şi gri, iar punctele roşu, verde şi albastru sunt stimulate simultan de către radiaţiile de electroni la nivele de energie diferită (intensităţi) formând astfel o imagine color continuă.

Majoritatea transformărilor unitare au tendinţa de compactare a unei importante părţi a informaţiilor dintr-o imagine într-un număr relativ mic de coeficienţi ai transformatei imaginii. Datorită faptului că energia totală se conservă, rezultă că o mare parte a coeficienţilor vor conţine o cantitate foarte mică de energie si pot fi astfel neglijaţi. Datorită acestor proprietăţi transformatele liniare sunt utile în compresia imaginilor şi recunoaşterea formelor. Un alt avantaj ce trebuie remarcat este faptul că reprezentarea imaginilor în domeniul frecvenţă ajută în diferite situaţii la reconstrucţia semnalelor discrete prin folosirea unor metode de interpolare. În astfel de sisteme imaginile sunt semnale bidimensionale discretizate în timp şi se bazează practic pe descompunerea semnalului imagine în funcţii de sinus şi cosinus, cunoscute sub denumirea de funcţii armonice [HOG06 ,GUI99, JAI89].

Cele mai utilizate transformări utilizate în prelucrarea imaginilor pentru generarea de algoritmi steganografici sunt: Transformata Fourier (FT), Transformata Fourier Discretă (DFT), Transformata Cosinus Discretă (DCT). În mod cert mai există şi alte tipuri de transformări, dar care au o utilitate mai redusă în steganografie.

În [TAC04] este propusă o metodă de ascundere a unui watermark digital prin selectarea unui coeficient diferit DCT a fiecărui bloc în procesul de încorporare. Alegând aleator coeficienţii selectaţi în fiecare bloc, metoda propusă poate schimba calitatea imaginii în mod independent.

[CHE06] Spre deosebire de abordările domeniului spaţial, mesajele secrete pot fi încorporate în coeficienţii de înaltă frecvenţă rezultaţi din Transformata Discretă de Undă (DWT). În [CHE06] sunt executate câteva operaţii matematice de bază, astfel încât coeficienţii din sub-banda de frecvenţă joasă sunt conservaţi fără a fi alteraţi, cu scopul de a îmbunătăţii calitatea imaginii.

4.2.1 Transformata Fourier

Trecerea de la *domeniul spațial* la *domeniul frecvenţă* se face cu ajutorul transformatei Fourier. Orice semnal periodic poate fi descompus într-o sumă de semnale sinusoidale şi cosinus. Această sumă este cunoscută sub denumirea de serie Fourier [HOG06, GUI99, JAI89].

Pentru a descrie un astfel de proces se ia ca exemplu un semnal periodic, notat $f(t)$ cu pulsatia. ω_0. Seria Fourier pentru acest semnal are expresia:

$$f(t) = \sum_{k=0}^{\infty} [[A]_k \cos(k\omega_0 t) + B_k \sin(k\omega_0 t)] \tag{4.8}$$

O relaţie asemănătoare se poate scrie şi pentru semnale neperiodice, diferenţa constă în aceea că de astă dată suma se transforma în integrală.

$$f(t) = \int_0^{\infty} (A_\omega \cos(\omega t) + B_\omega \sin(\omega t))\, d\omega \tag{4.9}$$

A_ω şi B_ω sunt definite de următoarele expresii:

$$A_\omega = A(\omega) = \frac{1}{\pi}\int_{-\infty}^{\infty} f(t)\cos(\omega t)dt \tag{4.10}$$

$$B_\omega = B(\omega) = \frac{1}{\pi}\int_{-\infty}^{\infty} f(t)\sin(\omega t)\,dt \tag{4.11}$$

Transformata Fourier interpretează, atât semnalul iniţial cât şi spectrul rezultat ca valori complexe. Spectrul Fourier $F(\omega)$ al unei funcţii date $f(t)$ se exprimă prin relaţia:

$$F(\omega) = \sqrt{\frac{\pi}{2}}[A(\omega) - iB(\omega)] = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty} f(t)[\cos(\omega t) - i\sin(\omega t)]dt = \frac{1}{2\pi}\int_{-\infty}^{\infty} f(t)\cdot e^{-i\omega t}dt \tag{4.12}$$

Tranziţia inversă se face prin formula:

$$f(t) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty} F(\omega)e^{i\omega t}dt \tag{4.13}$$

4.2.2 Transformata Fourier Discretă

În situaţia în care într-un proces de transformare între domenii se primeşte ca intrare un semnal discret, relaţiile mai sus descrise nu pot fi folosite. Însă, în modul de lucru ce utiliza calculatorul era necesară existenţa unei transformate care să accepte astfel de semnale la intrare. Din acest motiv s-a introdus Transformata Fourier Discretă (Discrete Fourier Transform - DFT). Domeniul de frecvenţă obţinut prin aplicarea acestei transformate nu conţine toate frecvenţele care compun imaginea, dar conţine suficientă informaţie astfel încât să permită o descriere a acesteia [HOG06, GUI99, JAI89]. Spre exemplu, pentru o imagine 2D de dimensiune $N \times N$ Transformata Fourier Discretă are relaţia :

$$F(k,l) = \frac{1}{N^2} \cdot \sum_{a=0}^{N-1} \sum_{b=0}^{N-1} f(a,b) e^{-i2\pi\left(\frac{ka}{N}+\frac{lb}{N}\right)} \tag{4.14}$$

Funcţia $f(a,b)$ caracterizează imaginea în domeniul spaţial.

Transformata inversă are expresia:

$$f(a,b) = \frac{1}{N^2} \cdot \sum_{k=0}^{N-1} \sum_{l=0}^{N-1} F(k,l) e^{2\pi i\left(\frac{ka}{N}+\frac{lb}{N}\right)} \tag{4.15}$$

Se observă faptul că în relaţiile (4.14) şi (4.15) se calculează două sume pentru fiecare punct din imagine. Pentru a uşura calculele se face apel la proprietatea de separabilitate a transformatei Fourier şi astfel se pot aplica următoarele formule:

$$F(k,l) = \frac{1}{N} \sum_{b=0}^{N-1} P(k,b) e^{-2\pi i \frac{lb}{N}} \tag{4.16}$$

Unde:

$$P(k,b) = \frac{1}{N} \sum_{a=0}^{N-1} f(a,b) e^{-2\pi i \frac{ka}{N}} \tag{4.17}$$

Cu ajutorul acestor formule într-o primă fază rezultă o imagine intermediară, calculând un număr de N transformate Fourier discrete unidimensionale după care este transformată în imaginea finală aplicând aceleaşi calcule. În acest mod se reduce practic numărul de calcule.

Cu toate acestea, complexitatea algoritmului este de N^2. Prin folosirea Transformatei Fourier Rapide (Fast Fourier Transform - FFT) se poate ajunge la complexitatea de $N \times log_2 N$. Această îmbunătăţire este semnificativă în special pentru imaginile de dimensiuni mari. Transformata Fourier Rapidă are acelaşi efect ca şi Transformata Fourier Discretă, doar că efectuează calculele mult mai rapid.

4.2.3 Transformata Cosinus Discretă

Transformata similară cu DFT, dar care operează cu numere reale este cunoscută sub denumirea de Transformata Cosinus Discretă (Discrete Cosine Transform - DCT). Cu ajutorul aceste transformări un şir de valori poate fi exprimat ca o sumă de funcţii cosinus de frecvenţe diferite. Folosirea funcţiei cosinus în loc de sinus este importantă, deoarece în urma experimentelor se pare că în cazul unei comprimări funcţia cosinus este mai eficientă.

Transformata cosinus discreta este o funcţie $F: R^N \rightarrow R^N$ care transformă secvenţa de N numere reale $x_0 \cdots x_{N-1}$ în numerele reale $X_0 \cdots X_{N-1}$ după una din formulele caracteristice [HOG06]. Cea mai des folosită formulă a transformatei cosinus discretă este următoarea:

$$X_k = \sum_{n=0}^{N-1} x_n \cos\left[\frac{\pi}{N}\left(n+\frac{1}{2}\right)k\right] \quad ; \quad k = 0,..N-1 \tag{4.18}$$

Transformata inversă are formula:

$$X_k = \frac{1}{2}x_0 + \sum_{n=1}^{N-1} x_n \cos\left[\frac{\pi}{N}n\left(k+\frac{1}{2}\right)\right] \quad ; \quad k = 0, \ldots, N-1 \tag{4.19}$$

În concluzie, reprezentarea în domeniul frecvenţă a semnalului imagine permite o îmbunătăţire a operaţiilor de procesare a imaginii, în special prin creşterea puterii de procesare a calculatorului. Aceste transformări au un impact în domeniul compresiei, reconstrucţiei şi recunoaşterii imaginilor şi ajută mecanismul de discretizare a semnalului continuu. Domeniul frecvenţei a fost exploatat şi în steganografie cu rezultate bune din punct de vedere al robusteţii mesajului secret, dar cu rezultate mai puţin mulţumitoare din punctul de vedere al cantităţii de informaţie ascunsă. Este de remarcat că în acest domeniu recuperarea imaginilor se poate obţine în condiţii bune, chiar şi în cazul în care canalul de transmisie este afectat de zgomot.

4.3 *Domeniul vectorial*

În ultimii ani există o tendinţă tot mai mare pentru ca fotografiile clasice să fie înlocuite de imagini digitale deoarece aceste prezintă avantaje legate de claritatea imaginii captate (rezoluţie), de stocarea şi prelucrarea acesteia în diferite formate.

Metodele şi tehnicile folosite în prelucrarea imaginilor digitale au la bază un puternic fundament matematic bazat pe diferite transformări ce au loc în domeniile de reprezentare ale imaginilor.

Se poate constata că relaţia matematică (4.1) poate fi interpretată ca fiind expresia unui vector într-un sistem tridimensional considerând R,G şi B versorii axelor. Pentru ca o imagine digitală să fie reprezentată în domeniul vectorial este necesară efectuarea unor transformări ce constau în reprezentarea imaginilor printr-o serie de funcţii ortogonale având un set de vectori de bază, numit imagine de bază [HOG06]. Acest set este generat cu ajutorul unor matrice unitare. Ca alternativă la reprezentarea matricială, o imagine de dimensiuni $n \times m$ poate fi considerată ca n vectori de dimensiune m . O transformare de imagini are ca rezultat un set de coordonate sau vectori de bază în acest spaţiu vectorial. Ca punct de plecare îl constituie transformarea liniară ce are la bază un suport teoretic care a fost creat

înainte de dezvoltarea prelucrărilor numerice de imagini. Un caz particular îl prezintă transformarea unitară ce are ca efect concentrarea energiei şi decorelarea datelor. Acest aspect poate fi utilizat la compresia imaginilor, recunoaşterea formelor şi prelucrarea rapidă în domeniul transformat. În urma schimbărilor de coordonate componentele obţinute sunt numite proiecţiile vectorului iniţial în noua bază.

Dacă elementele vectorilor de intrare sunt puternic corelaţi, coeficienţii rezultaţi au tendinţa de a nu se corela. Prin transformare, fiecare element al matricei transformate reprezintă coeficientul cu care se înmulţeşte imaginea de bază corespunzătoare. Transformarea directă realizează descompunerea, prin determinarea coeficienţilor, iar transformarea inversă realizează reconstrucţia prin însumarea imaginilor de bază, ponderate cu aceşti coeficienţi.

Spre deosebire de domeniul spaţial în care imaginea este reprezentată printr-o matrice de pixeli, în domeniul vectorial imaginea este reprezentată ca o matrice de vectori de pixeli. În acest sens, liniile sau coloanele unei matrice sunt considerate vectori de o anumită lungime. Fiecare vector de pixeli este format din valorile pixelilor în ordinea dată de linia de scalare.

Imaginile digitale reprezentate în domeniul vectorial derivă practic din utilizarea unor funcţii matematice regăsite în algebra liniară [HOG06]. Stocarea unei astfel de imagini necesită ocuparea unui spaţiu destul de mic în memoria calculatorului, iar dimensiunea acestora se poate mări oricât de mult, fără a se pierde din rezoluţie, deoarece în acest proces se schimbă doar parametrii funcţiilor matematice şi nu numărul elementelor imaginii.

4.3.1 Transformata Karhunen Lòeve bazată pe descompunerea în vectori şi valori proprii

Deoarece imaginile digitale sunt caracterizate prin matrice de pixeli pe baza algebrei liniare acestea pot fi transformate din domeniul spaţial RGB într-un domeniu al vectorilor şi valorilor proprii definit în continuare ca fiind domeniul vectorial la care se face referire în această lucrare.

Cel mai optim algoritm de transformare liniară a unui spaţiu în alt spaţiu este cunoscut sub numele de KLT (Karhunen Lòeve Transform). Ideea pe care se bazează acest algoritm este că face transformări dintr-o bază în alta, în urma cărora reţine (cunoaşte şi recunoaşte) informaţia cea mai importantă prin vectorii şi valorile proprii corespunzătoare. Pe aceste considerente este de asemenea clasificat ca fiind cel mai optim în termeni de energie de compactare şi eroare de reconstrucţie [YUN99].

În algebra liniară [HOG06] un vector se notează astfel:

$$\vec{v} = \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix} \tag{4.20}$$

Sau pentru simplitate, se poate nota şi:

$$\vec{v} = [1, \quad 2, \quad 3, \quad 4] \tag{4.21}$$

Fiecare vector are doi parametrii ce îl caracterizează:

- *Dimensiunea unui vector*: este dată de numărul de elemente/componente din care este format; Un element al

vectorului se notează v_i şi reprezintă valoarea vectorului $\vec{v}$ în dimensiunea i ;

- *Lungimea unui vector*: reprezintă radical din suma pătratelor componentelor sale:

$$\vec{v} = \sqrt{\sum_{i=1}^{n} x_i^2} \tag{4.22}$$

De asemenea există diferite condiţii matematice impuse astfel încât un vector oarecare poate fi definit ca vector propriu caracterizat de o valoare proprie. În acest sens, un vector propriu este un vector diferit de zero care satisface următoarea ecuaţie:

$$A\vec{v} = \lambda\vec{v} \tag{4.23}$$

Unde A este o matrice pătratică, $\vec{v}$ este un vector propriu, iar λ este un scalar considerat valoare proprie. Valorile proprii şi vectorii proprii sunt cunoscute şi ca rădăcini caracteristice/singulare şi vectori caracteristici/singulari [HOG06].

În transformata KLT se consideră o imagine ca fiind reprezentată sub forma unei matrice formată din "m" linii şi "n" coloane. Această matrice poate fi interpretată şi ca un tablou de vectori de dimensiune "m".

Transformata KLT aplică relaţia:

$$Y = Q^T X \tag{4.24}$$

Unde:

X - este matricea iniţială (de dimensiune $m \times n$).

Q - reprezintă o matrice de vectori proprii ai matricei de covarianţă.

Q^T - reprezintă matricea transpusă a matricei de vectori proprii.

Y - este proiecţia matricei iniţiale în noile coordonate.

$$Cov = \begin{bmatrix} cov(x,x) & cov(x,y) & cov(x,z) \\ cov(y,x) & cov(y,y) & cov(y,z) \\ cov(z,x) & cov(z,y) & cov(z,z) \end{bmatrix} \tag{4.25}$$

Diagonala principală conţine covarianţa între o dimensiune şi ea însăşi $(x,x), (y,y), (z,z)$ şi reprezintă de fapt, varianţa. O matrice de covarianţă este simetrică faţă de diagonala principală deoarece:

$$cov(x,y) = cov(y,x) \tag{4.26}$$

$Cov(x,y)$ se calculeaza folosind relaţia:

$$Cov(x,y) = \frac{\sum_{i=1}^{n}[(x]_i - \vec{x})(y_i - \vec{y})}{n-1} \tag{4.27}$$

Unde:

$\vec{x}$, $\vec{y}$ - media aritmetică a lui x_i , respectiv y_i , pentru $i = 1, \dots, n$

Q - matricea de vectori proprii ai matricei de covarianţă

Pentru a obţine matricea de vectori proprii se pleacă de la premisa că dacă A este o matrice pătratică, atunci un vector $x < R^n$ se numeşte vector propriu în raport cu A [STR03];

Un vector propriu ($\vec{x}$) este un vector diferit de zero care satisface următoarea ecuaţie:

$$A\vec{x} = \lambda\vec{x} \tag{4.28}$$

Numărul λ se numeşte şi valoare proprie.

Valorile proprii şi vectorii proprii se pot determina tratând o matrice ca un sistem de ecuaţii liniare, iar în urma rezolvării acestora se obţin valorile variabilelor ce formează în final componentele vectorilor proprii.

Sistemul de ecuaţii liniare descris de ecuaţia (4.28) se poate scrie:

$$(A - \lambda I) \times x = \mathbf{0} \tag{4.29}$$

Acest sistem este omogen şi admite o soluţie nenulă dacă şi numai dacă determinantul stemului are valoare zero.

Valorile proprii ale matricei A sunt rădăcinile polinomului caracteristic:

$$P(\lambda) = \det(A - \lambda I) = \mathbf{0} \tag{4.30}$$

Polinomul de grad ”n”, $P(\lambda)$ se numeşte polinom caracteristic al matricei A, iar ecuaţia (4.30) se numeşte ecuaţie caracteristică. I reprezintă matricea identitate. Dacă matricea A este simetrică, atunci valorile sale proprii sunt reale şi există o bază formată din vectori proprii, ce transformă astfel matricea A într-o matrice diagonală.

Tehnica folosită de către transformata KLT are ca scop reducerea dimensiunilor seturilor de date pentru a fi analizate mai uşor. În principiu, din punct de vedere matematic transformata KLT este o transformare liniară, ortogonală ce transformă un set de date într-un nou sistem de coordonate.

Această transformare poate fi regăsită în multiple aplicaţii cum ar fi: generarea variabilelor random normale corelate [FEG02]. Alt tip de aplicaţii ale transformatei KLT constau în utilizarea tehnicilor de calculare pentru generarea filtrelor Wiener [PRA72].

În domeniul imaginilor digitale cu ajutorul transformatei KLT se poate obţine o compresie optimă a semnalelor ceea ce reduce complexitatea calculelor prin aplicarea acestui algoritm [WAR97, QUI00]. În principiu se regăsesc aceleaşi valori ca şi în cazul unei transformări DCT , dar tehnica KLT prezintă avantaje superioare când sunt utilizate scheme adaptive frecvent aplicate în industrie [SHI93], [EFF03].

Tot în domeniul video se pot utiliza transformări KLT în codificarea avansată audio pentru standardele MPEG [YAN01].

Transformata KLT are diverse aplicaţii, ceea ce permite prelucrarea statistică a unor informaţii din diferite domenii, cum ar fi: seismologie (domeniul prelucrărilor statistice ale semnalelor seismografice) [LON05] sau a semnalelor electrocardiografice (EKG) [HER06].

În mod frecvent în domeniul procesării semnalelor digitale,respectiv: procesarea imaginilor, a sunetului, recunoaşterea semnalelor, în sistemele de comunicaţii şi generarea de filtre, transformata KLT este considerată ca o prelucrare optimă a semnalelor pentru reprezentarea, compresia, analiza şi procesarea datelor.

Astfel în [GAS06] transformata KLT reprezintă elementul cheie privind procesarea semnalelor şi transmiterea obiectelor de procesare în mod distribuit.

Mai mult, în [UNS84] se demonstrează că transformata KLT este superioară altor tipuri de transformate, cum ar fi: DFT (Discret Fourier Transform), DCT (Discret Cosinus Transform), DREFT (Discret Real Even Fourier Transform), DOFT (Discret Odd Fourier Transform), DROFT (Discret Real Odd Fourier Transform).

Acest lucru devine cu atât mai evident dacă se utilizează o aproximare a transformatei KLT.

Fritsch propune în [FRI08] folosirea transformatei KLT pentru realizarea unor codoare şi decodoare de imagini în momentul transmiterii acestora pe diferite canale de comunicaţii cum ar fi: Internetul, telefonia mobilă, etc.

Avându-se în vedere multitudinea aplicaţiilor ce utilizează transformata KLT, aceasta constituie o alternativă în domeniul steganografiei, fiind folosită într-un proces de ascundere fie prin comprimarea mesajului ce urmează a fi încorporat, fie prin înlocuirea coordonatelor de grad inferior cu mesajul secret.

Transformata KLT poate fi folosită la comprimarea datelor secrete urmând ca acestea să fie încorporate prin diferite procedee în obiectul de acoperire ales.

O altă posibilitate de utilizare a transformatei KLT într-un proces steganografic o constituie proiecţia în noi coordonate atât a mesajului, cât şi a obiectului de acoperire, după care are loc substituirea proiecţiilor de grad inferior a obiectului de acoperire cu mesajul secret [DAF03].

4.3.2 Transformata bazată pe descompunerea în valori singulare

Transformata bazată pe descompunerea în valori singulare este notată prescurtat SVD (Singular Value Decomposition) şi are ca fundament matematic faptul că orice matrice se poate descompune ca un produs de trei matrice [STR03]:

$$A_{mn} = U_{mm} S_{mn} V_{nn}^{T} \tag{4.31}$$

Unde: U - matricea ortogonalã

S - matricea diagonalã

V - transpusa matricei ortogonale

Cele trei matrice au urmãtoarele proprietãþi: : $U^T U = I$, $V^T V = I$,coloanele lui U sunt vectori proprii ortonormali ai lui AA^T, coloanele lui V sunt vectori proprii ai lui $A^T A$, iar S este o matrice diagonală conţinând rădăcinile pătratice ale valorilor proprii ale lui U sau V în ordine descrescătoare.

În mod frecvent transformata SVD este utilizatã pentru compresia imaginilor digitale, a semnalelor audio ºi mai nou în algoritmi steganografici deoarece prezintã proprietatea cã sunt rezistenþi la atacuri.

În concluzie, ca alternativă la reprezentarea matricială o imagine de dimensiuni $n \times m$ poate fi considerată ca n vectori de dimensiune m . O transformare de imagini are ca rezultat un set de coordonate sau vectori de bază în acest spaţiu vectorial ce realizează o rotaţie a coordonatelor de bază, iar componentele obţinute sunt numite proiecţiile vectorului iniţial în noua bază. Dacă elementele vectorilor de intrare sunt puternici corelaţi, coeficienţii transformării au tendinţa de a nu se corela. În acest sens transformata KLT împachetează maximum de informaţii într-un număr dat de coeficienţi ai transformării.

Domeniul vectorial este relativ puţin exploatat în momentul de faţă în steganografie deoarece utilizarea transformatei KLT este însoţită de costuri apreciabile, chiar dacă performanţele în domeniul prelucrării de date sunt foarte atrăgătoare. În realitate majoritatea algoritmilor steganografici pot implica costuri relativ mari indiferent de metoda aplicată, în special în cazul în care mediul utilizat este de tipul imagine digitală. Din acest motiv consider că domeniul vectorial poate constitui o îmbinare optimă calitate-cost, afirmaţie ce-o voi demonstra în capitolele următoare.

4.4 *Concluzii referitoare la domeniile de reprezentare a imaginilor digitale*

Imaginea digitală este una dintre cele mai utilizate medii în steganografie datorită acţiunii directe cu sistemul senzorial uman şi este dezvoltată în trei domenii de reprezentare prezentate în acest capitol.

Domeniul spaţial s-a dezvoltat pe baza exprimării pixelilor într-un spaţiu reprezentat prin cele trei axe de bază ce reprezintă culorile primare roşu, verde şi albastru. La ora actuală există mai multe reprezentări spaţiale ale pixelului, unele sunt bazate pe modalitatea de captare şi reproducere a imaginilor, altele bazate pe mecanismele fiziologice de percepţie a culorilor de către ochiul uman. Indiferent de formatul ales al domeniului spaţial, imaginea digitală exprimată sub formă binară, alb-negru sau color este reprezentată printr-o matrice sau mai multe matrice de M coloane şi N linii, unde dimensiunea matricei exprimă rezoluţia imaginii respective.

Din acest motiv majoritatea algoritmilor steganografici constau în prelucrări de matrice de aşa manieră încât mesajul ascuns să fie încorporat în imaginea purtătoare (obiectul de acoperire) prin substituirea unor valori nesemnificative a pixelilor din imaginea purtătoare cu valori semnificative ale mesajului încorporat, rezultând în felul acesta imaginea steganografică. Metodele folosite în steganografie trebuie astfel alese încât o analiză vizuală sau chiar matematică a imaginii steganografice să nu conducă la suspiciunea că aceasta este purtătoare de mesaj ascuns.

Plecând de la acest principiu se pot concepe strategii mult mai sofisticate prin care chiar în eventualitatea unei suspiciuni că în imaginea steganografică ar putea exista un mesaj secret, acesta să nu poată fi recuperat de către persoane neautorizate. Se poate afirma că algoritmii de ascundere ce utilizează ca domeniu de reprezentare domeniul spaţial sunt unii dintre cei mai răspândiţi la ora actuală având cele mai multe aplicaţii în domeniul steganografiei, fiind în general mai uşor de implementat pentru că necesită operaţii de calcul repetitive. În aceeaşi măsură presupun un volum mare de prelucrare în cazul încorporării unor mesaje de dimensiuni mari, ceea ce implică un timp de execuţie relativ mare pentru astfel de algoritmi. O soluţie pentru micşorarea timpului de execuţie ar fi cablarea hardware a acestor algoritmi sau utilizarea unor microprocesoare dedicate acestui scop.

Reprezentarea imaginilor în domeniul frecvenţă se bazează pe descompunerea semnalelor din domeniul timp în domeniul frecvenţă plecându-se de la Transformata Fourier Discretă şi ajungând la Transformata Cosinus Discretă. În funcţie de tipul aplicaţiei se pot utiliza şi alte transformări. Ceea ce este caracteristic acestui domeniu este faptul că un număr mic de coeficienţi ai transformatelor înglobează o cantitate mare din energia transformării imaginilor. Acest domeniu se pretează cu precădere în prelucrări de imagini, recunoaşterea formelor şi comprimarea datelor, dar este un domeniu potrivit şi pentru ascunderea datelor.

Se poate spune că acest domeniu este unul dintre cele mai exploatate în steganografie şi se constată că algoritmii steganografici care sunt implementaţi în domeniul frecvenţă prezintă un grad sporit de robusteţe fiind cu precădere recomandaţi în ascunderea watermark-urilor. Pe de altă parte, indiferent de algoritmul implementat cantitatea de informaţii ascunsă este relativ redusă. Din

acest motiv, acest domeniu a constituit pentru mine o etapă tranzitorie de cercetare. Rezultatele obţinute au condus la ascunderea unor mesaje watermark cu un grad ridicat de robusteţe [STA07b, STA08a].

Domeniul vectorial prezintă un optim din punct de vedere statistic având performanţe ridicate şi constă în interpretarea pixelilor sub formă de vectori. În urma transformării domeniului spaţial în domeniul vectorial se generează valori şi vectori proprii ce pot fi încorporaţi fie într-o imagine reprezentată în domeniul spaţial, fie într-o imagine reprezentată în domeniul vectorial. Mai mult, acest domeniu permite o compresie a datelor fără pierderea calităţii imaginii. Datorită acestei ultime proprietăţi acest domeniu poate fi atrăgător pentru aplicaţii steganografice. Cu toate acestea sunt puţini cercetători care au abordat acest aspect, fiindu-le probabil mai la îndemână procesările în domeniul frecvenţă.

În capitolele ce urmează voi dezvolta proprietăţile acestui domeniu pentru a obţine algoritmi steganografici cu o rată de încorporare care poate ajunge la o capacitate de 100% raportată la mărimea obiectului de acoperire, cu obţinerea unei imagini steganografice de o foarte bună calitate şi cu un grad de recuperare a mesajului ce poate atinge 99% din mesajul iniţial. Menţionez că domeniul vectorial este puţin abordat în literatura de specialitate în domeniul steganografiei, fiind folosit cu precădere în alte domenii.

Pe baza celor arătate mai sus apreciez că pentru domeniul steganografic în care cantitatea de informaţii ascunse este mare, domeniul spaţial şi cel vectorial prezintă candidaturile cele mai potrivite.

5 STEGANOGRAFIA BAZATĂ PE IMPLEMENTARE HARDWARE

Cercetarea în domeniul steganografiei se poate spune că a ajuns la maturitate atât prin generarea unor concepte de modele teoretice pentru dezvoltarea unor modele steganografice cu o siguranţă sporită, cât şi în realizarea unor algoritmi relativ puternici din punct de vedere al ascunderii de informaţie. Este de dorit ca algoritmii creaţi în acest sens să genereze obiecte steganografice robuste la atacurile din exterior, cu un grad de detectabilitate redus a mesajelor secrete, cu o recuperare bună a datelor la recepţie şi cu o capacitate mare de ascundere [MOS01].

După cum am arătat în Capitolul 4 privind mediile de ascundere în care se încorporează mesajul secret, flexibilitatea cea mai mare în abordarea sistemelor steganografice o reprezintă mediile digitale în general, respectiv imaginile digitale în particular. Ca urmare a utilizării acestor medii, după cum se va vedea în capitolele următoare au fost generaţi o serie de algoritmi steganografici care să îndeplinească principalele cerinţe ale etapei actuale de dezvoltare în acest domeniu privind securitatea şi capacitatea informaţiilor ascunse.

Într-un raport Mark Owens de la Institutul de Securitate a Informaţiilor din SUA [OWE02] se prezintă diferite modalităţi de securizare a informaţiilor transmise pe căile de comunicaţie electronice. În acest raport autorul a abordat şi "Problema prizonierilor" [SIM84] scoţând în evidenţă mai multe aspecte legate de steganografie, cum ar fi : ascunderea cât mai perfectă prin metode steganografice, cifrarea mesajelor sau/şi folosirea combinată a celor două metode. Evident că aceste cerinţe legate de securitate în domeniul steganografiei implică utilizarea tuturor resurselor hardware şi software ale sistemelor numerice.

Dacă din punct de vedere software la ora actuală algoritmii de ascundere sunt bine reprezentaţi în literatura de specialitate, nu se poate spune acelaşi lucru despre utilizarea lor în hardware. În acest sens au fost realizate destul de puţine încercări pentru implementarea algoritmilor steganografici în hardware. Acest domeniu ridică o serie de probleme, cum ar fi cunoştinţe atât în domeniul programării în limbaj maşină, respectiv despre structura microsistemului, microprocesorului, simulare în arii programabile cât şi o dotare de laborator corespunzătoare. Astfel de cerinţe sunt mai greu de îndeplinit indiferent cât de puternic este calculatorul din dotarea cercetătorului. Mai mult, obiectivul final al cercetării implementării hardware al algoritmilor steganografici impune dezvoltarea sau adaptarea sistemelor hardware la cerinţele domeniului, obţinerea unor performanţe ridicate în special în domeniul timpului real, consum de putere mică pentru a fi folosite ca echipamente mobile (spre exemplu în telefonia mobilă). De asemenea soluţiile propuse trebuie să fie independente, sigure în funcţionare şi să prezinte costuri reduse.

O astfel de abordare poate fi obţinută doar prin îmbinarea eficientă a unor implementări hardware şi generarea unor algoritmi adecvaţi sistemului utilizat, respectiv adaptarea software la configuraţia echipamentului folosit. Acest aspect poate fi dezvoltat pe mai multe nivele, cum ar fi : integrarea la nivel de circuit prin dezvoltarea unor arhitecturi adecvate în conceperea de circuite dedicate scopului menţionat. Un alt nivel ar consta în utilizarea microsistemelor, microprocesoarelor existente şi generarea unor codoare şi decodoare steganografice pe acestea.

O colaborare cu firmele producătoare de procesoare ar putea îmbina universalitatea microprocesoarelor prin încorporarea în interiorul acestora a unor codoare - decodoare steganografice, care să fie folosite la transmiterea securizată a unor informaţii. În perspectivă se tinde la generarea unor astfel de microsisteme, microprocesoare cu funcţii de ascundere steganografice care să fie utilizate la ora actuală în telefonia mobilă.

5.1 *Steganografia în arii programabile*

Ariile programabile denumite FPGA (Field Programmable Gate Array) prezintă avantajul că sunt relativ simplu de programat, dispun de o largă documentaţie tehnică şi o bibliotecă de programe şi funcţii bine susţinută în literatura de specialitate. Din punct de vedere al costurilor FPGA - urile sunt scumpe şi limitate în ceea ce priveşte flexibilitatea lor.

Printre primele încercări de implementare a unui mesaj ascuns pentru protecţia proprietăţii intelectuale, în [LAC99] autorii prezintă o soluţie tehnică verificată pe arii programabile FPGA - uri pentru protecţia şi integritatea mărcii unui produs privind măştile circuitelor integrate. Soluţia rezultată este deosebit de robustă şi face imposibilă copierea acestora. Arhitectura FPGA rezultată este considerată de autori ca fiind cu 25% mai mică decât în cazul folosirii microprocesoarele pe 32 de biţi din familia ARM de tip RISC. În lucrare nu sunt specificate clar costurile unei astfel de implementări hard care după părerea mea sunt mult mai ridicate decât în cazul utilizării unui microprocesor. Timpii de execuţie rezultaţi pentru introducerea unei mărci ascunse sunt declaraţi a fi comparabili faţă de executarea algoritmului pe un microprocesor.

În [EIS00] sunt propuse mecanisme de reconfigurare pentru crearea unor sisteme de inserare axate pe partiţionare şi planificare. Toate detaliile de nivel inferior ale resurselor reconfigurabile sunt ascunse acoperind atât timpul de compilare a reconfigurării, cât şi timpul de rulare. Se specifică faptul că există posibilitatea mapării aplicaţiei atât pe acelaşi FPGA, cât şi pe diferite alte fuga-uri. Un studiu de caz demonstrează eficienţa şi utilitatea acestei abordări.

În [FAR05] autorii folosesc un algoritm hibrid de ascundere ce poate fi folosit în steganografie. Algoritmul a fost îmbunătăţit prin utilizarea unui FPGA prin exploatarea posibilităţii de execuţie paralelă ce conduce la obţinerea unei cantităţi mari de prelucrare apreciată la 106 Mbps, ceea ce ar permite o execuţie în timp real. Rezultatele implementării au fost verificate pe un FPGA din familia Spartan 2 şi au fost comparate cu alte arhitecturi FPGA ce au utilizat algoritmi steganografici diferiţi. Astfel a fost obţinută o rată de transfer a obiectului steganografic de 95,53 Mbps.

În [ELT07] a fost implementată o tehnică de modificare a imaginii cu ajutorul coeficienţilor de bandă mijlocie. Tehnica propusă permite utilizarea a 49% din zona chip-ului şi operează pe o frecvenţă de 36 MHz. În urma comparării performanţelor dintre implementarea soft şi hard s-a obţinut o îmbunătăţire a timpului de execuţie de 7 ori mai rapidă în comparaţie cu implementarea software.

O arhitectură de ascundere a unor mesaje discrete este propusă în lucrarea [MOH07] prin utilizarea a două moduri de implementare : prin folosirea unor circuite Xilinx de arii programabile, respectiv prin construirea unui circuit integrat modificat. Aceste prototipuri de circuite obţinute prin simulare permit obţinerea unor capacităţi de ascundere satisfăcătoare şi obţinerea unui mesaj steganografic robust.

Un proces de ascundere a informaţiei este descris în lucrarea [GOM08] unde este folosită o metodă de depistare a schimbărilor abrupte ale nivelelor de gri şi

ascunderea mesajului în astfel de regiuni. Autorii susţin că procesul de localizare a zonelor în care se ascunde mesajul este scump de implementat, iar cantitatea de informaţii inserate permite viteze mari de procesare, putând ajunge până la 61,5 Mbps.

Prin introducerea unei noi abordări prin care se ascunde însăşi existenţa mesajului, El Zouka [ZOU08] utilizează un fişier gazdă a obiectului de acoperire, practic nemodificat, dar ce apelează la o cheie ce reprezintă elementul de start care va genera o secvenţă de numere ce vor identifica biţii din fişierul gazdă a obiectului de acoperire şi care conţine de fapt mesajul secret. Prin urmare orice atac face imposibilă depistarea mesajului secret. Metoda prezintă dezavantajul că implică ascunderea unei cantităţi mici de informaţie ce ar putea fi îmbunătăţită prin implementare hardware pe un FPGA.

Un algoritm de ascundere bazat pe transformata cosinus discretă DCT este implementat şi descris în [SAL08]. Pentru materializarea implementării a fost utilizat un FPGA din familia Xilinx care utilizează aproximativ o treime din zonă având un timp de execuţie de 2 ori mai mic decât în cazul implementării software. Din punct de vedere al eficienţei algoritmului folosit este de remarcat faptul că un bit al imaginii secrete este ascuns într-un bloc de 8 × 8 biţi ai imaginii gazdă. Se remarcă faptul că algoritmul permite ascunderea unei cantităţi mici de date, dar folosind o implementare hardware a condus la îmbunătăţirea timpului de execuţie.

Toate încercările de implementare şi dezvoltare a unor algoritmi steganografici care să poată fi implementaţi în arii programabile scot în evidenţă faptul că în urma alegerii unei arhitecturi adecvate şi prin adaptarea corespunzătoare a acestora, rezultatele obţinute sunt superioare implementărilor software, chiar dacă frecvenţa de lucru a ariilor programabile este semnificativ mai mică decât frecvenţa procesoarelor din calculatoare. În plus se obţine o utilizare mai eficientă a memoriei operative, ceea ce face ca astfel de aplicaţii să devină atractive în viitorul apropiat. Cu toate acestea consider că ariile programabile pot constitui doar o etapă intermediară până la obţinerea unui produs cablat care sa încorporeze un sistem steganografic, deoarece din punct de vedere practic astfel de echipamente sunt relativ scumpe şi nu se pot constitui ca un produs final, în schimb constituie un suport benefic în domeniul cercetării.

5.2 *Steganografia în circuite*

Altă modalitate de ascundere a datelor secrete se poate baza pe aranjarea fizică a unui obiect de acoperire ales în procesul steganografic. Aranjamentul poate fi o semnătură ascunsă care este unică pentru cel ce trimite mesajul. Un astfel de exemplu ar putea fi, traseul liniilor de cod distribuite într-un program sau schema unui circuit electronic pe o placă. Acest tip de marcare poate fi utilizat pentru identificarea unică a desenului original şi nu poate fi şters fără schimbări semnificative.

[FAR04] prezintă un model steganografic ce constă în alegerea unui obiect de acoperire şi implementarea unei chei secrete într-o micro-arhitectură. Pentru validarea ideii s-au folosit ariile programabile ce au fost utilizate în simularea procesului. Conţinutul mesajului secret este distribuit în obiectul de acoperire într-un anumit mod, care se bazează pe o cheie secretă ce este cunoscută doar de emiţător şi receptor. În astfel de situaţii, chiar dacă o persoană neautorizată descoperă existenţa mesajului, fără cheia secretă nu este posibilă recuperarea

acestuia. Scopul urmărit în astfel de cazuri este reasamblarea conţinutului mesajului secret.

Datorită faptului că tot mai mulţi oameni sunt tentaţi să copieze în mod ilegal diferite produse, a dus la dezvoltarea de noi tehnici în vederea protejării dreptului de autor prin introducerea unor informaţii ascunse şi numere de serie în produse audio şi video.

În [YUC08] se propune o schemă de watermarking ce se bazează pe diferite testări în vederea identificării proprietăţii intelectuale (IP). Se urmăreşte dezvoltarea unor proceduri de identificare a unui semn watermark. Conceptul de bază al procesului steganografic prezentat constă în încorporarea unui circuit de generare a semnului watermark şi a unui circuit de test. Ca urmare, schema propusă poate să reziste unor atacuri şi poate identifica IP-ul la diferite nivele ale schemei. În timpul procesului general de testare este dovedită identitatea IP-ului fără a necesita o altă implementare în plus. Ca rezultat obţinut în urma testelor pe o schemă reală se poate constata că schema hardware propusă conţine un număr relativ mic de componente suplimentare, costuri reduse, un timp de procesare mic. Metoda propusă rezolvă problema identificării proprietăţii intelectuale.

[MOH05] prezintă o arhitectură integrată pe scară largă (VLSI) pentru implementarea a două imagini de watermarking pentru orice cameră digitală. Prototipul circuitului integrat implementat este constituit din aproximativ 28500 de porţi folosind tehnologia de integrare de 0,35 μm cu un consum de 6,9 MW şi operând la o frecvenţă de aproximativ 300 MHz. Scopul lucrării este de a asigura protecţia intelectuală, iar pentru aceasta a fost folosit un algoritm steganografic bazat pe metoda celui mai puţin semnificativ bit. Autorii pretind că această arhitectură VLSI este prima din domeniu.

Mohanty continuă în [MOH07] cercetarea efectuată în lucrarea anterioară [MOH05] prin construirea unui prototip de circuit integrat modificat faţă de cel anterior cu scopul executării unor algoritmi de ascundere a unui mesaj secret invizibil într-o imagine. Ascunderea mesajului secret se face în domeniul spaţial. Rezultatele implementării algoritmului de ascundere confirmă faptul că sunt generate mesaje robuste ce pot fi greu perturbate sau distruse de către un eventual atacator.

Este de remarcat că încercările de implementare a unui algoritm steganografic în măştile circuitelor integrate sau generarea unui circuit dedicat acestui scop prezintă până în prezent încercări timide, ceea ce poate fi explicat prin faptul că domeniul steganografic este unul relativ nou. Utilizarea microprocesoarelor pentru generarea de obiecte steganografice pot spune că este un domeniu şi mai nou, ceea ce explică numărul redus de publicaţii pe această direcţie de cercetare. Consider că utilizarea procesoarelor poate conduce la rezultate apreciabile în implementarea şi generarea unor algoritmi steganografici cu proprietăţi deosebite în ceea ce priveşte timpul de execuţie (care poate rezolva problema timpului real), a capacităţii de ascundere, respectiv dificultăţi deosebite în detecţia mesajelor ascunse.

5.3 *Steganografia în telefonia mobilă*

Se poate constata tot mai frecvent utilizarea telefonului mobil pentru comunicare fie utilizând transferul sigur de date dintre un calculator ºi-un utilizator de telefoane mobile, fie prin comunicarea directã între doi utilizatori de telefonie mobilã. Este de dorit ca toate aceste comunicaþii sã fie cât mai sigure ºi sã asigure în acelaºi timp ºi confidenþialitate.

Astfel în [SHA05] este prezentată o metodă pentru ascunderea datelor în imagini folosind algoritmi steganografici. Metoda descrisă constă în transferul de date sigure dintre un calculator către utilizatori de telefoane mobile ce au încorporat un decodor pentru extragerea informaţiei ascunse folosind un program JAVA. Decodificatorul a fost implementat pe un telefon mobil şi testat pe un aparat NOKIA 6600. Metoda constă în ascunderea unei informaţii într-o imagine trimisă de pe un calculator prevăzut cu o parolă personal. La trimiterea imaginii steganografice către utilizatorul de telefoane mobile, în cazul în care acesta are prevăzut un program de decodificare poate extrage mesajul ascuns. Se poate remarca faptul că în această lucrare decodorul implementat pe telefonul mobil este sub forma unui program de decodificare, iar mesajul recuperat este de tip static. Un caz particular în exploatarea algoritmului prezentat a constat în postarea notelor private ale unui student în cauză. În acest fel se constată că metoda permite transmiterea unei cantităţi mici de informaţii.

Pentru ascunderea informaţiilor în cazul convorbirilor telefonice se propune o nouă metodă steganografică în [JUN02] pentru generarea unor comunicaţii sigure pe reţelele de telefonie publică. În vederea implementării unui astfel de sistem de convorbire telefonică securizată folosind tehnica ascunderii informaţiei au fost utilizate microcontrolere de tip DSP (Digital Signal Processor) din familia TM (produs de Texas Instruments). Rezultatul cercetării confirmă posibilitatea transmiterii unei convorbiri telefonice suprapusă peste un obiect steganografic ce încorporează un mesaj confidenţial.

În lucrarea [JUN03] se propune ascunderea informaţiei prin utilizarea unui microcontroler DSP cu posibilităţi de lucru în paralel privind procesarea vorbirii. Acesta este încorporat într-un telefon cu rolul de a procesa mesajele verbale ce urmează a fi ascunse. Fiind folosită transmiterea informaţiei pe cale audio este evident că în acest fel cantitatea de informaţii ce poate fi ascunsă este relativ redusă.

O aplicaţie interesantă a steganografiei prezentată în [SUZ08] constă în realizarea unor interacţiuni dintre telefonul mobil şi alte dispozitive hardware folosind ca elemente de recunoaştere camera digitală a telefonului. Această interacţiune implică conexiunea a două echipamente hard fără nici un fel de soft suplimentar prin diferite proceduri, cum ar fi: selectarea imaginii, afişarea imaginii pe întreg ecranul sau conectarea camerei mobilului la dispozitivul cu care trebuie să fie interconectat. Cheia interacţiunii se bazează pe FPcode (Fine Picture code) ce utilizează o metodă de ascundere a codului dispozitivului hard ce urmează a fi conectat la mobil.

[KEJ04, KEJ05] propune partiţionarea algoritmilor de inserare şi extragere a mărcii de protecţie intelectuală pentru produsele transmise prin telefonia mobilă. Autorii afirmă că algoritmii de ascundere necesită un consum mare de energie, iar telefoanele mobile nu posedă o cantitate de energie inepuizabilă. Pentru a soluţiona problema consumului de energie este propus ca procesul de inserare şi extragere să fie executat pe un server care ar putea reduce consumul total de energie a telefoanelor mobile cu 80% şi îmbunătăţeşte performanţele procesului steganografic. Practic telefonul mobil este folosit doar ca dispozitiv de transmitere.

Se constată un interes sporit în crearea unor soluţii ce vin în întâmpinarea unui număr tot mai mare de utilizatori de telefonie mobilă privind securizarea comunicării şi/sau confidenţialitatea acesteia. O soluţie în această direcţie o poate asigura dezvoltarea unor algoritmi steganografici pentru telefoanele mobile existente sau adăugarea la microprocesoarele folosite în telefoanele mobile a unor astfel de soluţii implementate hardware. În telefonia mobilă de regulă sunt utilizate

procesoare dedicate, multe din acestea făcând parte din clasa procesoarelor RISC (Reduced Instruction Set Computer). Printre cele mai cunoscute din această clasă sunt procesoarele ARM (Advanced RISC Machine). Ca atare, o parte din algoritmii steganografici pe care i-am dezvoltat au fost implementaţi pe un astfel de procesor.

5.4 *Microprocesoare propuse pentru utilizare în steganografie*

Este foarte bine ştiut că în ultima vreme dispozitivele mobile prezintă performanţe deosebit de avansate încât pot face o mulţime de lucruri care înainte erau posibil de realizat doar cu ajutorul unor calculatoare performante. La ora actuală telefonia mobilă a trecut de la simple realizări de contacte la aplicaţii deosebit de complexe cum ar fi procesarea de sunet, imagini, ceea ce face ca la ora actuală telefoanele mobile să înlocuiască cu succes multe din necesităţile pe care ni le ofereau calculatoarele personale.

În privinţa dezvoltării telefoniei mobile până în prezent s-a pus accentul creşterii frecvenţei de lucru a procesoarelor utilizate în acest scop, în ideea îmbunătăţirii performanţelor computaţionale. Evident, acest aspect nu poate merge la infinit pe această direcţie. Din acest motiv marii producători de procesoare au căutat soluţii alternative în acest scop. Una dintre aceste soluţii impuse constă în paralelizarea calculelor şi a fost adoptată pentru a fi utilizată în platformele mobile. Este de aşteptat ca în cel mai scurt timp locul procesoarelor ARM ce sunt folosite în prezent în telefonia mobilă să fie luat în curând de microprocesoare cu mai multe nuclee. Ca urmare este de aşteptat o scădere a puterii consumate şi creşterea performanţelor permiţând dezvoltări de aplicaţii complexe. O aplicaţie demult impusă dar dificil de realizat până în prezent constă în confidenţialitatea transmiterii mesajelor tip: text, audio, imagine, video. Este de aşteptat ca următoarele generaţii de telefoane mobile să conţină aplicaţii domeniile: inteligenţei artificiale, grafică 3D, procesare audio-video, respectiv steganografie.

În continuare voi prezenta pe scurt două platforme ce au în componenţa lor microprocesoarele cele mai utilizate în telefonia mobilă în prezent (ARM), respectiv microprocesorul cu mai multe unităţi de prelucrare ISAAC produs de firma MOVIDIA ce va fi utilizat în viitor.

5.4.1 Microprocesoare cu o singură unitate de prelucrare. Caracteristici generale.

Primele procesoare ARM au fost realizate de către compania Acorn Computer Group. Scopul iniţial al acestei arhitecturi a fost construirea unor procesoare cu consum redus de energie şi cu performanţe ridicate în acelaşi timp. Ulterior Acorn împreună cu Apple Computer a pus bazele companiei Advanced RISC Machines Ltd. Aceasta nu realizează fizic procesoare ci doar dezvoltă arhitectura pentru ele.

Procesoarele ce au ca fundament ARM7 sunt procesoare de tip RISC bazate pe arhitectură de tip Von Neumann sau Harvard, cu structuri de tip pipeline (bandă de asamblare) ce au ca şi caracteristică de bază simplitatea fără a pierde din performanţă şi cu un consum de energie redus. Astfel de procesoare se pretează cel

mai bine scopului propus în această lucrare, mai mult, datorită consumului redus pot fi utilizate în telefonia mobilă.

O variantă îmbunătăţită a clasicei arhitecturi ARM7 este procesorul ARM7TDMI-S. Acesta aduce în plus modul Thumb (caz în care se înjumătăţeşte dimensiunea unei instrucţii fără a afecta performanţa), facilităţi în plus legate de depanarea codului precum şi o unitate aritmetică şi logică mai dezvoltată şi mai rapidă [4].

Punctul forte al acestei arhitecturi este banda de asamblare. Aceasta este formată din 3 stagii: încărcarea, decodificarea şi execuţia instrucţiunii. Performanţele cele mai ridicate oferite de banda de asamblare sunt atunci când se operează pe cod liniar, astfel că majoritatea instrucţiunilor pot fi executate într-un singur ciclu maşină. În cazul apariţiei unei instrucţiuni de salt pipeline-ul o tratează printr-o tehnică de tip flush and refill (pipeline-ul se goleşte complet). Pentru a evita aceste situaţii când performanţa este serios degradată, arhitectura pune la dispoziţie un set de instrucţiuni ce ajută la evitarea salturilor, şi anume un set de instrucţiuni cu condiţie. Acest tip de instrucţiuni se execută normal în cazul unei condiţii adevărate, iar în cazul unei condiţii false acestea sunt înlocuite cu instrucţiuni de tip NOP (No Operation). Prin aceasta banda de asamblare nu se goleşte crescând astfel performanţa. Din acest motiv aici nu sunt întâlnite clasicele hazarde de date întâlnite în benzile de asamblare cu mai multe stagii.

Arhitectura ARM pune la dispoziţie 16 registre generale (R0 – R15) pe 32 biţi, unde R13-R15 au funcţii speciale. Dintre acestea, R13 (SP – stack pointer), R14 (LR– link register) – poartă numele de registru de încărcare, R15 (PC – program counter) este registrul numărător de program. R14 este folosit pentru a salva numărătorul de programe în momentul unui apel de subrutină făcând posibilă întoarcerea din apel. Existenţa registrului LR oferă o facilitate ce reduce mult timpul de execuţie în momentul în care se face apel de subrutină, nefiind nevoie în acest caz de a se salva conţinutul registrului PC pe stivă aşa cum se face în situaţiile clasice. Se recurge în schimb la metode obişnuite de salvare în stivă doar atunci când se face apel de subrutină din interiorul unei alte subrutine. O altă facilitate a arhitecturii este aceea că registrele speciale gen numărător de program, stack pointer, registru de încărcare sunt considerate registre generale şi astfel pot fi folosite ca argumente în orice instrucţiuni fără nici un fel de restricţii.

Pe lângă setul de 16 registre arhitectura mai dispune de un registru de dimensiune 32 biţi numit registru de stare (CPSR – Current Program Status Register) ce conţine diferite fanioane care indică şi controlează modul de funcţionare al procesorului.

Procesoarele ARM7 prezintă mai multe moduri de lucru: System & User – mod utilizator, FIQ (fast interrupt) – mod ce intră în operare în momentul unei întreruperi rapide de tip FIQ, Supervisor – mod de lucru ce oferă privilegii maxime, Abort – mod ce se declanşează la o eroare internă, IRQ – mod ce întră în operare în momentul unei întreruperi clasice IRQ, Undefined Instruction – mod ce apare când se decodifică o instrucţiune necunoscută.

Comutarea între aceste moduri de lucru se poate face explicit prin cod dar poate apărea şi în cazul unor evenimente speciale gen întrerupere rapidă sau instrucţiune nedefinită după care automat se comută în modul ce era stabilit înainte de eveniment. De exemplu, în cazul în care procesorul operează în modul supervizor şi se generează o întrerupere rapidă (FIQ) acesta comută automat în modul respectiv şi sare apoi la rutina de tratare a întreruperii. La ieşirea din această rutină procesorul comută înapoi în modul supervizor. În cazul unei astfel de comutări în modul de lucru FIQ utilizatorului i se pun la dispoziţie un subset copiat al registrelor

R7-R12, conţinutul anterior schimbării modului de lucru fiind salvat. Practic există mai multe subseturi de registre astfel că în momentul unei schimbări a modului de lucru nu este necesară salvarea acestora în memorie ca şi la procesoarele clasice. De această facilitate beneficiază doar modul de lucru FIQ dar este totuşi prezentă şi la celelalte moduri de lucru, însă restricţionată la registrele R13 şi R14 (SP, PC). Astfel se poate spune ca fiecare mod de lucru are stiva proprie şi numărătorul de program propriu. De asemenea fiecare mod de lucru beneficiază şi de propriul registru CPSR. Procesoarele bazate pe ARM7 folosesc instrucţiuni cu lungime de 32 biţi dar în cazul în care memoria de program este insuficientă se poate opta în detrimentul performanţei la un set de instrucţiuni cu lungimea unei instrucţiuni de 16 biţi. Setul de instrucţii ce este pus la dispoziţie de această arhitectură este unul foarte bogat şi oferă, după cum s-a precizat anterior, mecanisme pentru evitarea instrucţiunilor de salt. După cum se ştie există o mare diferenţă de viteză între nucleul unui procesor şi memoria în care este stocat programul chiar dacă memoria este una extrem de performantă. Arhitectura ARM prezintă anumite mecanisme pentru a rezolva într-o oarecare măsură această situaţie.

În această situaţie în majoritatea cazurilor memoria în care este stocat programul este o memorie de tip FLASH cu un timp de acces de 50 ns limitând astfel procesorul la 20 MHz. Soluţiile clasice în acest caz constau în mare parte în introducerea între memoria FLASH si procesor a unei memorii de tip cache. Acest lucru ar complica prea mult arhitectura procesorului ridicând astfel şi costul acestuia. În cazul arhitecturii ARM se introduce între memoria FLASH şi nucleul procesorului un modul de accelerare numit Memory Accelerator Module (MAM). Ca şi o memorie de tip cache acesta stochează următoarea instrucţiune şi o furnizează procesorului când acesta o cere [TRE05].

Funcţionarea acestui modul este strâns legată de organizarea memoriei FLASH. Aceasta este împărţită în două blocuri întreţesute ce pot fi accesate independent. În acest mod se încearcă furnizarea instrucţiunilor la viteza procesorului. Avantajul arhitecturii este acela că pentru programator modulul MAM este transparent.

Există trei moduri de funcţionare pentru modulul MAM:

- Dezactivat complet (Disabled) – în acest caz modulul este ocolit iar memoria FLASH este accesată direct de către procesor. Astfel, performanţele procesorului sunt limitate de timpul de acces al memoriei.
- Activat parţial (Partially enabled) – în acest caz memoria FLASH este accesată de către modulul MAM dar numai în cazul codului liniar. Instrucţiunile de salt şi datele constante sunt accesate direct de către procesor. Performanţele cresc faţă de modul precedent iar execuţia codului este deterministă în sensul ca se poate garanta un anumit timp de execuţie.
- Activat (Fully enabled) – în acest caz memoria FLASH este accesată doar de către modulul MAM. Ca urmare există şi mecanisme de predicţie în cazul instrucţiunilor de salt şi performanţele sunt superioare modurilor de operare precedente. Totuşi acest mod nu este determinist în sensul că este imposibil să se facă orice analiză a timpului de execuţie al codului.

În [STA09] am adaptat un algoritm steganografic dezvoltat în domeniul spaţial pentru un microprocesor ARM din familia RISC. Rezultatele implementării algoritmului conduc la obţinerea unor soluţii ce permit încorporarea unor mesaje de

dimensiuni relativ mari. Astfel, imaginea obiectului de acoperire şi a obiectului steganografic au o dimensiune de 648 de kbiţi, mesajul ascuns are aceeaşi dimensiune, iar metoda utilizată constă în ascunderea celor mai semnificativi biţi din mesaj în cei mai puţini semnificativi biţi din obiectul de ascundere. Obiectul steganografic rezultat nu prezintă modificări vizibile faţă de obiectul de acoperire. În vederea obţinerii acestor rezultate am făcut adaptările necesare implementării algoritmului utilizat pe microprocesorul existent. Pentru experimentele mele privind implementarea algoritmilor steganografici am folosit o placă de dezvoltare produsă de Olimex (figura 5.1).

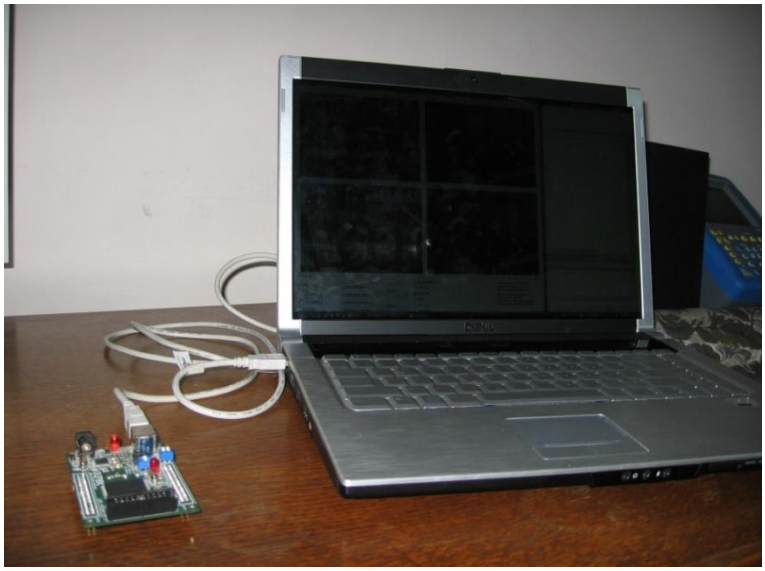


Figura 5.1 Placa de dezvoltare bazată pe microprocesorul ARM7

Modelul plăcii este Olimex LPC-H2294 [5] şi conţine printre altele un microprocesor ARM7 ce poate opera la o frecvenţă de 60 MHz, o memorie SRAM de 1 MB cu timp de acces de 12 ns, memorie FLASH de 4 MB cu timp de acces de 70 ns şi interfeţe de intrare - ieşire. Procesorul dispune de magistrale externe de date, adrese şi control putând astfel adresa o memorie externă. Magistrala externă face parte dintr-un periferic specializat al microcontrolerului cu rolul de a controla memoriile externe conectate la procesor [6].

5.4.2 Microprocesoare cu mai multe unităţi de prelucrare. Caracteristici generale.

Unul dintre microprocesoarele cu mai multe unităţi de prelucrare ce va fi utilizat în telefonia mobilă în viitorul apropiat este microprocesorul ISAAC ce conţine mai multe nuclee de procesare şi este produs de MOVIDIA. Această nouă generaţie de procesoare are ca principal scop oferirea unor performanţe superioare de prelucrare grafică, în special în domeniul jocurilor şi aplicaţiilor video. Procesorul

este astfel conceput încât să fie folosit într-un sistem pe post de coprocesor fiind controlat de către un procesor gazdă, eventual unitatea de procesare ce controlează întregul sistem mobil. În interiorul capsulei se află 8 nuclee de procesare. Dintre acestea 6 sunt identice şi nu pot adresa decât un MB din totalul de memorie, iar al 7-lea are capacitatea de a adresa întreg spaţiul de memorie. Al 8-lea nucleu (LEON) este de tip RISC cu o arhitectură SPARC şi poate adresa de asemenea întreg spaţiul de memorie. Acest nucleu are următoare caracteristici principale: bandă de asamblare cu 7 stagii, unitate specializată de înmulţire şi împărţire, unitate de virgulă flotantă, cache separat pentru instrucţii şi date, unitate dedicată pentru depanarea codului şi mod de lucru cu consum redus. LEON este cel care se ocupă de configurarea celorlalte 7 nuclee având grijă să genereze codul aplicaţiei ce urmează a fi rulat pe ele, să configureze memoria şi să dea startul execuţiei aplicaţiei [7].

Procesorul MOVIDIA ISAAC prezintă performanţe de 27 Gflops la o frecvenţă a tactului până la maxim 200 MHz. Întregul procesor este integrat într-o platformă de test pe care se găseşte microprocesorul ISAAC precum şi câteva periferice, cum ar fi un ecran LCD color, camere video, interfaţă CD şi o interfaţă I2S şi un ecran cu senzor (figura 5.2).

Figura 5.2 Placă de dezvoltare bazată pe microprocesorul ISAAC

În cazul procesării algoritmilor steganografici este de remarcat că prezintă o adevărată provocare chiar şi în cazul rulării pe un calculator personal performant. Algoritmii implică atât putere de calcul mare, dar şi timp de rulare relativ mare. Din acest motiv implementarea acestora pe un procesor cu mai multe nuclee presupune utilizarea unor procedee de paralelizare a lor. Prin încercările făcute am constatat că această operaţie este dificilă şi nu se pretează pentru orice tip de algoritm.

5.4.3 Concluzii privind rezultatele experimentale obţinute prin utilizarea microprocesoarelor propuse în steganografie

Pentru a compara comportarea algoritmilor steganografici pe diferite platforme hardware am conceput un algoritm de ascundere pe biţii cei mai puţini semnificativi ai obiectului de acoperire plecând de la aspectele teoretice prezentate în literatură [KAT00]. Modul în care a fost realizat acest algoritm a trebuit să ţină seama de caracteristicile platformelor pe care a urmat să fie rulat. În acest sens s-a folosit un calculator personal de tipul Hewlett-Packard cu un procesor Intel de 2,4GHz, un sistem de dezvoltare ce are încorporat un microprocesor ARM utilizat în telefonia mobilă şi o platformă de dezvoltare ce are în componenţă microprocesorul ISAAC ce urmează a fi încorporat în viitoarele telefoane iPhone. Pentru efectuarea experimentelor s-a încercat ca cele trei platforme să prezinte frecvenţe de lucru compatibile.

Este de menţionat faptul că în situaţia în care calculatorul execută algoritmul în mod secvenţial, la microprocesorul ARM execuția acestuia trebuie să ţină cont de arhitectura bazată pe banda de asamblare. Microprocesorul ISAAC prezintă particularitatea pe lângă faptul că are o arhitectură bazată pe bandă de asamblare, mai are în componenţă 6 nuclee ce pot procesa algoritmul în paralel coordonate de un nucleu numit LEON. Aceste arhitecturi diferite au impus adaptarea algoritmului steganografic de aşa manieră încât executarea lui să fie cât mai unitară pentru a compara performanţele acestuia pe cele trei platforme.

De remarcat este faptul că pe microprocesorul ARM şi ISAAC nu a mai fost implementat nici un algoritm steganografic până în prezent, iar din acest motiv consider că este prima aplicaţie de acest tip. Mai mult, implementarea algoritmului pe microprocesorul ISAAC a fost cerută de către firma producătoare a acestuia cu intenţia de a fi furnizată ca aplicaţie viitorilor utilizatori de iPhone.

În figura 5.3 se dau două exemple privind rezultatele dezvoltării unor algoritmi steganografici pe cele două microprocesoare ARM şi ISAAC.

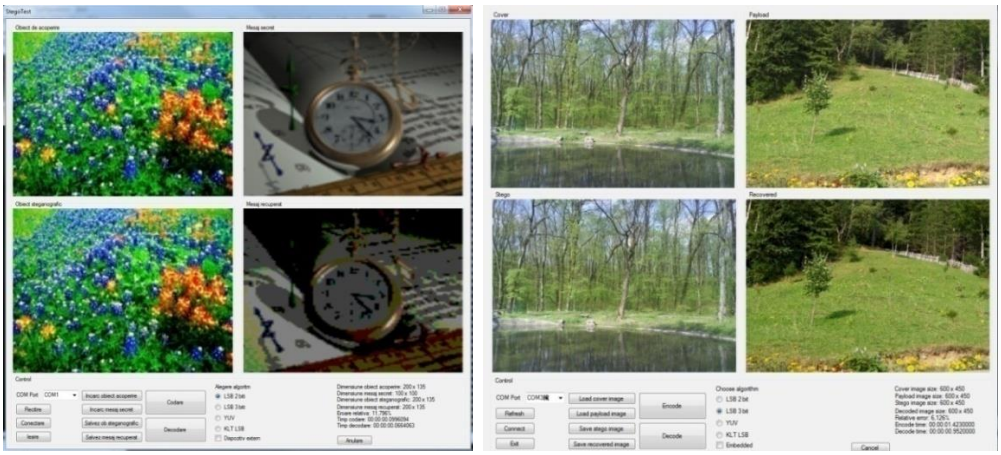


Figura 5.3 Rezultate experimentale obţinute pe microprocesoarele ARM şi ISAAC

Trebuie specificat că spre deosebire de celelalte platforme utilizate pentru comparare, în cazul microprocesorului ISAAC au fost concepute soluţii originale de paralelizare a algoritmului steganografic.

Ca urmare timpul de execuţie pe microprocesorul ISAAC se reduce semnificativ, respectiv de 4 până la 8 ori mai mic faţă de timpul de rulare pe microprocesorul ARM şi de circa 12 până la 18 ori faţă de calculatorul utilizat. Aceste rezultate sunt prezentate în tabelul 5.1 şi figura 5.4.

Tabel 5.1 Compararea timpului de execuţie pentru algoritmul *LSB-*P_2

Nr. crt.	Obiect de acoperire		Mesaj secret		PC	ARM	ISAAC
	Nume	Dimensiune(bytes)	Nume	Dimensiune(bytes)	[ms]	[ms]	[ms]
1	camp_cu_flori.jpg	81.000	porumbel.jpg	33.930	70	25	3,66
2	camp_cu_flori.jpg	81.000	ceas_2.jpg	45.450	72	25	3,66
3	camp_cu_flori.jpg	81.000	ceas_3.jpg	81.000	73	25	3,66
4	lac_3.jpg	202.500	porumbel.jpg	33.930	161	63	8,55
5	lac_3.jpg	202.500	ceas_3.jpg	81.000	160	63	8,55
6	lac_3.jpg	202.500	ceas_4.jpg	182.700	162	63	8,55
7	lac_2.jpg	360.000	porumbel.jpg	33.930	280	112	14,9
8	lac_2.jpg	360.000	ceas_3.jpg	81.000	276	112	14,9
9	lac_2.jpg	360.000	ceas_4.jpg	182.700	269	112	14,9
10	lac_2.jpg	360.000	peisaj_1.jpg	360.000	289	112	14,9
11	lac_1.jpg	810.000	porumbel.jpg	33.930	613	253	33,6
12	lac_1.jpg	810.000	ceas_3.jpg	81.000	616	253	33,6
13	lac_1.jpg	810.000	ceas_4.jpg	182.700	615	253	33,6
14	lac_1.jpg	810.000	peisaj_1.jpg	360.000	605	253	33,6
15	lac_1.jpg	810.000	peisaj_2.jpg	562.500	618	253	33,6
16	lac_1.jpg	810.000	peisaj_1.jpg	810.000	630	253	33,6

În tabelul 5.1 am ales pentru exemplificare o parte din testele efectuate pe cele trei platforme. În prima şi a treia coloană se specifică numele obiectelor şi mesajelor secrete folosite, în coloana a doua şi a patra se prezintă dimensiunile imaginilor exprimate în octeţi, iar în ultimele trei coloane se regăsesc timpii de execuţie în milisecunde pentru algoritmul rulat, ce urmează a fi prezentat mai pe larg în capitolul 7. De menţionat că o parte din testele efectuate pe cele trei platforme se regăsesc şi în capitolele 7, respective 9, iar rezultatele obţinute conduc la aceleaşi concluzii ca şi cele din acest capitol.

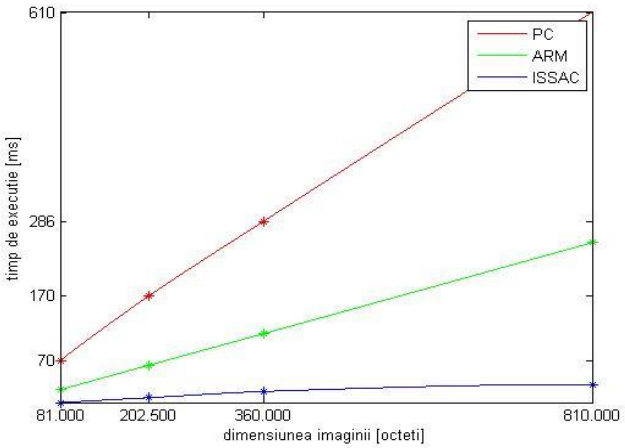


Figura 5.4 Reprezentarea grafică a timpilor de execuţie pentru algoritmul *LSB-P_2*

Urmărind tabelul de mai sus şi figura 5.4 se poate constata că timpul de execuţie al algoritmului steganografic este semnificativ influenţat de dimensiunea imaginii de acoperire. Aşadar, cu cât aceasta are dimensiuni mai mari şi timpul de execuţie creşte. Însă este de observat faptul că dacă pe celelalte două platforme timpul de execuţie creşte proporţional cu dimensiunea obiectului de acoperire, respectiv de la 1 la 10, la microprocesorul ISAAC această creştere este doar de la 1 la 6 pentru dimensiuni ale obiectului de acoperire cu creştere de la 1 la 10. Acest rezultat confirmă faptul că paralelizarea algoritmului steganografic conduce la o îmbunătăţire substanţială a timpului de execuţie şi validează soluţiile alese.

5.5 ***Concluzii***

În cadrul acestui capitol a fost făcută o trecere în revistă a principalelor realizări în domeniul steganografiei bazată pe implementare hardware având ca suport circuite integrate, arii programabile, respectiv exploatarea unor facilităţi de care beneficiază actualele telefoane mobile. În prezent algoritmii steganografici cablaţi şi integraţi într-un circuit putem spune că reprezintă o opţiune de viitor fiind foarte puţin abordată din punct de vedere practic. Poate o soluţie integrată să fie de actualitate în viitorul apropiat pe măsură ce cerinţele pieţei îşi vor spune cuvântul.

Din punct de vedere al cercetării o astfel de abordare a fost tratată cu multă timiditate existând poate o explicaţie legată de faptul că steganografia este un domeniu de curând abordat pe scară mai largă, iar o soluţie steganografică care să se impună în acest moment faţă de altele ar trebui să implice o validare a valabilităţii ei. Poate în acest sens să se stabilească eventual un standard pe baza căruia să se poată concepe un circuit integrat dedicat steganografiei.

Până la găsirea unei astfel de soluţii o serie de cercetători au folosit ca unealtă de lucru pentru implementarea unor algoritmi steganografici ariile programabile fie pentru a verifica unele aspecte legate de soluţiile abordate în domeniul steganografiei, fie de a testa valabilitatea vreunui algoritm propus de ei şi

care să fie adaptabil configuraţiei platformei deţinute de aceştia. Sigur că o astfel de soluţie poate fi abordată din punct de vedere al cercetării, dar din punct de vedere al obţinerii unui astfel de produs este o direcţie a cărei finalizare este mai greu de aşteptat, în primul rând din motivul că ariile programabile necesită costuri mari, însă pot constitui în continuare unelte utile de lucru.

În continuarea capitolului am abordat o perspectivă cu totul nouă în sensul dorinţei de a utiliza facilităţile microprocesoarelor folosite în telefonia mobilă şi totodată având în vedere cerinţele pieţei de a exista un produs steganografic cu posibilităţi de încorporare într-un telefon mobil. În acest sens pornind de la cerinţele manifestate de către un producător de microprocesoare ce vor fi utilizate în viitoarele generaţii de telefoane mobile, am direcţionat tema mea de cercetare în ideea satisfacerii acestor cerinţe.

Astfel, în acest capitol am prezentat rezultatele experimentelor efectuate pe o parte din algoritmii concepuţi de mine pe două platforme dintre care una are încorporat un microprocesor utilizat în prezent în telefonia mobilă, respectiv a doua un microprocesor ce va fi utilizat în viitor în telefonia mobilă. Rezultatele experimentale obţinute pe cele două platforme au fost comparate cu executarea aceloraşi algoritmi pe un calculator personal. Menţionez că ultimul microprocesor se găseşte în etapa de testare în cadrul firmei producătoare.

Scopul urmărit a fost multiplu, în sensul că s-a dorit a se identifica algoritmii cei mai performanţi realizaţi de mine ce pot fi implementaţi pe astfel de microprocesoare şi de a se găsi soluţiile cele mai potrivite pentru adaptarea acestora la arhitectura microprocesoarelor propuse a fi utilizate în telefonia mobilă. Totodată s-a urmărit optimizarea acestora în vederea obţinerii unor timpi de execuţie cât mai mici. În final s-au analizat performanţele din punct de vedere steganografic ale acestora. Evidenţiez faptul că o astfel de abordare nu am identificat a mai fi abordată în literatură.

Consider că scopul ce mi l-am propus a fost atins dovedind în primul rând valabilitatea performanţei algoritmilor propuşi, cât şi posibilitatea ca aceştia să facă parte dintr-un viitor produs.

6 MODELE STEGANOGRAFICE

6.1 *Model clasic*

Pentru a avea o viziune şi o înţelegere mai bună asupra steganografiei, în cele ce urmează se face referire la modelul clasic pentru comunicarea invizibilă, propus de Simmons ca "Problema prizonierilor". [SIM84]

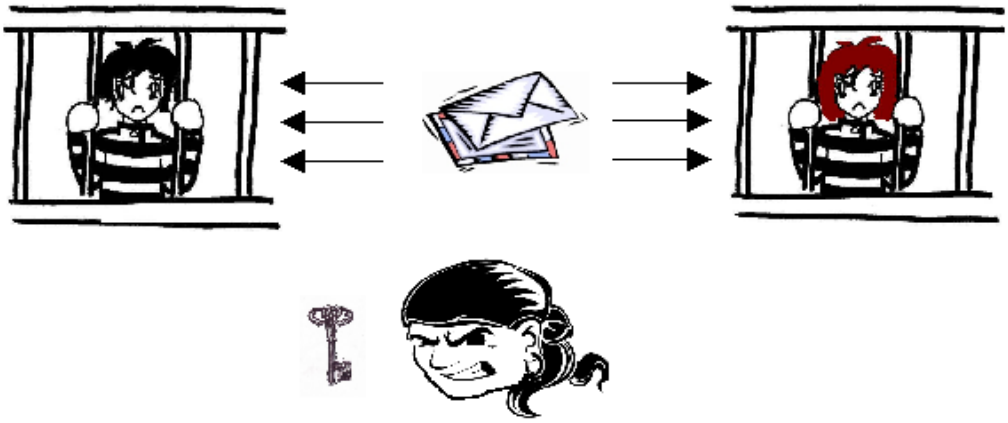


Figura 6.1 Modelul clasic steganografic "Problema prizonierilor"

După cum se observă în figura 6.1 Simmons pleacă de la premisa ca Alice si Bob sunt arestaţi datorită unor infracţiuni comise şi sunt repartizaţi în celule diferite. Aceştia doresc să realizeze un plan de evadare. Comunicarea dintre cei doi este posibilă doar prin intermediul unui gardian, numit Wendy, care nu le permite comunicarea prin codare. În cazul în care observă orice tip de comunicare suspicioasă, îi va încarcera, astfel eliminând orice tip de schimburi de mesaje. Soluţia aleasă de cei doi constă în ascunderea mesajului într-o informaţie la vedere inofensivă. De exemplu, Alice ar putea să primească de la Bob un desen pictat în care este reprezentat un câmp cu florile ei preferate. Acest mesaj pentru gardian ar fi doar o operă de artă, în timp ce pentru Alice codificarea culorilor reprezintă informaţia valoroasă, mesajul secret constând chiar într-un plan de evadare.

Modelul prezentat este aplicat în general în situaţiile în care are loc comunicarea invizibilă şi anume steganografia. Cei doi protagonişti din exemplul de mai sus, Alice si Bob se identifică cu cele două părţi care doresc să comunice şi să schimbe informaţii secrete într-un mod invizibil, iar gardianul poate fi considerat atacatorul ce încearcă să intercepteze şi să extragă mesajul ascuns.

Cu toate ca mesajul secret este ascuns, părţile care comunică trebuie să ia în permanenţă în calcul şi interferenţa unui atacator, care în funcţie de intenţiile ce le are poate fi pasiv, activ sau rău voitor. În exemplul propus, Simmons face încă o presupunere pentru a explica mai bine mecanismul pe care se bazează comunicarea invizibilă, steganografia. Această presupunere constă în posibilitatea schimbării

mesajelor în diferite formate cum ar fi text, imagini digitale sau sunet digital, Alice si Bob având acces în celulele lor la sisteme computerizate. Chiar si acest mod de comunicare nu presupune lipsa potenţialilor atacatori.

6.2 *Model de bază propus pentru un sistem steganografic*

În urma analizei "Problemei prizonierilor" [SIM84], în literatura de specialitate [KUR92, ZOL98, CAH04, KHA06] s-a adoptat modelul de comunicare steganografică prezentat în figura 6.2.

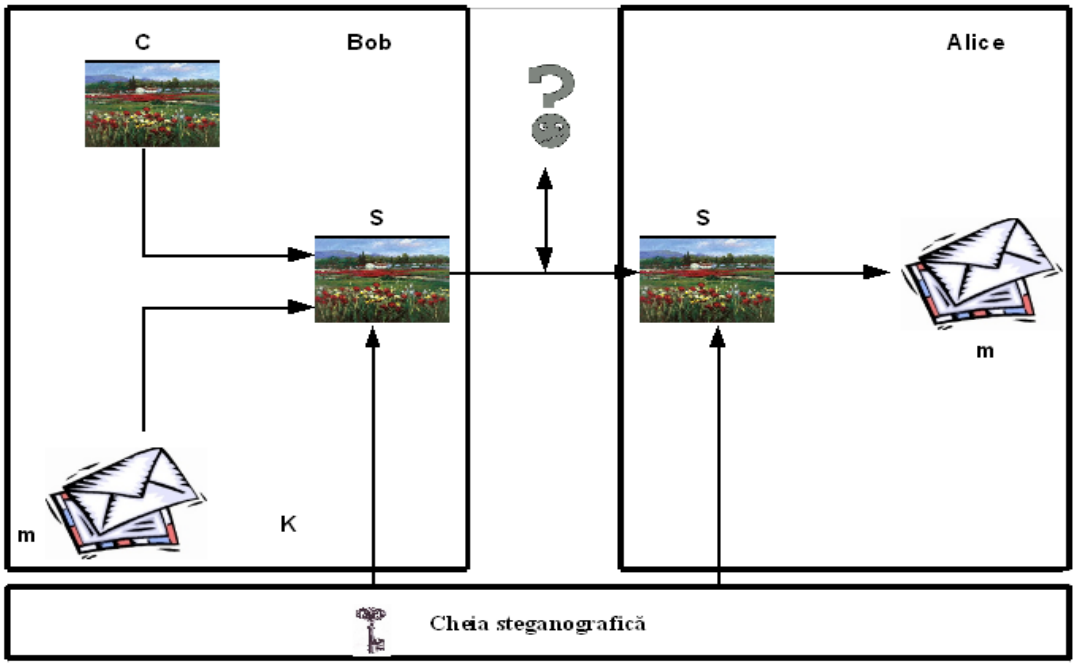


Figura 6.2 Model particularizat al "Problemei prizonierilor"

La analizarea acestui model se poate observa apariţia unor termeni abstracţi. În continuare se prezintă semnificaţia acestor termeni, făcând referire şi la exemplul prizonierilor. Se notează cu „m" mesajul secret pe care Bob doreşte să-l transmită lui Alice. Pentru aceasta are nevoie de un mesaj inofensiv în care să-l ascundă, denumit în continuare obiect de acoperire, notat cu „c".

Pentru a creşte securitatea transmiterii informaţiei private, se poate apela la folosirea unei chei secrete notată cu „k" denumită în continuare cheie steganografică. Aceasta este cunoscută de ambii parteneri în procesul de comunicare şi are rolul de a coda şi decoda mesajul secret. Mesajul rezultat în urma procesului de încorporare şi codare reprezintă obiectul steganografic şi este notat cu „s". În urma procesului de ascundere a unui mesaj secret „m" într-un obiect de acoperire „c" este necesar ca acesta să nu se deosebească de obiectul steganografic rezultat „s". Dacă este îndeplinită această condiţie se poate spune că sistemul steganografic şi-a atins scopul.

Modalitatea prin care sunt transmise informaţiile între cei doi protagonişti este reprezentată de canale nesecurizate, care au fost simbolizate în exemplul de mai sus prin gardianul Wendy. Singurii care înţeleg mesajul ascuns „m" sunt cei doi care comunică: emiţătorul, care ascunde şi codifică mesajul şi receptorul, care este capabil să preia şi să decodifice mesajul ascuns. Bineînţeles că obiectul de acoperire „c" care reprezintă interfaţa pentru mesajul secret poate fi de orice tip de date: text, sunet, imagine, etc. Securitatea şi calitatea transmiterii de informaţii secrete constă în abilitatea celor ce transmit mesaje secrete într-o aşa manieră încât să nu existe o distincţie sesizabilă între obiectul de acoperire şi obiectul steganografic.

Este de preferat ca obiectul de acoperire să conţină informaţii suplimentare, proporţional ca şi număr cu datele secrete care se doresc a fi ascunse, deoarece aceste date suplimentare pot fi înlocuite cu informaţiile secrete. Un exemplu elocvent îl reprezintă zgomotele care apar inerent datorită proceselor fizice. Chiar dacă sunt nedorite, datorită toleranţelor pe care le impun sistemelor, ele totodată pot constitui o modalitate de transmitere a mesajelor steganografice. Într-un mesaj pot fi introduse semnale suplimentare care să conţină informaţie secretă şi care pentru un observator să fie interpretate ca simple zgomote, dar aceasta trebuie să se facă într-un mod controlat, pentru că ar putea exista cazul în care se adaugă zgomot suplimentar la cel deja existent într-un obiect de acoperire ceea ce ar putea duce la descoperirea procesului steganografic.

În cele prezentate anterior s-a făcut o trecere în revistă a principiilor steganografice de bază prin explicarea termenilor aferenţi domeniului cu exemplificări elocvente ale acestora. În continuare vor fi abordate mai în detaliu cele mai reprezentative modele steganografice existente până în prezent.

6.3 *Model încorporat*

Transmiterea unui mesaj steganografic presupune parcurgerea unor etape bine definite ce presupun folosirea unor algoritmi matematici specifici care sunt implementaţi atât la încorporarea mesajului secret cât şi la extragerea lui. Aceşti algoritmi vor avea ca date de intrare un mesaj secret, un obiect de acoperire şi eventual o cheie secretă. În cazul în care se foloseşte o cheie secretă pentru codarea datelor ce urmează a fi transmise, aceasta este cunoscută atât emiţătorului cât şi receptorului de mesaj. Informaţia rezultată din acest proces constituie obiectul steganografic. La recepţie, mesajul primit urmează a fi decodificat cu ajutorul aceleiaşi chei având ca rezultat obţinerea mesajului secret şi, ca informaţie secundară, obiectul de acoperire.

Sistemele steganografice pot fi fundamentate matematic în diferite moduri. În [ZOL98] a fost formalizat aşa numitul "model încorporat" şi este prezentat în figura 6.3.

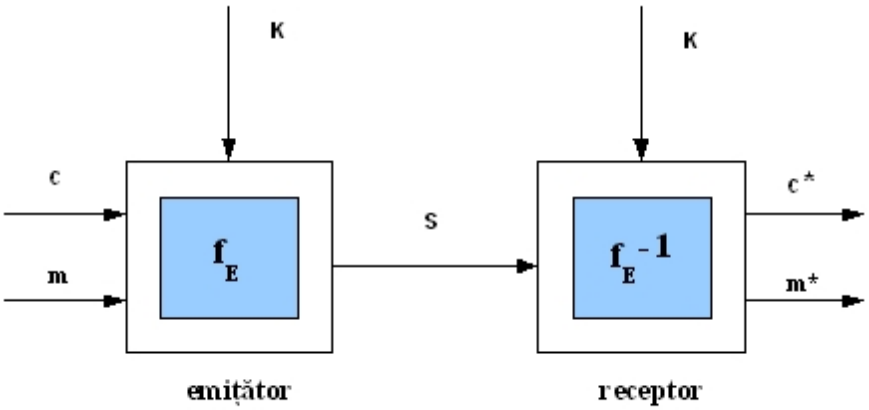


Figura 6.3 Model încorporat [ZOL98]

"Problema prizonierilor" prezentată de Simmons drept modelul clasic steganografic[SIM84] este abstractizată prin modelul propus în [ZOL98]. O primă observaţie este că cei doi protagonişti sunt acum reprezentaţi prin denumirile de "emiţător" şi "receptor".

Emiţătorul se exprimă printr-o funcţie matematică directă f_E, iar receptorul prin funcţia matematică inversă f_E^{-1}. Cele două funcţii matematice f_E şi f_E^{-1} folosesc algoritmi steganografici pentru a codifica şi decodifica mesajul secret. Formalizând, se poate spune că f_E reprezintă funcţia de "încorporare" a datelor secrete. Funcţia matematică f_E^{-1} este utilizată la recepţia mesajului şi are rolul de a decodifica informaţia primită , aceasta realizând funcţia de „extragere" a informaţiei secrete.

Modelul propus are ca şi date de intrare un obiect de acoperire "c" care constituie mesajul inofensiv. Tot la intrare se află şi funcţia de codare f_E, care prelucrează datele secrete „m" şi le încorporează în „c". În urma acestor operaţii se formează mesajul steganografic „s" care va fi transmis. Evident că acesta conţine deja, mesajul secret „m". Până în acest moment s-a făcut referire la datele de intrare si la modalitatea de prelucrare a acestora.

Pentru a decodifica mesajul de la ieşire se face apel la funcţia f_E^{-1} care extrage datele încorporate. După această etapă vor rezulta doi termeni: „m^{*}" şi „c^{*}", iar dacă decodarea este corectă „m^{*}" ar trebui să fie egal cu „m".

Ideile expuse până acum au avut rolul de a explica funcţionalitatea principiului steganografic folosind doar datele reprezentate în figura 6.3. Acest fapt nu include o evaluare calitativă a modului prin care informaţia secretă este securizată sub obiectul de acoperire „c".

Analiza siguranţei sistemului steganografic presupune şi existenţa unui eventual atacator. Drept urmare, presupunerile făcute şi logica formulată nu sunt utile în cazul în care se doreşte să se evalueze calitatea ascunderii informaţiei.

Modelul propus poate fi comparat cu un sistem la care sunt cunoscute intrările şi ieşirile, dar nu este luat în calcul modul de procesare a datelor de către un eventual interceptor.

[ZOL98] exemplifică şi urmăreşte să demonstreze cu ajutorul teoriei informaţiei cazul în care un sistem steganografic are cele mai mari şanse să fie sigur. Pentru aceasta pleacă de la presupunerea că un atacator are informaţii atât despre obiectul steganografic „s" rezultat în urma încorporării, cât şi despre obiectul de acoperire „c" în care a fost ascuns mesajul secret „m" şi demonstrează că în acest caz sistemul steganografic nu poate fi sub nici o formă sigur. Pentru a îmbunătăţi această situaţie defavorabilă propune un set de posibilităţi de realizare a unui obiect de acoperire dat, astfel încât prin acest mod induce în eroare un eventual atacator deoarece acesta nu are acces la forma originală a obiectului de acoperire şi în acest fel este mult mai greu de a depista unde a fost ascuns mesajul secret.

Aşadar, dacă se doreşte a avea o transmitere de informaţie secretă reuşită, este necesar ca atacatorul să nu poată face diferenţa între mesajul „s" rezultat după prelucrarea datelor „c" cu ajutorul funcţiei f_E. Sistemul steganografic nu este sigur în cazul în care funcţia f_E permite atacatorului să observe diferenţe între „s" şi „c".

Un sistem steganografic presupune prelucrarea datelor de intrare (*c, m* şi *k*) prin intermediul funcţiei f_E în modul următor [ZOL98]:

$$s = f_E(c, m, k) \tag{6.1}$$

Asupra diferitelor date de intrare sau ieşire corespunzătoare unui sistem steganografic pot exista incertitudini ce pot fi evaluate cu ajutorul unei mărimi denumită entropie. Entropia reprezintă gradul de dezordine sau de dispunere aleatoare a elementelor dintr-un sistem care conţine energie sau informaţie.

Principiul steganografiei se referă la ascunderea unei informaţii secrete într-o informaţie oarecare astfel încât acest proces să treacă neobservat atât de ochiul uman cât şi de programele de detecţie şi protecţie ale unui calculator. În acest sens entropia prezintă o metrică importantă de care se poate ţine seama în evaluarea securităţii transmiterii unei informaţii într-un proces steganografic. Există diferite metode prin care o informaţie secretă poate fi încorporată în alta, dar toate acestea implică o modificare atât a mesajului ascuns, cât şi a obiectului de acoperire în care a fost ascuns. Entropia informaţiei măsoară schimbările ce au loc în cadrul obiectelor implicate într-un proces steganografic. Pentru ca informaţia secretă să nu fie detectată de un eventual atacator, este foarte important ca entropia obiectului steganografic la care acesta poate avea acces să fie cât mai apropiată de cea a obiectului de acoperire.

În [ZOL98] se face o analiză abstractă a siguranţei unui sistem steganografic prin evaluarea gradului entropiei rezultate în urma modificărilor ce au loc atât în mesajul secret ce urmează a fi încorporat, cât şi în obiectul steganografic rezultat. În cele ce urmează se face o paralelă a acestui caz particular, cu definirea entropiei în conformitate cu teoria informaţiei.

În acest sens, se consideră că pentru un set de valori $\{x_1, \ldots x_n\}$ entropia elementului X, notată cu $H(X)$ descrie "incertitudinea asociata lui X". De asemenea, entropia poate fi văzută şi ca şi cantitatea de informaţie pe care o conţine X.

Pentru exemplificare se prezintă în figura 6.4. diagrama ce exprimă legătura dintre entropiile a două elemente X şi Y.

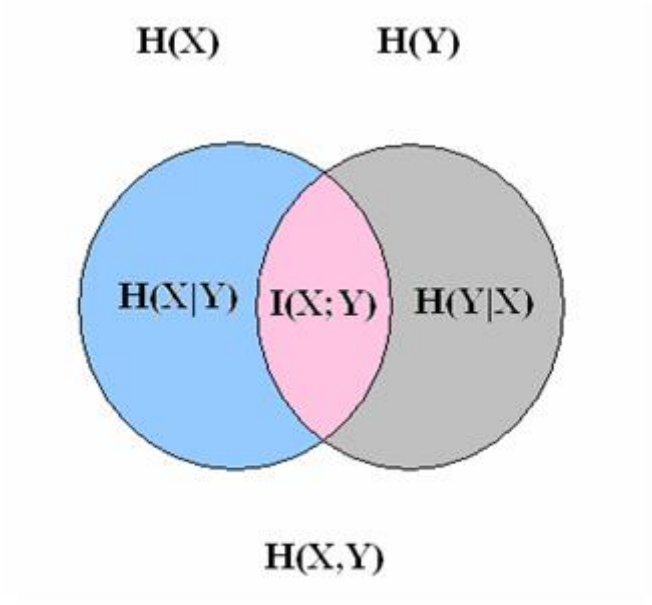


Figura 6.4 Diagrama entropiilor [BOR05]

Entropia condiţională $H(X|Y)$ rămâne incertitudinea lui X când este cunoscut Y.

Entropia de legătură este suma dintre entropia condiţională şi incertitudinea asociată elementului X [BOR05]:

$$H(X,Y) = H(X) + H(Y|X) \tag{6.2}$$

Informaţia mutuală $I(X;Y)$ descrie volumul informaţiei aflate despre Y dacă se obţine X:

$$I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) \tag{6.3}$$

Prin particularizarea celor două elemente X şi Y cu obiectele implicate într-un proces steganografic C respectiv S autorii fac o serie de presupuneri în ceea ce priveşte cunoştinţele şi abilităţile unui atacator de succes şi iau în calcul toate rezultatele raportate la gradul de modificare a entropiei unui element în urma încorporării de informaţie suplimentară. Pentru obţinerea rezultatelor se ia în considerare analiza a două tipuri de sisteme: deterministe şi nedeterministe.

O caracteristică a sistemelor steganografice deterministe este faptul că se pleacă de la presupunerea că atacatorul cunoaşte atât obiectul de acoperire „c" cât şi obiectul steganografic „s" obţinut în urma încorporării mesajului secret „m". Fiind vorba de un model abstract, „c" este exprimat la modul general, fiind asimilat cu o mulţime de obiecte de acoperire, notate cu C , acelaşi principiu fiind valabil şi pentru mulţimea obiectelor steganografice S . Pentru ca procesul de ascundere să nu fie identificat este necesar ca la o simplă comparaţie făcută de un observator cele

două obiecte să pară identice. Din punct de vedere matematic, dacă două elemente sunt egale se presupune că şi entropiile lor sunt egale, astfel că:

$$S = C \Rightarrow H(S) = H(C) \tag{6.4}$$

Autorii din [ZOL98] demonstrează că acest lucru este imposibil de realizat deoarece adăugarea de informaţie suplimentară într-unul din obiecte duce la creşterea entropiei acestuia şi astfel nu poate fi îndeplinită condiţia de securitate impusă, prin care diferenţa dintre entropiile celor două elemente supuse comparării să fie zero.

Condiţia de securitate care ar trebui îndeplinită pentru ca sistemul steganografic să fie sigur este:

$$H(S|C) = H(C|S) = \mathbf{0} \tag{6.5}$$

Dar, datorită faptului că există totuşi informaţie încorporată în „C" rezultă:

$$H(S|C) = H(C|S) > \mathbf{0} \tag{6.6}$$

Ca urmare, se poate spune că nu este îndeplinită în totalitate condiţia de securitate.

Din aceasta rezultă că un sistem steganografic determinist nu poate fi sigur atunci când un atacator cunoaşte S şi C .

În sistemele steganografice nedeterministe se aleg obiecte de acoperire inofensive C în care se ascund informaţii secrete M rezultând astfel obiecte steganografice S ce sunt vizibile şi sunt transmise pe canale publice, putând fi astfel interceptate şi chiar atacate de persoane neautorizate. Astfel, analiza siguranţei unui sistem steganografic considerat nedeterminist de astă dată, pleacă de la presupunerea că orice obiect de acoperire C are la dispoziţie o Sursă notată cu C_S din care poate fi realizat în diferite moduri. Obiectul de acoperire se obţine din această Sursă în urma unor procedee de transformare care introduc mici perturbări aleatoare în rezultat. Chiar dacă se cunoaşte Sursa şi procedeul de transformare, de către un eventual atacator, mai multe realizări succesive vor genera rezultate diferite.

Pentru ca sistemul steganografic să fie sigur este necesar ca atacatorul să nu obţină nici un fel de informaţie despre mesajul ascuns M la examinarea Sursei C_S, respectiv S . Autorii din [ZOL98] demonstrează faptul că atâta timp cât nu se poate obţine obiectul de acoperire original în care a fost ascuns mesajul pentru a-l compara cu obiectul steganografic rezultat, poate fi îndeplinită condiţia fundamentala a securităţii sistemului steganografic pentru cazul de faţă.

$$H\big(M\big|(S, C_S)\big) = H(M) \tag{6.7}$$

Din punct de vedere matematic relaţia (6.7) exprimă faptul că entropia mesajului secret $H(M)$ nu trebuie să se micşoreze la aflarea lui S şi C_S. Altfel spus, pentru a avea un proces steganografic îndeplinit cu succes este absolut necesar ca incertitudinea lui C să fie mai mare decât entropia indusă de mesaj în tot sistemul.

$$H\big(C\big|(S, C_S)\big) \geq H(M) \tag{6.8}$$

Rezultă din cele prezentate mai sus că sistemele steganografice nedeterministe devin sigure atunci când atacatorul nu cunoaşte obiectul de acoperire C chiar dacă are acces la obiectul steganografic S . Întreaga tehnologie privind generarea obiectelor steganografice constă în furnizarea unor informaţii cât mai reduse eventualilor atacatori. Cele mai sigure sisteme steganografice rezultate pe baza analizei gradului de securitate sunt sistemele steganografice nedeterministe

care printr-o metodă de randomizare furnizează obiectul de ascundere realizat într-un mod aleator şi de preferat să fie adecvat mesajului ce urmează a fi ascuns.

În concluzie, în [ZOL98] se consideră că eventualii atacatori pot avea acces doar la obiectul steganografic. Ca urmare orice prelucrare de informaţii ce ar putea avea loc înaintea transmiterii obiectului steganografic poate conduce la o îmbunătăţire a procesului. În acest scop, fără a face o demonstraţie teoretică, ci doar bazându-se pe deducţie logică, autorii propun adăugarea unei funcţii de preprocesare asupra obiectului de acoperire introdusă înaintea generării acestuia.

6.4 *Model probabilistic*

Pentru dezvoltarea unui model steganografic cu un grad ridicat de securitate în [CAH04] se presupune că un atacator are putere de calcul nelimitată şi este capabil să efectueze o varietate de atacuri. Dacă acesta nu poate să confirme ipoteza lui că obiectul testat conţine mesaj secret, atunci sistemul este teoretic sigur.

Cachin ridică problema securităţii unui sistem steganografic plecând de la presupunerea că emiţătorul are la dispoziţie un set de obiecte de acoperire în care încorporează în mod aleator informaţie secretă şi le trimite către receptor. În acest mod, un eventual atacator care interceptează informaţiile transmise astfel pe un canal nesecurizat nu poate stabili care dintre ele conţin mesaj secret şi care nu. Practic acesta nu poate deosebi obiectele steganografice care conţin date secrete faţă de obiectele de acoperire simple trimise doar pentru a-l induce în eroare.

Pentru a face o analiză a securităţii sistemului steganografic în acest caz Cachin consideră că unui obiect de acoperire C îi corespunde distribuţia de probabilitate P_C, iar prin încorporarea unui mesaj în acesta rezultă un obiect steganografic S cu distribuţia de probabilitate P_S.

În cazul în care introducerea mesajului modifică distribuţia de probabilitate, adică P_S devine diferit de P_C, atunci această diferenţă poate da un semnal de alarmă atacatorului. Autorul presupune că deşi atacatorul nu cunoaşte obiectul de acoperire, cunoaşte distribuţia de probabilitate a acestuia P_C şi funcţia de ascundere a mesajului.

Securitatea perfectă a unui sistem steganografic este definită în [CAH04] pe baza entropiei relative $D(P_C||P_S)$ care este o măsură a diferenţei dintre distribuţiile de probabilitate a obiectelor ce caracterizează procesul de ascundere.

Astfel condiţia care trebuie îndeplinită pentru a obţine un sistem steganografic perfect sigur este ca:

$$D(P_C||P_S)=0 \tag{6.9}$$

Practic, autorul admite că entropia relativă $D(P_C||P_S)$ poate să nu fie 0, ci mai mică decât un ε dat.

$$D(P_C||P_S) \leq \varepsilon \tag{6.10}$$

În acest caz denumeşte sistemul steganografic ε sigur.

Dacă este îndeplinită această condiţie un atacator nu poate stabili din punct de vedere probabilistic dacă obiectul ce-l interceptează este obiect de acoperire sau obiect steganografic. Acest lucru nu poate sa-l facă nici receptorul, iar pentru a rezolva această problemă autorul presupune că acesta are acces la un oracol care îi spune când emiţătorul este activ şi când nu. În cazul în care distribuţiile de probabilitate a celor două obiecte sunt egale, din punct de vedere statistic informaţia existentă în acestea este distribuită la fel în ambele cazuri (cu şi fără

mesaj secret). În cazul în care atacatorul are cunoştinţă de distribuţia de probabilitate P_C şi entropia relativă este mai mare decât 0, îi induce acestuia un grad de suspiciune deoarece observă că cele două distribuţii sunt diferite. Acest fapt îl poate determina să bănuiască existenţa unui mesaj ascuns. Din acest motiv, cazul ideal pentru ca un sistem steganografic să fie sigur este ca distribuţiile de probabilitate P_C şi P_S ce corespund celor două obiecte C şi S să nu poată fi deosebite.

Pentru a demonstra existenţa unui astfel de sistem, precum si pentru a încerca eliminarea noţiunii de oracol, se propun două exemple în [CAH04], dar aceste exemple se bazează pe reprezentarea unui mecanism criptografic. Putem spune că exemplificările făcute fac referire mai mult la criptografie decât la steganografie în sensul clasic al cuvântului.

Cachin remarcă faptul că un sistem steganografic poate fi sigur din punctul de vedere al teoriei probabilităţilor ca urmare a analizării modelului propus, dar în realitate un asemenea model face abstracţie de mediile purtătoare utilizate în mod practic la realizarea obiectelor steganografice. Acestea au o distribuţie de probabilitate mai complexă, nu sub forma ideală cum este considerat în [CAH04]. Ca exemplu, într-o imagine aleasă ca şi obiect de acoperire probabilitatea ca toţi pixelii din imagine să aibă aceeaşi culoare tinde la 0. Cum cele mai utilizate medii pentru steganografie rămân obiectele text, audio, imagine, video care se adresează în ultimă instanţă fiinţei umane şi care au o bogată structură statistică în termeni de corelaţie, modelul propus rămâne o unealtă utilă din punct de vedere teoretic, dar cu reduse aplicabilităţi practice. Mai mult, nu se specifică modalitatea de scădere a distribuţiei dintre P_C şi P_S.

6.5 *Model adaptiv*

Pentru a creşte gradul de protecţie a datelor unii autori [FRA04] au propus diferite sisteme steganografice adaptive. Soluţia propusă constă în suprapunerea unei măşti peste obiectul de acoperire. Masca ia valori de 0 şi 255 (alb, negru). Noua imagine obţinută este utilizată pentru încorporarea mesajului secret rezultând în felul acesta o imagine steganografică directă. O a doua prelucrare constă în utilizarea obiectului de acoperire iniţial, a obiectului steganografic prelucrat în care se încorporează mesajul, rezultând o imagine steganografică mascată. Cele două imagini steganografice sunt emise către receptor, urmând ca din ele să se extragă mesajul ascuns. Pentru alegerea măştii autorii calculează un prag în vederea stabilirii valorii fiecărui pixel component. În acest fel, masca se construieşte pixel cu pixel în funcţie de intensitatea imaginii originale. Mesajul secret este ascuns în biţii cei mai puţini semnificativi ai obiectului de acoperire. Pentru a face mai dificilă detectarea mesajului, în algoritmul de ascundere se apelează la utilizarea unor şiruri de numere pseudoaleatoare cunoscute atât de emiţător cât şi de receptor. Prin acest procedeu autorii arată că rata de detecţie a unui eventual atacator scade semnificativ.

Un alt model propus în [CHA04] constă în adaptarea modelului steganografic de bază într-un model ce permite obţinerea obiectului steganografic prin utilizarea unui cod aleator pentru ascunderea mesajului secret în aşa numitele ”zgomote albe”.

În [BOH04] se adaptează modelul steganografic de bază prin divizarea obiectului de acoperire în două variabile: deterministe şi nedeterministe. Prin aceasta se încearcă găsirea distribuţiei condiţionate dintre acestea folosind ca parametrii variabilele deterministe, iar pe baza unei funcţii de decompresie biţii mesajului sunt distribuiţi în variabilele nedeterministe. În final se însumează cele două tipuri de variabile rezultând obiectul steganografic.

6.6 *Optimizarea modelelor steganografice*

Toate modelele steganografice tind să ascundă cât mai bine o informaţie secretă.

Scopul steganografiei este ca transmiterea informaţiilor ascunse să fie făcută astfel încât să nu creeze suspiciuni, deoarece există şi metode ce ar putea distruge mesajul transmis în cazul în care acesta poate fi descoperit. În [CHE08b] sunt prezentate discuţii despre soluţiile propuse pentru rezolvarea unor astfel de probleme ce pot apărea în timpul unui proces steganografic.

Generarea unor metode de comunicare ascunsă care să permită construirea unor obiecte steganografice cât mai rezistente la potenţiale atacuri este o direcţie de cercetare diferită de steganografie şi este cunoscută ca steganaliză. Este de menţionat faptul că generarea algoritmilor de steganaliză este tot timpul dependentă de generarea unor noi algoritmi steganografici. Din acest motiv astfel de algoritmi au apărut permanent în urma algoritmilor steganografici [WAT08, KER08, HUL08, MEH08, FER08, YUX08, KHO09].

Pentru ca un mesaj ascuns să fie detectat un prim pas l-ar putea constitui observarea de către un analist a unor diferenţe sesizabile în imaginea steganografică rezultată în urma încorporării informaţiei secrete în obiectul de acoperire ales. Pasul următor ar presupune un atac asupra imaginii detectate, astfel că prin diferite tehnici de distorsiune aplicate imaginii steganografice, mesajul încorporat în ea va fi astfel modificat încât nu mai poate fi recuperat. Aşadar, dacă algoritmul ales pentru ascundere nu a fost bine conceput sau implementat, nu este necesar ca mesajul secret să fie identificat, ci este suficient să fie depistată existenţa lui. În acest caz sunt foarte mari şansele ca informaţia ascunsă să fie distrusă sau deteriorată.

Un exemplu în acest sens se poate regăsi în [BON07a] unde este prezentată o metodă de steganaliză pentru imagini ce conţin informaţii secrete ascunse în cei mai puţini semnificativi biţi ai imaginii de acoperire aleasă. Pentru a genera statistici în vederea obţinerii unor rezultate comparative este folosită compresia fără pierderi a imaginilor .

Atacurile asupra sistemelor steganografice pot fi clasificate în două categorii: pasive şi active [JOH01]. Deoarece acestea nu pot fi stopate se fac în permanenţă cercetări pentru a fi contracarate. În literatura de specialitate se poate remarca frecvent faptul că aceiaşi autori care concep algoritmi steganografici, concep şi măsuri de atac şi contraatac [GUL06, GUL07a, GUL08a]. Astfel că, o parte din algoritmii steganografici propuşi pentru a ascunde o informaţie secretă presupun şi măsuri de precauţie în cazul în care sunt atacaţi. O posibilă contramăsură pentru a evita distorsionarea presupune încorporarea datelor secrete în zonele percepute ca fiind cele mai semnificative din imaginea de acoperire, această metodă face foarte dificilă alterarea informaţiei ascunse [JOH01].

Pentru marea majoritate a algoritmilor steganografici pentru care au fost concepuţi algoritmi de atac s-au găsit măsuri de contraatac prin mărirea rezistenţei la detecţia mesajului ascuns [ABO08, LIX08, ZHA07a, XIA08a, XIA08b].

Alte metode concepute pentru a mări rezistenţa obiectelor steganografice la diferite atacuri constă în combinarea unor algoritmi diferiţi, cum ar fi: metoda bitului celui mai puţin semnificativ (LSB) cu transformata cosinus discretă (DCT) [RAJ05].

În [ABR09] se prezintă o metodă robustă la atacuri prin zgomot şi distorsionarea imaginii prin combinarea metodei SSIS (Spread-Spectrum Steganography Sistem) cu tehnici de ascundere în domeniul frecvenţei (DCT). Această metodă prezintă imperceptibilitate mare la imaginea steganografică, iar recuperarea datelor se face complet.

În [CHI05a] se propune o soluţie prin care imaginea este comprimată , apoi criptată , iar încorporarea imaginii se face în domeniul frecvenţei DCT.

[CHI09] propune o metodă de încorporare a datelor pe nivele pentru îmbunătăţirea capacităţii de ascundere din schemele DCT, iar rezultatele experimentale confirmă faptul că se obţine o capacitate de ascundere mai eficientă decât în alte lucrări luate ca referinţă.

În [MOH08, GUL07a] este propusă o tehnică de ascundere bazată pe descompunerea valorii singulare (SVD) (Singular Value Decomposition) şi pe metode de cuantizare. Prin aceste metode autorii sugerează obţinerea unor imagini digitale steganografice deosebit de robuste, aproape nedetectabilă la aplicarea metodelor steganalitice existente.

Algoritmul propus în [GOR03] se bazează tot pe tehnica SVD şi introducerea unor combinaţii liniare de valori aparţinând imaginii de acoperire. Această tehnică nu-şi propune realizarea unei capacităţi mari de ascundere, ci doar realizarea unei imagini steganografice robuste.

În [NAV08] se propune o combinare bazată pe trei metode DWT (transformata de undă discretă) (Discret Wavelette Transform), DCT şi SVD. Metoda ascunderii discrete dovedeşte că recuperarea mesajului poate fi făcută în condiţii bune şi în situaţii de atac asupra sistemului.

Pentru realizarea unui proces steganografic sunt utilizate diferite tehnici de bază ce pot fi diferenţiate în funcţie de metodele de ascundere folosite, dintre care cele mai cunoscute sunt:

a) Metoda injecţiei se bazează pe inserarea mesajelor secrete în diferite zone dintr-un obiect de acoperire, ce ar putea fi ignorate la prima vedere. Un dezavantaj al acestei metode de ascundere îl constituie modificarea mărimii obiectului de acoperire folosit. În cazul în care datele înserate modifică prea mult dimensiunile acestuia, procesul steganografic poate fi mai uşor detectat.

b) Metoda substituţiei are ca principal scop găsirea informaţiilor nesemnificative dintr-un obiect de acoperire şi înlocuirea acestora cu date secrete [CHI05b]. Dezavantajul acestei metode constă în faptul că este posibil ca obiectul steganografic obţinut să fie puţin diferit faţă de obiectul de acoperire, ceea ce ar putea conduce la detecţia eventuală a mesajului secret. Cu toate acestea metoda conduce la rezultate foarte bune dacă algoritmii steganografici utilizaţi sunt bine concepuţi.

c) Metoda generării realizează crearea unor noi obiecte steganografice ca urmare a încorporării informaţiilor secrete în obiectele de acoperire folosite în acest scop.

În [CHI05a] se propune un model bazat pe ascunderea unei imagini secrete într-o imagine fractală ce pare inofensivă la prima vedere. Pentru aceasta se alege o imagine de acoperire şi se foloseşte metoda compresiei imaginii. După implementarea imaginii secrete, scopul procesului steganografic a fost îndeplinit cu succes. Prin metoda generării, obiectul de acoperire este ales şi folosit pentru a crea obiectul steganografic ce este public. Această metodă este totodată expusă riscului

detectării procesului steganografic. În cazul în care o persoană neautorizată obţine accesul la amândouă obiectele, aceasta are posibilitatea de a observa existenţa a două structuri binare diferite. Dacă se apelează la folosirea imaginilor fractale ca şi imagini steganografice este de preferat să se ţină seama de profilul unui eventual atacator. În acest sens, nu este indicat să se trimită imagini fractale la persoane ce nu au mai primit astfel de imagini, deoarece acest lucru ar trezi suspiciuni.

Pentru ca un proces steganografic să fie realizat cu succes un rol important îl are alegerea unor algoritmi adecvaţi pentru ascunderea mesajului.

În acest sens algoritmii utilizaţi trebuie să îndeplinească mai multe caracteristici, cum ar fi: posibilitatea de a ascunde o cantitate cât mai mare de informaţii fără degradarea imaginii putătoare în mod vizibil, iar în cazul unui atac cu intenţia de a distruge informaţia algoritmii trebuie să fie suficienţi de robuşti pentru a face faţă unor astfel de încercări.

De asemenea este foarte importantă şi puterea de computaţie, respectiv timpul de execuţie al algoritmilor în timp real, resursele consumate, memoria necesară adiţională.

Pentru testarea gradului de rezistenţă a informaţiei ascunse în vederea obţinerii unui model steganografic cât mai robust sunt necesare parcurgerea următoarelor etape:

1. Folosirea obiectelor de acoperire standard existente şi crearea unor noi obiecte pentru testare. Contracararea acestui obiectiv constă în utilizarea unor obiecte cât mai inofensive necunoscute eventualului atacator.
2. Încorporarea mesajelor secrete în obiectele de acoperire prin folosirea unor algoritmi care să permită un proces de ascundere cât mai eficient. În acest sens este de dorit implementarea unor algoritmi care să difere de cei clasici existenţi.
3. Verificarea obiectelor steganografice rezultate în urma încorporării mesajului urmată de compararea obiectelor steganografice cu obiectele originale în vederea obţinerii unor erori relative cât mai mici între ele.
4. Căutarea unor obiecte de ascundere adecvate mesajului încorporat astfel încât o terţă persoană să nu poată sesiza prezenţa acestuia.
5. Generarea unor procedee de procesare a obiectelor de acoperire care să inducă în eroare un eventual atacator, dar care să nu afecteze mesajul ascuns.

În timpul realizării unor astfel de teste obiectele de acoperire, respectiv informaţiile secrete pot trece prin trei tipuri de operaţii: conversie, procesare şi extragerea mesajului.

Prin conversia obiectelor de acoperire se poate realiza transpunerea acestora dintr-un domeniu în alt domeniu (ex: din domeniul spaţial în domeniul frecvenţă, vectorial sau chiar alt domeniu spaţial).

Procesarea obiectelor constă în utilizarea diferitelor tehnici ce pot presupune introducerea zgomotelor, comprimarea mesajului sau dispersarea lui în cadrul acestora într-un mod pseudoaleator prin utilizarea unor algoritmi specifici. Extragerea mesajului presupune aplicarea inversă a procesării şi conversiei obiectelor steganografice pentru obţinerea cu o fidelitate cât mai bună a mesajului ascuns. Un mesaj recuperat este considerat de bună calitate dacă eroarea relativă dintre el şi mesajul iniţial este mică.

Pentru optimizarea modelelor steganografice propun în continuare două soluţii, dintre care una presupune prelucrarea obiectelor de acoperire înainte de

încorporarea informaţiei secrete, iar a doua implică atât procesarea obiectelor de acoperire, cât şi a mesajului ce urmează a fi ascuns.

6.7 *Model bazat pe procesare*

Pe baza modelelor prezentate în paragrafele anterioare dezvoltate în literatura de specialitate [ZOL98] şi [CAH04] se poate desprinde concluzia că singura modalitate prin care un atacator poate ajunge la mesajul secret o constituie intervenţia acestuia pe căile de comunicare. Din acest punct de vedere o posibilitate de a mări gradul de securizare a unui sistem steganografic o constituie protejarea informaţiilor doar pe două căi:

a) Procesarea informaţiei
b) Transmiterea informaţiei

În obţinerea obiectului steganografic un eventual atacator nu are nici un fel de acces, ceea ce permite ca în această etapă să fie generate diferite procedee ce-l pot induce în eroare şi îi pot îngreuna încercările de a extrage sau a distruge informaţia ascunsă. Soluţiile alese constau în procesarea obiectelor de acoperire rezultând astfel alte obiecte total necunoscute unui eventual atacator, şi/sau prelucrarea mesajului secret pentru a-l face neinteligibil în cazul unei detecţii de către terţe persoane.

Transmiterea informaţiei reprezintă calea de comunicare între emiţător şi receptor. Un eventual atacator ar putea avea acces doar la obiectul steganografic transmis. Pentru ca procesul steganografic să fie realizat cu succes este necesar ca obiectul steganografic să fie astfel obţinut încât să nu trezească nici un fel de suspiciune.

Voi prezenta în continuare două modele steganografice bazate atât pe procesarea obiectelor de acoperire, cât şi pe procesarea mesajului secret.

6.7.1 Procesarea obiectelor de acoperire: MPOA

6.7.1.1 Descrierea modelului MPOA

Modelul MPOA presupune combinarea celor două obiective privind îmbunătăţirea procesului de ascundere amintite mai sus folosind procesarea şi transmiterea obiectelor de acoperire într-o aşa manieră care să conducă din punct de vedere matematic şi practic la creşterea gradului de securizare.

În figura 6.5 prezint schematic modelul propus, iar în continuare voi descrie modalitatea de funcţionare a acestuia.

În prima etapă se pleacă de la premisa că emiţătorul are la dispoziţie o mulţime de obiecte de acoperire originale C_R în vederea obţinerii unui set de obiecte de acoperire C folosite ulterior în procesul steganografic.

În a doua etapă se prevede introducerea unei funcţii de procesare f_p ce permite prelucrarea fiecărui obiect din setul dat C_R astfel încât să rezulte un set de

obiecte de acoperire C . Pentru a induce în eroare un eventual atacator emiţătorul încorporează aleator informaţia secretă doar în câteva obiecte de acoperire, acestea devenind astfel obiecte steganografice S . Către receptor este trimis tot setul de obiecte de acoperire, respectiv atât cele care conţin informaţie secretă, cât şi cele care nu conţin. Procedeul de selecţie este făcut cu ajutorul unui întrerupător „k" ce poate fi regăsit în figura 6.5.

În cazul în care întrerupătorul este pe „0", emiţătorul trimite doar obiectul de acoperire, care poate îndrepta atacatorul pe o pistă falsă. Din punct de vedere teoretic, acest obiect nu este considerat obiect steganografic, deoarece nu conţine informaţie suplimentară.

Dacă întrerupătorul este pe „1" emiţătorul trimite obiecte steganografice. Comanda întrerupătorului se va face după o funcție aleatoare cunoscută atât de emiţător cât şi de receptor.

Funcţia de procesare poate fi realizată prin metode ce urmează un anumit algoritm, cunoscut de emiţător, dar nu neapărat şi de receptor, în funcţie de posibilităţile de îmbunătăţire a entropiei obiectului rezultat. S-a prezentat în subcapitolul 6.3 că în momentul în care se introduce informaţie suplimentară într-un anumit obiect de acoperire, creşte gradul entropiei acestuia. Acest fapt, ar putea fi sesizat de către un eventual atacator, în cazul în care obiectul de acoperire nu a fost ales în mod corespunzător.

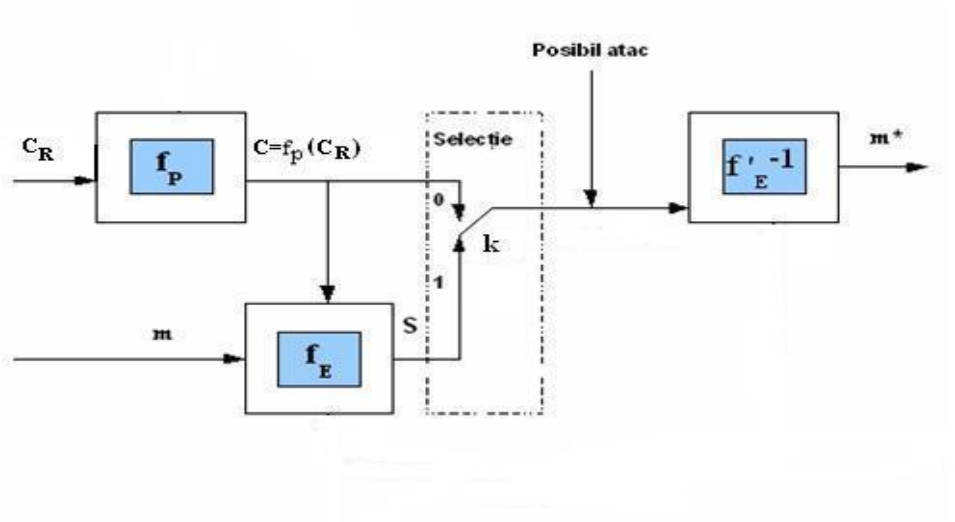


Figura 6.5. Model steganografic cu preprocesare directă şi inversă a obiectului de acoperire

Modificările făcute cu ajutorul funcţiei de procesare vor urmări ca diferenţa dintre realizarea obiectului de acoperire original să nu difere prea mult de cea a obiectului rezultat în urma prelucrării. Aşadar prin intermediul funcţiei de procesare f_p, se pot face diferite prelucrări, cum ar fi: eventuale zgomote, deplasarea informaţiei binare spre valori mai mari sau mai mici, etc. Astfel de prelucrări apar de astă dată, la toate obiectele de acoperire rezultate, astfel încât creşte gradul

entropiei în aceeaşi măsură la toate obiectele, nu doar la cel care urmează să aibă informaţie secretă. În acest fel, la un eventual atac este mai greu de detectat care obiect de acoperire din setul trimis ar putea conţine mesajul ascuns. Condiţia esenţială este ca atacatorul să nu aibă acces la obiectul de ascundere original.

În a treia etapă urmează încorporarea mesajului secret în obiectul de acoperire ales prin intermediul funcţiei steganografice f_E şi transmiterea de la emiţător la receptor atât a obiectelor de acoperire rezultate în urma preprocesării, cât şi a obiectului steganografic rezultat în urma încorporării informaţiei secrete.

La receptor are loc extragerea mesajului secret, reprezentată în figura 6.5 prin funcţia inversă $f_E^{'-1}$, care poate fi alcătuită din funcţia de preprocesare inversă f_p^{-1}, compusă cu funcţia steganografică inversă f_E^{-1}. Compunerea celor două funcţii are rolul de a recupera mesajul secret obţinut la ieşire „m^*" într-o formă cât mai apropiată de cel original.

Folosirea cheilor steganografice poate conduce la o îngreunare a descoperirii mesajului în cazul unui eventual atac. Se menţionează faptul că în cazul steganografiei pure prezenţa unei chei de codare nu este obligatorie, dacă algoritmii de ascundere folosiţi sunt bine aleşi [KAT00].

În continuare voi încerca să demonstrez din punct de vedere matematic îmbunătăţirile aduse prin modelul propus de mine mai sus în figura 6.5.

6.7.1.2 Demonstrarea teoretică a modelului MPOA

Conform [CAH04] un sistem steganografic este perfect sigur dacă este îndeplinită condiţia:

$$D\left(\frac{P_C}{P_S}\right) = 0 \tag{6.11}$$

Unde P_C este distribuţia de probabilitate a obiectului de acoperire C, iar P_S este distribuţia de probabilitate a obiectului steganografic S.

De asemenea $D\left(\frac{P_C}{P_S}\right)$ reprezintă entropia relativă sau discriminarea dintre două probabilităţi distribuite P_C, P_S şi exprimă o măsură a diferenţei dintre distribuţiile de probabilitate a obiectelor ce caracterizează procesul de ascundere. În [PET07] entropia relativă este dată de relaţia:

$$D\left(\frac{P_C}{P_S}\right) = \sum_{c \in C} P_C(c) \cdot \frac{\log(P_C(c))}{P_S(c)} \tag{6.12}$$

În situaţia în care $\mathbf{D\left(\frac{P_C}{P_S}\right) = 0}$ rezultă că nu există diferenţe între cele două distribuţii, ca atare cel ce doreşte să intercepteze mesajul steganografiat nu poate face diferenţa dintre obiectul de acoperire C şi obiectul steganografic S. În acest caz, atacatorul trebuie sa analizeze toate obiectele trimise (S şi C) nefiind în stare să extragă în timp real mesajul ascuns în S printr-un algoritm polinomial.

Dacă între P_S şi P_C există diferenţe atunci cel ce doreşte să extragă mesajul secret se poate concentra doar pe obiectele steganografice putând astfel desprinde mesajul ascuns în S într-un algoritm polinomial.

Deoarece o steganografie perfectă este greu de realizat în practică se caută o distribuţie P_S care sa nu difere prea mult de $\mathbf{P_C}$. În această situaţie tot Cachin defineşte în [CAH04] o stenografiere ε -securizata dacă:

$$\mathbf{D}\left(\frac{\mathbf{P_C}}{\mathbf{P_S}}\right) \leq \varepsilon \tag{6.13}$$

Cu cât ε este mai mic cu atât va fi mai greu pentru cel ce interceptează obiectele trimise să facă deosebirea dintre C şi S şi astfel să reuşească să desprindă mesajul ascuns în S.

Pornim de la presupunerea că avem la dispoziţie un comutator k ce poate avea două stări:

$$k = \begin{cases} 0, \text{dacă } c \epsilon C_0 \\ 1, \text{dacă } c \epsilon C_1 \end{cases} \tag{6.14}$$

unde alfabetul C se scrie ca:

$$C = C_0 \oplus C_1 \tag{6.15}$$

adică C_0 si C_1 reprezinta o partiţie a lui C : $C_0 \cup C_1 = C$, respectiv $C_0 \cap C_1 = \emptyset$ (6.16)

Conform [CAH04], în cazul descris mai sus o stenografie este ε – securizată pentru:

$$\varepsilon = \frac{\delta^2}{\mathbf{ln2}} \tag{6.17}$$

unde :

$$\delta = \mathbf{P_r[c \epsilon C_0]} - \mathbf{P_r[c \epsilon C_1]} \tag{6.18}$$

În relaţia (6.18) $\delta > \mathbf{0}$ deoarece $P_r[c \epsilon C_0] > P_r[c \epsilon C_1]$ altfel ar exista diferenţe mari între P_S şi P_C.

Toate acestea sunt demonstrate pornind de la relaţia:

$$P_S(c) = \begin{cases} \dfrac{P_C(c)}{1+\delta}, & daca\ c \epsilon C_0 \\ \dfrac{P_C(c)}{\mathbf{1}-\delta}, & daca\ c \epsilon C_1 \end{cases} \tag{6.19}$$

Care rezultă din partiţionarea lui $C = C_0 \oplus C_1$

Pe baza probabilităţii totale [PET07]:

$$P(A) = \sum_{i \epsilon I} P(A_i) \cdot P\left(\frac{A}{A_i}\right) \tag{6.20}$$

şi a probabilităţii condiţionate:

$$P\left(\frac{A}{B}\right) = \frac{P(A \cap B)}{P(B)} \quad \text{sau} \quad P(A \cap B) = P\left(\frac{A}{B}\right) P(B) \tag{6.21}$$

Într-adevăr avem:

$$P_Y[S=c] \cong P_Y\left[S=\frac{c}{c\epsilon C_0}\right]\cdot P_Y[c\epsilon C_0]+P_Y\left[S=\frac{c}{c\epsilon C_1}\right]\cdot P_Y\left[c\epsilon C_1\right] \quad (6.22)$$

Dar,

$$P_Y\left[S=\frac{c}{c\epsilon C_0}\right]=P_Y\left[C=\frac{c}{c\epsilon C_0 sau\ c\notin C_1}\right]=\frac{P_Y[C=c\ si\ (c\epsilon C_0 sau\ c\in C_1)]}{P_Y[c\epsilon C_0 sau\ c\in C_1]}=\frac{P_Y[C=c]}{1+\delta} \quad (6.23)$$

Dacă $c\epsilon C_0$, pentru că:

$$1+\delta=1+P_Y[c\epsilon C_0]-P_Y[c\epsilon C_1]=P_Y[c\epsilon C_0]+1-P_Y[c\epsilon C_1]$$
$$=P_Y[c\epsilon C_0]+P_Y[c\notin C_1]=P_Y[c\epsilon C_0 sau\ c\notin C_1] \quad (6.24)$$

Analog:

$$P_Y\left[S=\frac{c}{c\epsilon C_1}\right]=P_Y\left[C=\frac{c}{c\epsilon C_1 sau\ c\notin C_0}\right]=\frac{P_Y[C=c\ si\ (c\in C_0\ sau\ c\epsilon C_1)]}{P_Y[c\epsilon C_1 sau\ c\in C_0]}=\frac{P_Y[C=c]}{1-\delta} \quad (6.25)$$

Dacă $c\epsilon C_1$ pentru că:

$$1-\delta=1-P_Y[c\epsilon C_0]+P_Y[c\epsilon C_1]=P_Y[c\notin C_0]+P_Y[c\epsilon C_1]$$
$$=P_Y[c\epsilon C_1 sau\ c\notin C_0] \quad (6.26)$$

Iar,

$$P_Y[c\epsilon C_1]=\begin{cases}0, & dacă\ c\epsilon C_0\\ 1, & dacă\ c\epsilon C_1\end{cases} \quad (6.27)$$

$$P_Y[c\epsilon C_0]=\begin{cases}0, & dacă\ c\epsilon C_1\\ 1, & dacă\ c\epsilon C_0\end{cases} \quad (6.28)$$

Din cele prezentate în [ZOL98] anterior se remarcă faptul că sistemele steganografice nu pot fi sigure în cazul în care un atacator cunoaşte C şi S, adică are posibilitatea să compare două obiecte de aceeaşi natură ce par identice, dar care totuşi conţin informaţii diferite. Pentru a găsi o soluţie la această problemă, autorii introduc un grad de incertitudine la unul din obiecte C pentru a deruta atacatorul, deoarece de astă dată va compara un obiect ce conţine informaţie S cu un obiect pe care nu îl cunoaşte C, ci doar îşi imaginează cum ar putea arăta. Ca să poată fi realizată această analiză se recurge la cercetarea comportării unui parametru, numit entropie, ce caracterizează ambele elemente supuse comparaţiei de către atacator: incertitudinea şi informaţia.

Un exemplu în acest sens îl constituie realizarea unei poze şi alegerea acesteia ca mediu purtător pentru ascunderea unei informaţii secrete. Aşadar se stabileşte sursa, adică imaginea care urmează a fi captată şi se transformă în poză cu ajutorul unui aparat foto urmând un proces de prelucrare specific acestuia. Poza astfel obţinută constituie obiectul de acoperire C în care se încorporează în continuare un mesaj secret şi devine astfel obiect steganografic S care este trimis la vedere pe un canal nesecurizat. În momentul în care este interceptat de un observator sau atacator, acesta recunoaşte practic Sursa, adică imaginea ce a fost fotografiată, dar nu are acces direct la poza originală C, ce a fost obţinută imediat în urma captării, fapt care induce o incertitudine asupra acestui element. Neavând obiectul de acoperire original nu are termen de comparaţie cu ce are la vedere, şi anume obiectul steganografic S şi astfel nu poate depista mesajul secret.

Pentru a obţine obiectul original în care a fost ascunsă informaţia atacatorul poate apela la diferite metode. În primul rând ar putea încerca să identifice locul unde a fost făcută poza cu scopul de a face poze similare ca să poată compara cu S . Se poate presupune că ar obţine acces chiar la aparatul foto cu ajutorul căruia a fost făcută poza. Acesta are în interiorul său un senzor de captare format din circuite CMOS sau CCD, care sunt mai mult sau mai puţin sensibile la temperatură. Datorită faptului că temperatura este un factor ce nu poate fi controlat cu mare precizie, în cazul în care atacatorul hotărăşte să facă 10 poze consecutive pentru testare va constata că acestea vor diferi puţin una faţă de cealaltă. Existând această diferenţă între ele, poate trage concluzia că şi poza steganografică „S ” interceptată este normal să fie puţin diferită. Dacă ar exista situaţia ca toate cele 10 poze să fie identice şi doar cea steganografică să difere ar putea bănui cu uşurinţă că e vorba de mesaj ascuns în ea.

În concluzie, se poate spune că indiferent câte încercări ar face atacatorul pentru a obţine obiectul de acoperire original C , dacă aceste încercări vor diferi între ele datorită factorilor externi ce apar şi nu pot fi controlaţi de acesta, atunci faptul că obiectul steganografic S este şi el diferit, nu dă de bănuit. În caz contrar, dacă toate încercările atacatorului ar avea rezultate identice şi doar obiectul steganografic S diferă, l-ar face să se gândească la posibilitatea existenţei unui mesaj ascuns.

Ca atare, modelul propus de Zollner presupune alegerea unui obiect de acoperire necunoscut unui eventual atacator. Acesta este supus în prealabil unui proces de preprocesare ce presupune fie folosirea unor echipamente diferite de achiziţie şi digitizare a lui, fie realizarea unor prelucrări asupra sa. Odată ales, obiectul de acoperire este utilizat în obţinerea obiectului steganografic. În [ZOL98] nu se demonstrează matematic că modelul steganografic propus are siguranţă sporită.

Modelul propus în [CAH04] constă în alegerea unui set de obiecte de acoperire în care doar unele sunt folosite la realizarea obiectului steganografic. La receptor se trimit atât obiecte de acoperire cât şi obiecte steganografice.

Modelul propus de mine constă în alegerea unui set de obiecte de acoperire ce urmează a fi prelucrate individual urmând ca doar o parte dintre acestea să fie utilizate ca şi obiecte steganografice. În cele ce urmează voi demonstra matematic că introducerea unei funcţii de procesare asupra obiectelor de acoperire poate conduce la creşterea gradului de securitate a unui sistem steganografic.

În acest sens în modelul propus în figura 6.5 aplic pentru fiecare obiect de acoperire ales o funcţie de procesare care să genereze o mărime ε de o valoare mai mică decât cea obţinută în Teorema 2 de către Cachin în [CAH04] . Noua valoare a lui ε va fi estimată atât printr-o demonstraţie matematică, cât şi pe baza unor experimente.

Dacă presupunem că funcţia de procesare aleasă este de forma:

$$f_p(x) = a \cdot x, \text{ unde } a > 1 \tag{6.29}$$

Cu ajutorul acestei funcţii se va genera setul de obiecte de acoperire C obţinute din setul iniţial C_R , în următorul mod:

$$C = f_p(C_R) \tag{6.30}$$

În urma procesării voi demonstra că:

$$\varepsilon = \frac{1}{a^2} \cdot \frac{\delta^2}{ln2} \tag{6.31}$$

Mărimea ε obţinută este mai mică decât ε rezultat în [CAH04].

Pentru a demonstra afirmaţia exprimată de relaţia (6.31) se pleacă de la Teorema 1 şi Teorema 2 din [CAH04], conform căreia:

$$D\left(\frac{P_C}{P_S}\right) \leq D\left(\frac{P_{C_R}}{P_S}\right) \leq \frac{\delta^2}{ln2} \tag{6.32}$$

Însă,

$$D\left(\frac{P_C}{P_S}\right) = \sum_{c \in C} P_C(c) \cdot \frac{\log(P_C(c))}{P_S(c)} \tag{6.33}$$

Pe de altă parte se poate face o schimbare de variabilă astfel că relaţia (6.33) poate fi exprimată în funcţie de noua variabilă:

$$D\left(\frac{P_C}{P_S}\right) = \sum_{d \in C} P_C(d) \cdot \frac{\log(P_C(d))}{P_S(d)} \tag{6.34}$$

Dar,

$$P_S(d) = \begin{cases} \frac{P_C(d)}{1+\delta}, & dacă\ d \epsilon C_0 \\ \frac{P_C(d)}{1-\delta}, & dacă\ d \epsilon C_1 \end{cases} \tag{6.35}$$

Unde:

$$\delta = P_r[d \epsilon C_0] - P_r[d \epsilon C_1] \tag{6.36}$$

Deci:

$$D\left(\frac{P_C}{P_S}\right) = \sum_{d \in C_0} P_C(d) \cdot log(1+\delta) + \sum_{d \in C_1} P_C(d) \cdot log(1-\delta) \tag{6.37}$$

Dacă:

$C = f_p(C_R)$

Atunci, conform [CIU71]:

$$P_C(d) = \left|\frac{1}{f_p'\left(f_p^{-1}(d)\right)}\right| \cdot P_{C_R}\left(f_p^{-1}(d)\right) \tag{6.38}$$

Dacă:

$$f_p(x) = a \cdot x \quad \Rightarrow \quad \begin{cases} f_p^{-1}(x) = \frac{x}{a} \\ f_p'(x) = a \end{cases} \tag{6.39}$$

În continuare se adoptă următoarea notaţie:

$$f_p^{-1}(d) = \frac{d}{a} = c \tag{6.40}$$

Unde $d \epsilon C$, ceea ce implică:

$$c \epsilon C_a = \frac{1}{a} C \tag{6.41}$$

În cazul nostru mulţimea C constituie mulţimea pixelilor dintr-o imagine. În mod identic şi C_a reprezintă tot o mulţime a pixelilor, dar scalată cu valoarea a. Astfel din relaţiile (6.37, 6.38) rezultă:

$$D\left(\frac{P_C}{P_S}\right) = \frac{1}{a} \cdot \sum_{d \epsilon C_0} P_{C_R}\left(\frac{d}{a}\right) \cdot log(1+\delta) + \frac{1}{a} \cdot \sum_{d \epsilon C_1} P_{C_R}\left(\frac{d}{a}\right) \cdot log(1-\delta) =$$

$$= \frac{1}{a} \cdot \sum_{c \epsilon C_0} \frac{1}{a} P_{C_R}(c) \cdot log(1+\delta) + \frac{1}{a} \cdot \sum_{c \epsilon C_1} \frac{1}{a} P_{C_R}(c) \cdot log(1-\delta) =$$

$$= \frac{1}{a^2} \cdot \sum_{c \epsilon C_0} P_{C_R}(c) \cdot log(1+\delta) + \frac{1}{a^2} \cdot \sum_{c \epsilon C_1} P_{C_R}(c) \cdot log(1-\delta) \tag{6.42}$$

Cum:

$$log(1+x) \leq \frac{x}{ln2} \tag{6.43}$$

Iar:

$$\sum_{c \epsilon C_0} P_{C_R}(c) = \frac{1+\delta}{2} \tag{6.44}$$

$$\sum_{c \epsilon C_1} P_{C_R}(c) = \frac{1-\delta}{2} \tag{6.45}$$

Ştim că:

$$\sum_{c \epsilon C} P_{C_R}(c) = 1 \tag{6.46}$$

deoarece P_{C_R} este o distributie.

Rezultă:

$$D\left(\frac{P_C}{P_S}\right) = \frac{1}{a^2} \sum_{c \epsilon C_0} P_{C_R}(c) \cdot log(1+\delta) + \frac{1}{a^2} \sum_{c \epsilon C_1} P_{C_R}(c) \cdot log(1-\delta) =$$

$$= \frac{1}{a^2\left[\frac{1+\delta}{2} log(1+\delta) + \frac{1-\delta}{2} log(1-\delta)\right]} \tag{6.47}$$

Pe baza relaţiei (6.43), relaţia (6.47) devine:

$$D\left(\frac{P_C}{P_S}\right) \leq \frac{1}{a^2\left(\frac{1+\delta}{2} \cdot \frac{\delta}{ln2} + \frac{1-\delta}{2} \cdot \frac{-\delta}{ln2}\right)} = \frac{1}{a^2} \frac{\delta^2}{ln2} \tag{6.48}$$

Pe de altă parte:

$$D\left(\frac{P_{C_R}}{P_S}\right) = log(1+\delta)\cdot\sum_{c\in C_0} P_{C_R}(c) + log(1-\delta)\cdot\sum_{c\in C_1} P_{C_R}(c)$$

(6.49)

Iar:

$$\delta = P_{C_R}\left(c\frac{}{c}\in C_0\right) - P_{C_R}\left(c\frac{}{c}\in C_1\right)$$

(6.50)

$$1+\delta = P_{C_R}\left(c\frac{}{c}\in C_0\right) + 1 - P_{C_R}\left(c\frac{}{c}\in C_1\right) =$$

$$= P_{C_R}\left(c\frac{}{c}\in C_0\right) + P_{C_R}\left(c\frac{}{c}\in C_1\right)$$

(6.51)

Dacă $|C_{\downarrow}0\ | = |C_{\downarrow}1\ |$, atunci

$$\sum_{c\in C_0} P_{C_R}(c) = \sum_{c\in C_1} P_{C_R}(c) = \frac{1}{2}$$

(6.52)

Pentru că:

$$\sum_{c\in C} P_{C_R}(c) = 1$$

Rezultă:

$$D\left(\frac{P_{C_R}}{P_S}\right) = \frac{1+\delta}{2}log(1+\delta) + \frac{1-\delta}{2}log(1-\delta) \le \frac{1+\delta}{2}\cdot\frac{\delta}{ln2} + \frac{1-\delta}{2}\cdot\frac{-\delta}{ln2} =$$

$$= {}^{\delta^2}/_{ln2}$$

(6.53)

În final se poate constata că:

$$\frac{D\left(\frac{P_C}{P_S}\right)}{D\left(\frac{P_{C_R}}{P_S}\right)} = \frac{1}{a^2}$$

(6.54)

Unde a>1.

Pe baza celor demonstrate mai sus rezultă că o prelucrare a obiectelor de acoperire cu un coeficient de forma $\frac{1}{a^2}$ unde a>1 conduce la micşorarea entropiei relative dintre distribuţiile obiectului steganografic rezultat şi obiectul de acoperire folosit ca suport.

Ca urmare, modelul propus permite o îmbunătăţire a siguranţei sistemelor steganografice pe baza a trei principii: generarea unui set de obiecte de acoperire cunoscute de către emiţător şi nu neapărat şi de receptor, procesarea individuală a acestora şi alegerea în mod aleator a unui sau mai multe obiecte de acoperire în care urmează să fie încorporate mesaje secrete. Pentru a veni în sprijinul informaţiilor ascunse de către receptor este de dorit ca acesta să fie informat asupra modalităţii de alegere a obiectelor de acoperire folosite ca obiecte steganografice.

Dacă această informaţie lipseşte receptorul va trebui să aplice funcţia inversă de decodare $f_E^{'-1}$ pentru întregul set de obiecte primite, ceea ce ar mări timpul de recuperare al mesajului. Este posibil totodată ca mai multe mesaje recuperate să aibă o anumită semnificaţie putând induce în eroare astfel receptorul. Pentru a elimina astfel de situaţii o soluţie ar fi ca receptorul să cunoască funcţia după care este ales obiectul de acoperire în procesul steganografic.

6.7.1.3 Verificarea experimentală a modelului MPOA

Pentru validarea modelului am făcut o serie de experimente bazându-mă pe algoritmul $ASAC$ descris în capitolul 9. În cadrul experimentelor am încorporat mesaje secrete exprimate sub forma unor imagini color în obiecte de acoperire reprezentate de asemenea sub formă de imagini color. Am utilizat imagini de dimensiuni şi tipologii diferite, cât şi modalităţi de ascundere în cei mai puţini semnificativi 1, 2, respectiv 4 biţi ai obiectului de acoperire.

Asupra acestuia am efectuat o serie de prelucrări relativ simple în concordanţă cu rezultatele teoretice menţionate mai sus. În acest sens am efectuat o deplasare a fiecărui pixel cu diferiţi paşi spre culoarea negru, respectiv alb. Rezultatele acestor prelucrări sunt prezentate în tabelele 6.1, 6.2 şi 6.3.

În cele 3 tabele pe primele două coloane se prezintă denumirea obiectului de acoperire şi dimensiunea exprimată în pixeli, pe următoarele două coloane se exprimă acelaşi lucru pentru mesajul secret, în următoarele cinci coloane exprim erorile obţinute între obiectul de acoperire şi obiectul steganografic pentru cinci cazuri distincte: eroarea exprimată în cazul unei deplasări a pixelului spre valoarea negru cu 10, 6 unităţi, obiectul de acoperire fără nici o prelucrare, respectiv deplasarea fiecărui pixel a obiectului de acoperire cu 6, 10 unităţi spre valoarea alb. În ultima coloană am exprimat în procente îmbunătăţirea erorii relative dintre obiectul de acoperire şi obiectul steganografic obţinută în urma prelucrării.

Se poate constata în urma analizării rezultatelor obţinute că o procesare a obiectului de acoperire duce la micşorarea erorii relative dintre obiectul de acoperire şi obiectul steganografic, adică rezultatele acestei prelucrări conduc la obţinerea unui obiect steganografic superior în cazul în care procesarea nu ar fi avut loc.

Tabel 6.1. Procesare obiect de acoperire.
Experimente efectuate cu algoritmul steganografic $ASAC$ pe 1 bit

Nr. Crt	Obiect de acoperire		Mesaj secret		Prelucrare obiect de acoperire					
	Nume	**Dimensiune** (pixeli)	**Nume**	**Dimensiune** (pixeli)	$\varepsilon\ la - 10$	$\varepsilon\ la - 6$	$\varepsilon\ la\ 0$	$\varepsilon\ la + 6$	$\varepsilon\ la + 10$	%
1	lena	256x256	firefox	128x128	0,19735	0,19744	0,19745	0,19760	0,19778	2,17
2	Aquaria	256x256	firefox	128x128	0,19558	0,19611	0,19657	0,19652	0,19664	5,42
3	dogs	640x480	wildflowers	200x135	0,19510	0,19530	0,19592	0,19595	0,19605	4,86
4	dogs	640x480	watch	200x135	0,19506	0,19545	0,19617	0,19637	0,19689	9,38
5	fruit	512x512	lena	256x256	0,19428	0,19460	0,19557	0,19635	0,19664	1,21
6	fruit	512x512	Aquaria	256x256	0,19413	0,19452	0,19554	0,19635	0,19670	1,32
7	Lena512	512x512	Aquaria	256x256	0,19630	0,19631	0,19631	0,19638	0,19646	0,08
8	Lena512	512x512	lena	256x256	0,19619	0,19620	0,19620	0,19625	0,19628	0,04
9	building	640x480	wildflowers	200x135	0,18922	0,19062	0,19504	0,19772	0,19850	4,10
10	building	640x480	watch	200x130	0,18731	0,18930	0,19586	0,20201	0,20422	9,02
11	Alicia	1024x1024	Lena512	512x512	0,19419	0,19505	0,19576	0,19576	0,19576	0,8
12	Alicia	1024x1024	fruit	512x512	0,19102	0,19402	0,19566	0,19566	0,19566	2,4
13	Alicia	1024x1024	dogs	640x480	0,19081	0,19384	0,19565	0,19565	0,19565	2,5
14	car	1024x1036	dogs	640x480	0,19457	0,19459	0,19459	0,19461	0,19461	0,02
15	car	1024x1036	fruit	512x512	0,19400	0,19402	0,19402	0,19402	0,19403	0,015
16	car	1024x1036	Leno512	512x512	0,19638	0,19639	0,19639	0,19639	0,19640	0,01
17	football	1600x1200	building	640x480	0,19305	0,19416	0,19574	0,19629	0,19641	1,74
18	football	1600x1200	hawk	800x600	0,19301	0,19426	0,19590	0,19646	0,19660	1,86
19	football	1600x1200	sphinx	800x600	0,19435	0,19493	0,19583	0,19609	0,19617	0,9
20	fish	1600x1200	building	640x480	0,19373	0,19454	0,19559	0,19575	0,19586	1,1
21	fish	1600x1200	hawk	800x600	0,19353	0,19437	0,19552	0,19568	0,19580	1,17
22	fish	1600x1200	sphinx	800x600	0,19497	0,19538	0,19585	0,19591	0,19596	0,5

Tabel 6.2. Procesare obiect de acoperire.
Experimente efectuate cu algoritmul steganografic $ASAC$ pe 2 biţi

Nr. Crt	Obiect de acoperire		Mesaj secret		Prelucrare obiect de acoperire					
	Nume	**Dimensiune** (pixeli)	**Nume**	**Dimensiune** (pixeli)	$\varepsilon\ la - 10$	$\varepsilon\ la - 6$	$\varepsilon\ la\ 0$	$\varepsilon\ la + 6$	$\varepsilon\ la + 10$	%
1	lena	256x256	merlin	128x128	0,54283	0,54341	0,54516	0,54465	0,54605	0,59
2	Lena	256x256	firefox	128x128	0,54657	0,54734	0,54914	0,54873	0,55023	0,53
3	Aquaria	256x256	firefox	128x128	0,54226	0,54432	0,54822	0,55144	0,55219	1,83
4	Aquaria	256x256	merlin	128x128	0,53958	0,54173	0,54277	0,54904	0,54979	1,89
5	Aquaria	256x256	watch	200x135	0,51725	0,51843	0,52248	0,52335	0,52403	1,31
6	Lena	256x256	watch	200x135	0,52042	0,52071	0,52238	0,52155	0,52341	0,57
7	Lena512	512x512	Aquaria	256x256	0,55789	0,55791	0,55757	0,55833	0,55864	0,13
8	fruit	512x512	lena	256x256	0,56109	0,54215	0,54268	0,56330	0,56588	4,58
9	fruit	512x512	Aquaria	256x256	0,56718	0,54826	0,56248	0,57653	0,57993	5,77
10	sphinx	800x600	fruit	512x512	0,50414	0,50415	0,52086	0,53481	0,53739	8,57
11	hawk	800x600	fruit	512x512	0,51281	0,51281	0,51001	0,51974	0,52670	2,70
12	Alicia	1024x1024	hawk	800x600	0,51574	0,53007	0,53995	0,54134	0,54134	4,96
13	Alicia	1024x1024	sphinx	800x600	0,51144	0,52137	0,52615	0,52680	0,52680	3,00
14	car	1024x1036	hawk	800x600	0,53980	0,53995	0,53938	0,56009	0,54019	0,07
15	car	1024x1036	sphinx	800x600	0,52675	0,52677	0,52362	0,52679	0,52683	0,02
16	fish	1600x1200	Alicia	1024x1024	0,54490	0,54790	0,55266	0,55661	0,55705	2,22
17	football	1600x1200	Alicia	1024x1024	0,54110	0,54497	0,55655	0,56314	0,56442	4,30
18	football	1600x1200	car	1024x1036	0,52558	0,52844	0,53536	0,53898	0,53951	2,65

Tabel 6.3. Procesare obiect de acoperire.
Experimente efectuate cu algoritmul steganografic $ASAC$ pe 4 biţi

Nr. Crt	Obiect de acoperire		Mesaj secret		Prelucrare obiect de acoperire					
	Nume	**Dimensiune** (pixeli)	**Nume**	**Dimensiune** (pixeli)	$\varepsilon\ la - 10$	$\varepsilon\ la - 6$	$\varepsilon\ la\ 0$	$\varepsilon\ la + 6$	$\varepsilon\ la + 10$	**%**
1	merlin	128x128	firefox	128x128	2,20065	2,21202	2,23028	2,21129	2,21925	0,85
2	Wildflowes	200x135	watch	200x135	2,11924	2,10974	2,10306	2,09935	2,16363	2,09
3	Lena	256x256	Aquaria	256x256	2,34364	2,37548	2,43198	2,35479	2,39349	2,12
4	Aquaria	256x256	lena	256x256	2,19141	2,23095	2,23256	2,211317	2,25572	2,93
5	Lena512	512x512	Fruit	512x512	2,22543	2,26987	2,27184	2,22689	2,27292	2,13
6	building	640x480	Dogs	640x480	2,36194	2,36677	2,47886	2,55992	2,60113	10,12
7	sphinx	800x600	Hawk	800x600	2,41660	2,44265	2,65467	2,72818	2,74720	13,68
8	hawk	800x600	Sphinx	800x600	2,34786	2,32531	2,28728	2,41975	2,48425	5,80
9	Alicia	1024x1024	Car	1024x1036	2,36585	2,39247	2,41650	2,53694	2,47603	4,65
10	car	1024x1036	Alicia	1024x1024	2,64180	2,75105	2,55188	2,64529	2,75354	4,22
11	fish	1600x1200	football	1600x1200	2,32144	2,32860	2,35385	2,36267	2,36583	1,91

Menţionez că deplasarea pixelilor spre culoarea negru (întunecarea imaginii) conduce la obţinerea unor erori relative mai mici pentru toate cazurile analizate. Aceste rezultate s-au obţinut în mod asemănător atât în cazul în care ascunderea realizată cu algoritmul $ASAC$ s-a făcut pe 1 bit (tabelul 6.1), pe 2 biţi (tabelul 6.2), cât şi în cazul ascunderii pe 4 biţi (tabelul 6.3). Din analiza rezultatelor obţinute în urma procesării obiectului de ascundere se poate constata o îmbunătăţire a erorii relative de până la 13, 68%. Sigur, sunt experimente la care îmbunătăţirea erorii este nesemnificativă, însă în această situaţie se constată că obiectul de acoperire prezintă zone mari având aceeaşi culoare (spre exemplu un fundal). Din această constatare putem face afirmaţia fără a greşi că astfel de obiecte de acoperire nu sunt indicate a fi utilizate în steganografie.

În figura 6.6 se prezintă un exemplu de prelucrare a obiectului steganografic prin deplasarea pixelilor acestuia spre negru (figura 6.6.b), respectiv alb (figura 6.6.c) comparativ cu situaţia în care obiectul de ascundere nu este prelucrat. Menţionez că în urma prelucrărilor obiectelor de acoperire pot exista şi rezultate superioare celor menţionate anterior, aşa cum am prezentat mai sus.

a)Obiect de acoperire neprelucrat

Obiect steganografic

b)Obiect de acoperire cu deplasare spre negru — Obiect steganografic

c) Obiect de acoperire cu deplasare spre alb — Obiect steganografic

Figura 6.6 Exemplu de prelucrare a obiectului de ascundere

Se constată că diferenţa dintre obiectul de acoperire şi obiectul steganografic este nesesizabilă în toate cele trei cazuri, dar din punctul de vedere al erorii relative dintre obiectul de acoperire şi obiectul steganografic, valorile cele mai bune se obţin în cazul deplasării spre negru cu o îmbunătăţire de 2% (pentru acest exemplu). Rezultatele experimentale sunt prezentate şi în tabelul 6.3, linia 2. Procesarea obiectelor de acoperire şi a mesajelor secrete: MPOAM

6.7.1.4 Descrierea modelului MPOAM

Aşa cum s-a văzut în paragraful anterior o prelucrare a obiectelor de acoperire conduce atât din punct de vedere teoretic, cât şi experimental la creşterea siguranţei sistemelor steganografice deoarece este introdus un grad de nederminare în plus. În acest sens un eventual atacator este obligat să identifice şi funcţia de procesare a obiectelor de acoperire pentru a extrage mesajul ascuns.

De asemenea se constată că procesul de prelucrare a fiecărui pixel aşa cum s-a arătat mai sus, conduce la micşorarea entropiei relative dintre cele două distribuţii de probabilitate ale obiectului de acoperire şi obiectului steganografic rezultat. Acest aspect implică obţinerea unui sistem steganografic mai sigur.

Pe baza observaţiilor de mai sus şi având în vedere că mesajul secret nu este cunoscut de către un eventual atacator conduce logic la ideea că o prelucrare asupra mesajului va micşora şi mai mult entropia relativă dintre cele două distribuţii. Modul de

prelucrare poate avea un grad foarte mare de flexibilitate depinzând numai şi numai de ingeniozitatea şi posibilităţile de prelucrare ale emiţătorului.

Plecând de la aceste idei, propun în continuare un al doilea model care prevede pe lângă procesarea obiectelor de acoperire, aplicarea unei funcţii de procesare şi asupra mesajului original.

Modelul dezvoltat în figura 6.7 prezintă un grad ridicat de securitate prin faptul că există o procesare atât la nivelul obiectelor de acoperire, reprezentată prin funcţia, $f_{p,}$ cât şi la nivelul mesajului original, reprezentată prin funcţia f_m.

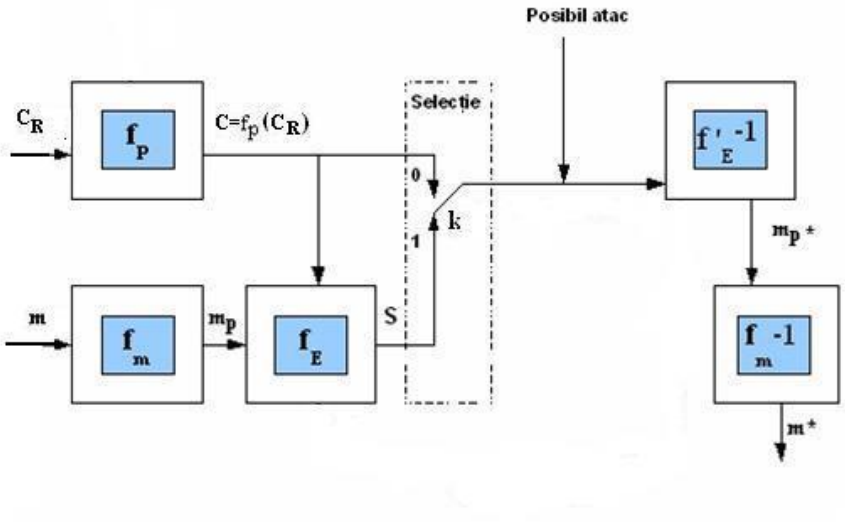


Figura 6.7. Model steganografic cu procesarea obiectului de acoperire şi a mesajului secret

Funcţia de procesare aplicată obiectelor de acoperire este diferită de funcţia de procesare aplicată mesajului secret.

Datorită faptului că acesta este invizibil şi prelucrările efectuate asupra sa pot fi mai complexe spre deosebire de cele aplicate asupra obiectelor de acoperire, care sunt trimise la vedere şi supuse direct unui eventual atac.

Un prim exemplu posibil de prelucrare a informaţiei secrete ar fi împărţirea acesteia în diferite cadrane, după care poate urma amestecarea acestora, astfel încât entropia fiecărui cadran să fie cât mai apropiată de cea a cadranelor din imagine. În felul acesta, vor putea creşte posibilităţile de îndeplinire a condiţiilor necesare în vederea realizării unui proces steganografic cât mai sigur [STA07a].

A doua modalitate de prelucrare a mesajului secret ar fi utilizarea unei funcţii f_m, de procesare directă a acestuia, urmată de încorporarea ulterioară a informaţiei astfel procesate, m_p în obiectul de acoperire. Funcţia de procesare se va alege de aşa manieră încât entropia relativă dintre distribuţiile de probabilitate dintre obiectele de acoperire şi cele steganografice să conducă la o eroare relativă cât mai mică.

O astfel de soluţie a condus la obţinerea unor rezultate foarte bune în special prin scăderea erorii relative dintre mesajul original şi mesajul recuperat la receptor, aşa cum se va vedea în continuare.

A treia modalitate ar consta în distribuirea modului de încorporare a mesajului secret pe baza unor funcţii pseudoaleatoare ce pot fi considerate ca o cheie suplimentară pentru protecţia datelor. Această abordare va fi exemplificată în capitolul 9.

Etapa de extragere a mesajului secret este reprezentată în figura 6.7 de funcţia $f_E^{'-1}$, ce realizează un proces de prelucrare inversă, în care într-o primă etapă, funcţia steganografică inversă f_E^{-1} compusă cu eventuala funcţie de procesare a obiectului de acoperire, f_p^{-1} vor genera atât obiectul de acoperire folosit, cât şi mesajul secret $m_p^{\bullet}$, ce se găseşte într-o fază deocamdată imperceptibilă receptorului, pentru că nu este încă procesat. Mesajul secret $m^{\bullet}$ va rezulta în urma prelucrării funcţiei inverse f_m^{-1}. Menţionez că algoritmul folosit pentru procesarea mesajului va fi cunoscut atât de emiţător, cât şi de receptor.

6.7.1.5 Verificarea experimentală a modelului MPOAM

Mesajul secret este singurul obiect al modelului steganografic care nu trebuie să fie descoperit de către un eventual atacator atât în procesul de transmitere, cât şi în timpul procesului de recuperare al lui. Din acest motiv este de presupus că asupra mesajului secret se pot efectua o serie de operaţii care să conducă la îngreunarea eventualei recuperări a lui de către terţe persoane. În situaţia prezentă privind modelul prezentat mai sus îmi propun să demonstrez că o prelucrare asupra mesajului secret poate conduce la îmbunătăţirea erorii de recuperare a acestuia de către receptor în cazul aplicării algoritmului de recuperare. În acest sens folosindu-mă de acelaşi algoritm $ASAC$ am efectuat o serie de prelucrări asupra mesajului secret ce a fost încorporat în obiectul de acoperire asupra căruia nu am efectuat de astă dată nici un fel de procesare.

Rezultatul prelucrării mesajului secret se prezintă în tabelele 6.4, 6.5 şi 6.6. Semnificaţia coloanelor din aceste tabele este asemănătoare cu cele arătate în tabelele anterioare, cu singura observaţie că de data aceasta prelucrările s-au făcut asupra mesajelor secrete prin deplasarea pixelilor acestora spre negru (întunecarea imaginii) ţinând cont de rezultatele obţinute în paragraful anterior.

Tabel 6.4

Procesare mesaj. Experimente efectuate cu algoritmul steganografic $ASAC$ pe 1 bit

Nr. Crt	Obiect de acoperire		Mesaj secret		Prelucrare obiect de acoperire			
	Nume	**Dimensiune** (pixeli)	**Nume**	**Dimensiune** (pixeli)	$\varepsilon\ la-0$	$\varepsilon\ la-10$	$\varepsilon\ la-20$	%
1	lena	256x256	firefox	128x128	5,27817	5,14270	4,45639	18,44
2	Aquaria	256x256	firefox	128x128	5,27817	5,14270	4,45639	18,44
3	dogs	640x480	wildflowers	200x135	1,33722	1,11358	1.00878	32,55
4	dogs	640x480	watch	200x135	0,77849	0,67695	0,63560	22,48
5	fruit	512x512	lena	256x256	3,29353	3,12670	2,82671	16,51
6	fruit	512x512	Aquaria	256x256	1,69496	1,68684	1,57271	7,77
7	Lena512	512x512	Aquaria	256x256	1,69496	1,68684	1,57271	7,77
8	Lena512	512x512	lena	256x256	3,29353	3,12670	2,82671	16,51
9	building	640x480	wildflowers	200x135	1,33722	1,11358	1.00878	32,55
10	building	640x480	watch	200x130	0,77849	0,67695	0,63560	22,48
11	Alicia	1024x1024	Lena512	512x512	1,69670	1,58939	1,48997	13,87
12	Alicia	1024x1024	fruit	512x512	1,42178	1,38428	1,32253	7,50
13	Alicia	1024x1024	dogs	640x480	0,80019	0,73135	0,69422	15,26
14	car	1024x1036	dogs	640x480	0,80019	0,73135	0,69422	15,26
15	car	1024x1036	fruit	512x512	1,42178	1,38428	1,32253	7,50
16	car	1024x1036	Leno512	512x512	1,25137	1,20761	1,16164	7,72
17	football	1600x1200	building	640x480	1,66823	1,60827	1,47824	12,85
18	football	1600x1200	hawk	800x600	1,77819	1,72532	1,66885	6,55
19	football	1600x1200	sphinx	800x600	4,64491	4,54116	4,38335	5,96
20	fish	1600x1200	building	640x480	1,66823	1,60827	1,47824	12,85
21	fish	1600x1200	hawk	800x600	1,77819	1,72532	1,66885	6,55
22	fish	1600x1200	sphinx	800x600	4,64491	4,54116	4,38335	5,96

Tabel 6.5

Procesare mesaj. Experimente efectuate cu algoritmul steganografic $ASAC$ pe 2 biţi

Nr. Crt	Obiect de acoperire		Mesaj secret		Prelucrare obiect de acoperire			
	Nume	**Dimensiune** (pixeli)	**Nume**	**Dimensiune** (pixeli)	$\varepsilon\ la-0$	$\varepsilon\ la-10$	$\varepsilon\ la-20$	%
1	lena	256x256	merlin	128x128	1,11953	1,06875	0,98156	14,06
2	Lena	256x256	firefox	128x128	5,27817	5,14270	4,45639	18,44
3	Aquaria	256x256	firefox	128x128	5,27817	5,14270	4,45639	18,44
4	Aquaria	256x256	merlin	128x128	1,11953	1,06875	0,98156	14,06
5	Aquaria	256x256	watch	200x135	0,77849	0,67695	0,63560	22,48
6	Lena	256x256	watch	200x135	0,77849	0,67695	0,63560	22,48
7	Lena512	512x512	Aquaria	256x256	1,89496	1,68684	1,57271	7,77
8	fruit	512x512	lena	256x256	3,29353	3,12670	2,82671	16,51
9	fruit	512x512	Aquaria	256x256	1,69496	1,68684	1,57271	7,77
10	sphinx	800x600	fruit	512x512	1,42178	1,38428	1,32253	7,50
11	hawk	800x600	fruit	512x512	1,42178	1,38428	1,32253	7,50
12	Alicia	1024x1024	hawk	800x600	1,77819	1,72532	1,66885	6,55
13	Alicia	1024x1024	sphinx	800x600	4,64491	4,54116	4,38335	5,96
14	car	1024x1036	hawk	800x600	1,77819	1,72532	1,66885	6,55
15	car	1024x1036	sphinx	800x600	4,64491	4,54116	4,38335	5,96
16	fish	1600x1200	Alicia	1024x1024	1,03804	0,85331	0,62588	65,85
17	football	1600x1200	Alicia	1024x1024	1,03804	0,85331	0,62588	65,85
18	football	1600x1200	car	1024x1036	1,23172	1,20449	1,12108	9,86

Tabel 6.6

Procesare mesaj. Experimente efectuate cu algoritmul steganografic $ASAC$ pe 4 biţi

Nr. Crt	Obiect de acoperire		Mesaj secret		Prelucrare obiect de acoperire			
	Nume	**Dimensiune** (pixeli)	**Nume**	**Dimensiune** (pixeli)	$\varepsilon\ la-0$	$\varepsilon\ la-10$	$\varepsilon\ la-20$	%
1	merlin	128x128	firefox	128x128	5,27817	5,14270	4,45639	18,44
2	Wildflowes	200x135	watch	200x135	0,77849	0,67695	0,63560	22,48
3	Lena	256x256	Aquaria	256x256	1,69496	1,68684	1,57271	7,77
4	Aquaria	256x256	lena	256x256	3,29353	3,12670	2,82671	16,51
5	Lena512	512x512	Fruit	512x512	1,42178	1,38428	1,32253	7,50
6	building	640x480	Dogs	640x480	0,80019	0,73135	0,69422	15,26
7	sphinx	800x600	Hawk	800x600	1,77819	1,72532	1,66885	6,55
8	hawk	800x600	Sphinx	800x600	4,64491	4,54116	4,38335	5,94
9	Alicia	1024x1024	Car	1024x1036	1,71707	1,64837	1,52477	12,61
10	car	1024x1036	Alicia	1024x1024	1,03804	0,85331	0,62588	65,85
11	fish	1600x1200	football	1600x1200	1.09190	1,00797	0,7278	50,02

În urma aplicării algoritmului $ASAC$ pe 1 bit (tabelul 6.4), pe 2 biţi (tabelul 6.5), respectiv pe 4 biţi (tabelul 6.6) am constat că în urma recuperării mesajului secret eroarea relativă dintre acesta şi mesajul original se îmbunătăţeşte semnificativ, obţinându-se astfel îmbunătăţiri de până la 65%.

Evident că plaja erorilor îmbunătăţite depinde în mod semnificativ de tipologia mesajului ce urmează a fi încorporat. Spre exemplu, dacă mesajul conţine mulţi pixeli cu valori ce se apropie de culoarea negru, îmbunătăţirea erorii este semnificativă, iar în situaţia în care mesajul secret conţine pixeli cu valori mai apropiate de culoarea alb, aceste îmbunătăţiri sunt mai puţin semnificative.

În toate exemplele utilizate am constatat că indiferent de tipul mesajului ascuns se obţine o îmbunătăţire a erorilor relative la recuperarea acestuia. Mai mult, eroarea relativă nu este dependentă de dimensiunea mesajului ascuns şi nici de dimensiunea obiectului de acoperire.

O altă constatare remarcată constă în faptul că indiferent de tipul algoritmului $ASAC$ utilizat la recuperarea mesajului se obţin aceleaşi erori. Concluzia pe care o pot trage constă în faptul că eroarea obţinută în cazul mesajului recuperat este dependentă de tipul acestuia, cât şi de ponderea pixelilor apropiaţi de culoarea negru.

În figura 6.8 prezint un exemplu în care prelucrarea s-a efectuat asupra mesajului secret original prin deplasarea pixelilor acestuia spre culoarea alb (figura 6.8.b), respectiv negru (figura 6.8.c). În urma acestor prelucrări am constat o îmbunătăţire a raportului de recuperare a mesajului secret de 22,5%, rezultat ce se regăseşte în tabelul 6.6, linia 2.

a)Mesaj original neprelucrat Mesaj recuperat

b)Mesaj original cu deplasare spre alb Mesaj recuperat

c)Mesaj original cu deplasare spre negru Mesaj recuperat

Figura 6.8 Exemplu de prelucrare a mesajului

În situaţia în care prelucrarea se efectuează atât asupra obiectului de acoperire, cât şi a mesajului secret, am constatat că observaţiile menţionate mai sus se păstrează şi în cazul acesta în sensul că deplasarea obiectului de ascundere spre

culoarea neagră îmbunătăţeşte eroarea dintre obiectul steganografic şi obiectul de acoperire, iar deplasarea spre negru a mesajului îmbunătăţeşte eroarea de recuperare a mesajului. Mai mult, aceste aspecte se întâmplă simultan în cazul prelucrării atât a obiectului de acoperire, cât şi a mesajului secret.

Pentru exemplificare voi arăta în tabelele 6.7, 6,8 şi 6.9 doar 3 astfel de prelucrări. Menţionez că şi în cazul celorlalte câtorva zeci de prelucrări pe care le-am efectuat rezultatele au aceeaşi tendinţă.

În tabelul 6.7 este dat un exemplu pentru un obiect de acoperire reprezentat printr-o imagine digitală color de dimensiunea 640 x 480 pixeli, iar mesajul secret încorporat constituie tot o imagine digitală color de dimensiune 200 x 135 pixeli.

Tabel 6.7 Exemplu de prelucrare a obiectului de acoperire şi a mesajului secret folosind algoritmul *ASAC* pe 1 bit

Nr.crt.	Mesaj secret	Obiect de acoperire
1	fara prelucrarea mesajului ε=0,778499	prelucrarea obiectului de acoperire ε la -10 : 0,187311 ε la -8 : 0,188259 ε la -6 : 0,189305 ε la -4 : 0,190402 ε la -2 : 0,191885 ε la 0 : 0,195865 ε la +2 : 0,199360 ε la +4 : 0,200855 ε la +6 : 0,202012 ε la +8 : 0,203152 ε la +10 : 0,204229
2	prelucrarea mesajului : -10 ε=0,676959	prelucrarea obiectului de acoperire ε la -10 : 0,187166 ε la -8 : 0,188111 ε la -6 : 0,189155 ε la -4 : 0,190256 ε la -2 : 0,191749 ε la 0 : 0,195726 ε la +2 : 0,199056 ε la +4 : 0,200475 ε la +6 : 0,201589 ε la +8 : 0,202667 ε la +10 : 0,203721
3	prelucrarea mesajului : -20 ε=0,635603	prelucrarea obiectului de acoperire ε la -10 : 0,187157 ε la -8 : 0,188108 ε la -6 : 0,189147 ε la -4 : 0,190242 ε la -2 : 0,191747 ε la 0 : 0,195725 ε la +2 : 0,199050 ε la +4 : 0,200449 ε la +6 : 0,201559 ε la +8 : 0,202617 ε la +10 : 0,203687

În urma prelucrării atât a mesajului secret, cât şi a obiectului de acoperire se constată o îmbunătăţire a recuperării mesajului secret de aproximativ 22,48% în comparaţie cu mesajul secret neprelucrat. Pe de altă parte obiectul steganografic prezintă o îmbunătăţire de 9,12% în comparaţie cu cazul în care obiectul de acoperire nu este prelucrat. Menţionez că mesajul secret a fost prelucrat printr-o

deplasare din 10 în 10 a fiecărui pixel spre negru, pe când obiectul de acoperire a fost deplasat cu valori din 2 în 2 atât spre negru cât şi spre alb. Am constat că deplasarea spre negru duce atât la îmbunătăţirea raportului de recuperare a mesajului secret, cât şi la îmbunătăţirea obiectului steganografic.

În tabelul 6.8 este dat un exemplu pentru un obiect de acoperire reprezentat printr-o imagine digitală color de dimensiunea 800 x 600 pixeli, iar mesajul secret încorporat constituie tot o imagine digitală color de dimensiune 512 x 512 pixeli. Modul de prelucrare s-a efectuat ca şi în exemplul anterior obţinându-se o îmbunătăţirea a raportului mesajului recuperat de 25,54% comparativ cu situaţia în care acesta nu a fost prelucrat. În cazul obiectului steganografic s-a obţinut o îmbunătăţire de 7,06% în comparaţie cu situaţia în care obiectul de acoperire nu a fost prelucrat.

Tabel 6.8 Exemplu de prelucrare a obiectului de acoperire şi a mesajului secret folosind algoritmul *ASAC* pe 2 biţi

Nr.crt.	Mesaj secret	Obiect de acoperire
1	fara prelucrarea mesajului ε=1,421784	prelucrarea obiectului de acoperire ε la -10 : 0,504149 ε la -8 : 0,520862 ε la -6 : 0,504159 ε la -4 : 0,520865 ε la -2 : 0,504159 ε la 0 : 0,520865 ε la +2 : 0,529569 ε la +4 : 0,533377 ε la +6 : 0,534816 ε la +8 : 0,536720 ε la +10 : 0,537294
2	prelucrarea mesajului : -10 ε=1,384285	prelucrarea obiectului de acoperire ε la -10 : 0,503384 ε la -8 : 0,519614 ε la -6 : 0,503397 ε la -4 : 0,519617 ε la -2 : 0,503396 ε la 0 : 0,519617 ε la +2 : 0,528330 ε la +4 : 0,532013 ε la +6 : 0,533548 ε la +8 : 0,535328 ε la +10 : 0,536060
3	prelucrarea mesajului : -20 ε=1,132530	prelucrarea obiectului de acoperire ε la -10 : 0,501953 ε la -8 : 0,518559 ε la -6 : 0,501968 ε la -4 : 0,518562 ε la -2 : 0,501970 ε la 0 : 0,518562 ε la +2 : 0,527786 ε la +4 : 0,531351 ε la +6 : 0,533191 ε la +8 : 0,534754 ε la +10 : 0,535878

Tabel 6.9 Exemplu de prelucrare a obiectului de acoperire şi a mesajului secret folosind algoritmul *ASAC* pe 4 biţi.

Nr.crt.	Mesaj secret	Obiect de acoperire
1	fara prelucrarea mesajului ε=0,800194	prelucrarea obiectului de acoperire ε la -10 : 2,361944 ε la -8 : 2,357427 ε la -6 : 2,66775 ε la -4 : 2,389200 ε la -2 : 2,429299 ε la 0 : 2,478860 ε la +2 : 2,502242 ε la +4 : 2,533042 ε la +6 : 2,559920 ε la +8 : 2,578005 ε la +10 : 2,601133
2	prelucrarea mesajului : -10 ε=0,731351	prelucrarea obiectului de acoperire ε la -10 : 2,367609 ε la -8 : 2,366596 ε la -6 : 2,374465 ε la -4 : 2,397374 ε la -2 : 2,437545 ε la 0 : 2,488185 ε la +2 : 2,511806 ε la +4 : 2,541580 ε la +6 : 2,569289 ε la +8 : 2,591867 ε la +10 : 2,614072
3	prelucrarea mesajului : -20 ε=0,694220	prelucrarea obiectului de acoperire ε la -10 : 2,359342 ε la -8 : 2,359459 ε la -6 :2,371537 ε la -4 : 2,396896 ε la -2 : 2,437531 ε la 0 : 2,488804 ε la +2 :2,511648 ε la +4 :2,541081 ε la +6 :2,568793 ε la +8 : 2,590085 ε la +10 : 2,614960

În tabelul 6.9 a fost dat un exemplu pentru un obiect de acoperire reprezentat printr-o imagine digitală color de dimensiunea 640 x 480 pixeli, iar mesajul secret încorporat constituie tot o imagine digitală color de dimensiune 640 x 480 pixeli. Şi în acest exemplu se constată o îmbunătăţire a recuperării mesajului secret cu 15,26% faţă de situaţia în care acesta nu e prelucrat, respectiv o îmbunătăţire de 10, 83% a obiectului steganografic faţă de situaţia în care obiectul de acoperire folosit nu este prelucrat.

În concluzie, pot spune că pentru toate exemplele utilizate am constatat îmbunătăţiri în ceea ce priveşte atât recuperarea mesajului secret, cât şi a obiectului steganografic comparativ cu situaţiile în care obiectul de acoperire, respectiv mesajul secret nu sunt prelucrate, ceea ce confirmă faptul că cele două variante ale modelului propus de mine pot conduce la îmbunătăţirea sistemelor steganografice. Menţionez că modalitatea de prelucrare a mesajului secret şi a obiectului de acoperire, nu constituie un obiect de sine stătător. Modalitatea de prelucrare aleasă a fost relativ simplă dorind doar să verific în acest moment valabilitatea modelului propus, însă poate constitui o direcţie de cercetare viitoare pentru găsirea celor mai bune soluţii de prelucrare în acest sens.

6.7.2 Concluzii privind comportarea modelelor MPOA şi MPOAM

Pe baza rezultatelor obţinute şi a observaţiilor constatate mi-am propus să realizez un set de algoritmi steganografici care să înglobeze totalitatea principiilor de

funcţionare a celor două modele prezentate. În acest sens am conceput algoritmi steganografici care să acopere domeniile de reprezentare ale imaginilor şi care să prevadă posibilitatea de prelucrare atât a obiectului de ascundere, cât şi al mesajului secret. Scopul urmărit constă în îmbunătăţirea obiectului steganografic, a recuperării cu fidelitate sporită a mesajului secret, a creşterii cantităţii de informaţie ce poate fi ascunsă fără a afecta proprietăţile menţionate anterior.

Menţionez că toţi algoritmii dezvoltaţi de mine prezintă într-o formă sau alta aspecte legate de procesarea obiectului de acoperire şi/sau a mesajului secret. În mod evident se pot imagina foarte multe idei de procesare, în schimb problema care se pune constă în faptul că acestea sunt mari consumatoare de timp. În situaţia în care aceşti algoritmi steganografici trebuie să lucreze în timp real se pune problema ca etapele de procesare a obiectului steganografic, a mesajului secret şi de generare a obiectului steganografic să fie executate într-un interval de timp cât mai scurt. Din acest motiv am considerat că este mai prioritar ca aceste prelucrări multiple să fie executate într-un timp cât mai scurt pentru a putea fi implementate sub formă concretă, cum ar fi un telefon mobil. Efortul depus în acest sens a constat în găsirea unor soluţii optime a tuturor proprietăţilor implicate în procesul steganografic, cum ar fi: timpul de execuţie al algoritmului, cantitatea de informaţii ce poate fi ascunsă, modul de protejare a mesajului secret încorporat, generarea unui obiect steganografic care să nu trezească suspiciuni, timpul necesar recuperării mesajului secret. Aceste obiective au călăuzit generarea algoritmilor steganografici expuşi în capitolele 7, 8 şi 9.

6.8 *Concluzii*

În acest capitol într-o primă etapă s-a elaborat un studiu de sinteză privind principalele modele steganografice existente la ora actuală în literatura de specialitate plecându-se de la problema prizonierilor care tratează unitar esenţa ideii de steganografie, respectiv transmiterea unei informaţii secrete între două persoane printr-un mesaj transmis la vedere şi care să nu trezească suspiciuni că ar conţine şi alte informaţii decât cele vizibile.

Pornind de la această idee ţinând cont de evoluţia tehnologiei de transmitere a informaţiilor şi de posibilitatea utilizării unor diferiţi algoritmi de ascundere a fost dezvoltat un model steganografic de bază şi enumerate principalele criterii pe care trebuie să le îndeplinească un astfel de model. Plecând de la modelul de bază au fost dezvoltate şi alte modele steganografice prin care s-au enunţat principiile teoretice legate de securitatea acestora.

Astfel, în cazul modelului încorporat dezvoltat de Zollner s-a analizat gradul de securitate a unui model steganografic în funcţie de diferenţa dintre entropia relativă a obiectului steganografic obţinut după încorporarea mesajului secret şi a obiectului de acoperire original.

Rezultatul studiului conduce la concluzia că procesul steganografic devine sigur atunci când diferenţa dintre cele două entropii relative tinde spre zero. Obţinerea unei astfel de cerinţe a condus la dezvoltarea unui model steganografic nedeterminist prin care se propune ca obiectul de acoperire să fie generat în mod aleator pentru a creşte astfel gradul de incertitudine asupra lui. Mai mult, se sugerează că orice prelucrare făcută asupra obiectului de acoperire ales va mări şi mai mult această incertitudine, ceea ce va îngreuna căutarea şi găsirea mesajului secret de către un eventual atacator. Soluţia rezultată în urma analizei făcută de autor conduce la concluzia că un proces steganografic are un grad de securitate

ridicat dacă obiectul de acoperire nu este cunoscut de către un eventual atacator.

Cachin dezvoltă un nou model steganografic prin care propune ca pe canalele de transmisie să fie trimis un set de obiecte de acoperire, urmând ca doar în unele dintre acestea să fie încorporat mesajul secret pentru a induce în eroare un eventual atacator în cazul în care acesta analizează setul de obiecte primite. În ceea ce priveşte securitatea modelului propus se face o analiză teoretică dezvoltată pe baza distribuţiilor de probabilitate corespunzătoare obiectelor steganografice, respectiv obiectelor de acoperire.

Concluzia la care a ajuns autorul constă în afirmaţia că un astfel de sistem steganografic este sigur atunci când diferenţa dintre cele două distribuţii de probabilitate este zero. Constatând însă că o astfel de condiţie este imposibil de realizat din punct de vedere practic se admite ca diferenţa dintre distribuţiile de probabilitate să tindă spre o valoare ε cât mai mică. Chiar şi cu această menţiune este de precizat că un astfel de model matematic face abstracţie de mediile purtătoare utilizate în mod practic pentru realizarea obiectului steganografic deoarece acestea au distribuţiile de probabilitate mai complexe, nu sub o formă ideală aşa cum este considerat de către autor.

Pornind de la ideile prezentate în modelele matematice amintite în acest capitol am dezvoltat un model steganografic cu două variante de prezentare. În prima variantă propun ca dintr-un set de obiecte de acoperire să se aleagă în mod aleator un număr de astfel de obiecte în care urmează să se încorporeze informaţie secretă. Precizez că fiecare obiect de acoperire este procesat înainte de încorporarea mesajului şi menţionez faptul că datele secrete se vor însera doar în unele dintre acestea. În continuare se vor trimite către emiţător atât obiectele de acoperire, cât şi obiectele steganografice. În acest fel, unui eventual atacator îi va fi foarte dificil de a determina care dintre obiecte conţine mesajul secret.

Funcţia de procesare adăugată obiectelor de acoperire va conduce la creşterea dificultăţii extragerii mesajului secret de către o persoană neautorizată.

Modelul steganografic astfel conceput a fost demonstrat din punct de vedere matematic în sensul că diferenţa distribuţiilor de probabilitate scade odată cu efectuarea unei funcţii de procesare asupra obiectelor de acoperire.

Din punct de vedere practic modelul a fost testat pe un set de imagini digitale, iar rezultatele obţinute confirmă faptul că în urma procesării obiectelor de acoperire sistemul steganografic prezintă o îmbunătăţire faţă de situaţia cazului în care obiectele de acoperire nu sunt prelucrate. Acest fapt se evidenţiază prin scăderea erorii relative dintre obiectul steganografic şi obiectul de acoperire, atingând astfel un raport de până la 13%, ceea ce face ca diferenţa dintre acestea să nu fie vizibilă, deci să nu creeze suspiciuni.

În a doua variantă a modelului propus pe lângă prelucrarea obiectelor de acoperire am propus şi o prelucrare asupra mesajului secret. Menţionez că asupra acestuia se pot efectua prelucrări cu un grad de complexitate mult mai mare decât asupra obiectului de acoperire, deoarece acesta nu este vizibil. Sub acest aspect, prelucrarea mesajului conduce la îngreunarea extragerii acestuia de către un eventual atacator, iar pe de altă parte permite îmbunătăţirea ratei de recuperare a acestuia.

Din punct de vedere practic şi această variantă a modelului a fost testată pe un set de imagini digitale şi a confirmat faptul că un anumit gen de prelucrare conduce în mod vizibil la creşterea gradului de recuperare a mesajului de până la 65% în condiţiile utilizării unor imagini adecvate ca şi obiecte de acoperire.

7 STEGANOGRAFIA ÎN DOMENIUL SPAŢIAL

Aşa cum au fost dezvoltate diferite modalităţi de reprezentare şi de transformare a imaginilor digitale, de-a lungul timpului au fost generaţi şi implementaţi algoritmi steganografici într-un anumit domeniu de reprezentare.

Una din tehnicile des utilizate o constituie metoda substituţiei prin care sunt obţinute rezultatele cele mai bune în domeniul steganografiei, iar prin îmbinarea cu algoritmi de ascundere dezvoltaţi în domeniul spaţial, aceasta conduce până în prezent la cele mai numeroase soluţii steganografice.

Algoritmii steganografici în domeniul spaţial prezintă avantajul că sunt relativ uşor de implementat, oferă o diversitate extrem de mare, asigură o cantitate mare de informaţie ascunsă şi pot fi combinaţi cu algoritmi specifici altor domenii de reprezentare. Ca un dezavantaj îl constituie faptul că aceşti algoritmi sunt relativ cunoscuţi, ceea ce îi predispune la diferite atacuri, unele având chiar şi succes. Cu toate acestea în steganografie se caută noi soluţii pentru îmbunătăţirea algoritmilor în reprezentarea spaţială şi acest lucru are ca mărturie numeroase lucrări din acest domeniu.

O tendinţă remarcată în ultima vreme constă în implementarea algoritmilor pe microprocesoare sau generarea unor circuite dedicate acestui scop. Ideea ce se desprinde din această tendinţă constă în faptul că echipamentele hardware pot fi prevăzute cu elemente suplimentare ce pot împiedica atacul asupra obiectului steganografic.

Tehnicile de ascundere a informaţiilor în imaginile digitale reprezentate în domeniul spaţial încorporează datele secrete direct în biţii imaginii aleasă ca obiect de acoperire, fără a implica o transformare a domeniului spaţial în alte domenii.

Cei mai cunoscuţi algoritmi steganografici ce folosesc tehnica domeniului spaţial sunt: LSB (Least Significant Bit), YUV, BPCS (Bit-Plane Complexity Segmentation Steganography) şi vor fi prezentaţi mai pe larg în cele ce urmează.

7.1 *Algoritmi steganografici bazaţi pe ascunderea informaţiei în cei mai puţini semnificativi biţi (LSB-P)*

Una dintre cele mai timpurii şi cele mai des folosite tehnici ale domeniului spaţial este cea numită inserarea în cel mai puţin semnificativ bit cunoscută sub denumirea de LSB (Least Significant Bit) [SUN07]. Metoda este foarte populară datorită faptului că este uşor de implementat şi prezintă o flexibilitate mare de aplicare. Din acest motiv, cu toate că algoritmul e relativ simplu, prin diversitatea sa această metodă continuă să fie utilizată pe larg. Prin ascunderea informaţiei secrete în bitul (biţii) cei mai puţin semnificativi ai obiectului de acoperire se obţin două caracteristici importante: se pot masca o cantitate mare de informaţii şi/sau se poate recupera într-o proporţie mare mesajul iniţial. Sigur există şi un dezavantaj, în sensul că bruierea mesajului steganografic face dificilă recuperarea mesajului ascuns de către receptor.

Algoritmul LSB este un algoritm relativ simplu, iterativ şi funcţionează după următorul principiu: biţii cei mai puţini semnificativi ai fiecărui pixel dintr-o imagine purtătoare, se înlocuiesc cu biţi ai informaţiei secrete ce se doreşte a fi ascunsă. În principiu se iau biţii cei mai semnificativi ai mesajului secret sau chiar toţi biţii mesajului secret. Această tehnică permite ascunderea unei cantităţi destul de mari de informaţie şi poate fi dezvoltată în diferite variante plecând de la reprezentarea în domeniul spaţial atât a obiectului de acoperire, cât şi a mesajului secret ce urmează a fi ascuns. În funcţie de modalitatea de încorporare a mesajului secret în obiectul de acoperire pentru a obţine obiectul steganografic se pot obţine o diversitate relativ mare de rezultate în funcţie de situaţia concretă de rezolvare.

Metoda se aplică atât imaginilor color pe 24 de biţi, cât şi a celor alb-negru pe 8 biţi. Ideea se bazează pe convingerea generală că, schimbările făcute în cadrul celui mai puţin semnificativ bit din culorile existente nu pot fi detectate, de un observator. Eventualele neclarităţi pot fi interpretate ca zgomote legate de transmitere, care pot fi prezente tot timpul în imaginile digitale [FRI01].

O metodă steganografică ce foloseşte tehnica de ascundere LSB în domeniul transformatei de undă cu o capacitate mare de ascundere şi o eroare relativă mică pentru un semnal audio este prezentată în [SHA07a]. Capacitatea de ascundere menţionată este de 200 de kbiţi-per-secundă (kbps) cu o rată de eroare de 0,3%.

[YAN08, JUN08] propun metode steganografice în care mesajele secrete sunt ascunse în cei mai puţini semnificativi biţi folosind valorile diferenţiale ale pixelilor imaginilor de acoperire alese. Aceste metode permit ascunderea unei capacităţi mari de informaţie şi au ca rezultat imagini steganografice de o foarte bună calitate.

Un algoritm steganografic ce foloseşte metoda LSB este propus în [POR08] pentru imagini în format GIF.

Autorii din [RAJ05] prezintă un algoritm steganografic bazat pe metoda bitului cel mai puţin semnificativ combinată cu transformata cosinus discretă şi tehnici de compresie pentru a spori securitatea imaginii steganografice.

În [AND05] imaginile digitale sunt folosite pentru ascunderea unei informaţii secrete folosind bitul cel mai puţin semnificativ a unui alt mesaj constituit tot dintr-o imagine digitală. Metoda propusă prezintă robusteţe la steganaliză pentru toate cazurile analizate în articol.

Este cunoscut faptul că toate metodele de ascundere de informaţie care modifică cei mai puţini semnificativi biţi, introduc distorsiuni în obiectele de acoperire. În [KIM07] se propune un algoritm ce foloseşte pentru încorporarea datelor secrete numai coeficienţi ai căror modificare nu introduce mari distorsiuni. În acest sens se foloseşte o codificare matricială pentru a alege coeficienţii ai căror modificare să introducă distorsiunea cea mai mică în urma inserării.

Necesitatea dezvoltării unor metode de protecţie a convorbirilor particulare a facilitat începerea unei serii de cercetări în vederea conceperii unor codoare şi decodoare steganografice care să fie ataşate sistemelor mobile. Ca primă încercare s-au utilizat FPGA - urile ca modalitate de simulare a unor astfel de dispozitive. Din nefericire FPGA - urile implică costuri mari şi nu sunt adaptate pentru a fi integrate în microprocesoarele utilizate în telefonia mobilă.

O arhitectură hardware de implementare a unei tehnici steganografice în care mesajul este ascuns în modificările abrupte de la alb la negru este prezentată în lucrarea [GOM08]. Utilizarea FPGA - urilor a condus la creşterea vitezei de procesare.

Autorii din [FAR04] folosesc pentru ascunderea mesajului o cheie secretă pentru a creşte siguranţa protecţiei mesajului ascuns.

Pentru protejarea proprietăţii intelectuale este propusă în [LAC99] utilizarea steganografiei prin folosirea unui FPGA în vederea inserării unui watermark.

Pe lângă aceste încercări în vederea conceperii unui codor şi decodor hard, în [SUZ08] autorii au conceput un algoritm de protecţie privind interconectarea unei camere de luat vederi cu un mobil şi cu un laptop PC. Transferul de date se poate realiza doar pe baza cunoaşterii algoritmului de ascundere între echipamentele menţionate.

În lucrările enumerate mai sus, algoritmii steganografici bazaţi pe ascunderea unor informaţii în biţii cei mai puţini semnificativi prin utilizarea FPGA-urilor nu au condus la realizarea efectivă a unor dispozitive steganografice cu utilitate practică, fiind doar implementările unor algoritmi prin care s-a încercat îmbunătăţirea performanţelor acestora.

Pentru a veni în întâmpinarea unui astfel de deziderat mi-am propus implementarea unor algoritmi steganografici pe microprocesoare utilizate în telefonia mobilă. În acest sens algoritmii implementaţi pe calculator am încercat să-i adaptez scopului menţionat mai sus, şi anume: să prezinte atât caracteristici legate de capacitatea limitată a memoriei a unui procesor folosit în telefonia mobilă, cât şi satisfacerea cerinţelor legate de codarea şi decodarea algoritmilor steganografici în timp real. Pentru toate acestea trebuie păstrate caracteristicile esenţiale ale steganografiei: invizibilitatea mesajului, recuperarea mesajului în condiţii cât mai bune, capacitate mare de ascundere.

Un prim rezultat de succes a fost prezentat în lucrarea [STA09] în care a fost adaptat pentru un microprocesor din familia ARM frecvent utilizat în telefonia mobilă un algoritm de încorporare a unui mesaj secret în biţii cei mai puţini semnificativi (LSB-P). Rezultatele obţinute confirmă faptul că algoritmul pe microprocesor permite îmbunătăţirea semnificativă a timpului de execuţie, ceea ce conduce la ideea că acesta poate fi executat chiar şi în timp real.

7.1.1 Algoritm de ascundere pe un bit (LSB-P_1)

Algoritmul LSB-1 foloseşte cel mai puţin semnificativ bit al obiectului de acoperire tip imagine pentru a ascunde informaţia secretă în el. Probabilitatea ca acest bit să se modifice faţă de valoarea lui iniţială este de 0,5.

Tot procesul de ascundere este realizat la nivel de biţi în obiectul de acoperire, iar pentru ca informaţia să nu se piardă trebuie ales un format corespunzător pentru imaginile implicate. Este cunoscut faptul că imaginile sunt disponibile sub diverse formate, cum ar fi: TGA, GIF, JPEG, BMP, etc. Pentru implementarea algoritmului sunt necesare date ce caracterizează matricea de pixeli atât a obiectului de acoperire, cât şi a mesajului secret. Altfel spus, dacă se cunoaşte organizarea internă a formatului se poate afla matricea de pixeli, doar prin citirea binară a acestuia. Din antet se obţin informaţii despre dimensiunile imaginii precum şi despre locul de unde încep efectiv biţii ce reprezintă imaginea (matricea propriu zisă de pixeli).

Dacă se folosesc imagini color, matricea de pixeli care este practic formată dintr-o matrice de puncte colorate, iar cum fiecare punct de culoare e format din procente ale celor trei culori de bază: roşu (Red - R), verde (Green - G) şi albastru (Blue - B), la fel şi pixelul este format din 3 canale sau vectori de biţi R, G, B. Astfel că pentru procesul de ascundere toţi cei 3 biţi, mai puţin semnificativi ai obiectului

de ascundere, din fiecare pixel vor fi înlocuiţi cu biţii (cei mai semnificativi) ai mesajului secret. Ochiul uman nu poate vedea că imaginea rezultată este diferită de cea iniţială, deoarece nu poate distinge o diferenţă nesemnificativă (0,39%) într-unul din canalele de culoare.

Este cunoscut faptul că substituirea LSB care este folosită cel mai des în steganografie degradează semnificativ calitatea obiectului de acoperire în momentul încorporării unei cantităţi mari de informaţie. În vederea rezolvării unei astfel de probleme în [RON06] se propune o metoda de mapare a blocurilor LSB bazată pe un algoritm ce aplică regula selectării celei mai bune mărimi a blocurilor.

Ideea principală urmărită în această lucrare este de a minimiza degradarea imaginii steganografice prin găsirea celei mai bune funcţii de mapare ce face legătura între blocurile corespunzătoare obiectului de acoperire şi cele ale imaginii secrete.

Algoritmul de ascundere

O privire de ansamblu a algoritmului LSB pe 1 bit se prezintă în figura 7.1.

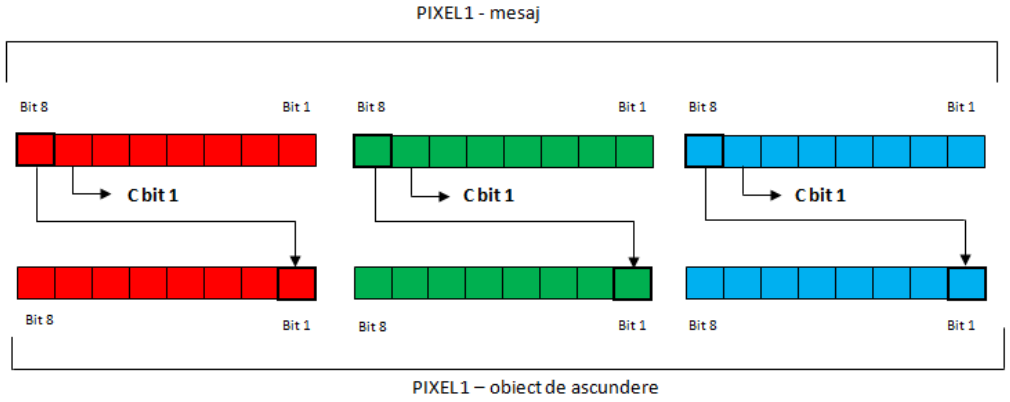


Figura 7.1. Algoritmul LSB pe 1 bit

Procedura teoretică a algoritmului steganografic LSB-1 poate fi descrisă în următorii paşi:

1) Extragerea matricei de pixeli dintr-o imagine.
2) Reprezentarea pe biţi a fiecărui pixel a obiectului imagine.
3) Reprezentarea pe biţi a mesajului ce urmează a fi ascuns.
4) Încorporarea fiecărui bit al mesajului secret în cel mai puţin semnificativ bit al fiecărui pixel din imaginea de acoperire

Practic se parcurg toate câmpurile obiectului de acoperire, iar la fiecare iteraţie se ia următorul bit din imaginea de ascuns şi se suprascrie peste cel mai puţin semnificativ bit al câmpului curent al imaginii în care se ascunde. În situaţia implementării algoritmului pe microprocesoare s-au efectuat modificări de aşa manieră încât să se valorifice particularităţile funcţionale ale acestora.

În cazul microprocesorului ARM pentru a beneficia de arhitectura bazată pe asamblare au fost evitate instrucţiunile de salt permiţând microprocesorului să poată opera liniar în majoritatea situaţiilor, ceea ce conduce la executarea tuturor operaţiilor într-un singur ciclu de maşină. Ca urmare a acestor adaptări ce au condus practic la generarea unui alt algoritm s-au obţinut timpi de execuţie de 3 ori

mai buni în comparaţie cu implementarea aceluiaşi algoritm pe un PC ce are performanţe comparabile cu a microprocesorului ARM.

Pentru implementarea pe microprocesorul ISAAC ce permite executarea în paralel a operaţiilor pe mai multe unităţi de procesare simultan, algoritmul a fost adaptat de aşa manieră încât să permită executarea lui în secvenţe paralele. Gestionarea procesării în paralel pe 6 unităţi de procesare s-a efectuat prin împărţirea imaginii în secvenţe de operare paralelă pentru cele 6 unităţi de procesare prin executarea algoritmului într-un astfel de mod în care prima linie din matricea imagine să fie executată de prima unitate de procesare, a doua linie de cea de-a doua unitate de procesare, ş.a.m.d. În final rezultatul executării algoritmului de ascundere s-a concatenat într-o imagine steganografică.

Managementul executării paralelismului este coordonat de cel de-al 8-lea nucleu de procesare care la rândul lui trebuie să fie coordonat de modificările ce au fost aduse în algoritmul de ascundere pe biţii cei mai puţini semnificativi în aşa fel încât să se utilizeze toate facilităţile microprocesorului. În principiu modalitatea de paralelizare poate fi utilizată şi pe alte microprocesoare cu mai multe unităţi de prelucrare efectuându-se eventual mici adaptări specifice arhitecturii particulare a acestora, în special în zona de organizare.

Toate modificările aduse asupra algoritmului pentru microprocesorul ARM şi ISAAC au fost realizate asupra tuturor algoritmilor bazaţi pe bitul cel mai puţin semnificativ. Consider ca aceste modificări sunt benefice deoarece conduc la îmbunătăţirea timpului de execuţie în mod spectaculos, respectiv de 3 ori pentru microprocesorul ARM şi de 8 ori pentru microprocesorul ISAAC. Rezultatele experimentale vor fi prezentate mai jos.

Algoritmul de extragere

Pentru extragerea mesajului secret se aplică procedura inversă caracteristică algoritmului de ascundere şi implică următorii paşi:

1) Extragerea matricei de pixeli din imaginea steganografică.
2) Extragerea ultimului bit al câmpului curent, bit care este apoi înserat în următoarea poziţie din mesajul ascuns.
3) Reconstituirea mesajului ascuns bit cu bit.

Pentru a putea face comparaţii între rezultatele obţinute în urma procesului steganografic se defineşte ca şi parametru de calcul eroarea relativă, notată cu ε_{rel}.

Formula de calcul pentru eroarea relativă este:

$$\varepsilon_{rel} = \frac{\sum_{i=1}^{m\times n}\left(\frac{|R-R^*|}{255}+\frac{|G-G^*|}{255}+\frac{|B-B^*|}{255}\right)}{3\times m\times n}\times 100\% \quad (7.1.)$$

R, G, B reprezintă cele trei componente de culoare ale pixelilor mesajului iniţial ce urmează a fi ascuns sau a obiectului de acoperire;

R*, G*, B* reprezintă cele trei componente de culoare ale pixelilor mesajului recuperat la recepţie sau a obiectului steganografic.

Metoda prezintă avantajul că eroarea relativă dintre obiectul de acoperire şi cel steganografic se reduce la 0,39%, în schimb cantitatea de informaţie ce poate fi

introdusă este de 12,5% în cazul în care mesajul este format dintr-o imagine color şi 37,5% în cazul în care mesajul este o imagine alb-negru. Eroarea relativă dintre mesajul iniţial şi mesajul recuperat tinde la zero dacă obiectul steganografic nu a fost afectat de zgomot.

7.1.2 Algoritm de ascundere pe 2 biţi (LSB-P_2)

În cazul în care se doreşte ascunderea unei cantităţi mai mari de informaţie, tehnica LSB poate fi extinsă prin încorporarea datelor secrete şi în biţii de ordin superior ai fiecărui pixel. Înlocuind astfel cei mai puţin semnificativi N biţi ai fiecărui pixel cu informaţie de ascuns va creşte de N ori capacitatea de încorporare. Ca urmare, intensitatea fiecărui pixel variază corespunzător cu numărul de biţi înlocuiţi, iar din acest motiv metoda nu ar trebui să fie extinsă la biţii de ordin superior fără discriminare.

Algoritmul ar consta în astfel de situaţii în înlocuirea celor N biţi mai puţini semnificativi ai fiecărui pixel din obiectul de acoperire cu biţii mai semnificativi ai mesajului secret [MIE06]. În acest caz biţii mai puţini semnificativi ai obiectului de acoperire se vor pierde, la fel ca şi biţii mai puţini semnificativi ai mesajului ascuns.

Procesul de substituţie realizat prin încorporarea datelor secrete în cei 2 cei mai puţin semnificativi biţi, şi nu doar în cel mai puţin semnificativ bit, prezintă dezavantajul că în timpul procesului de ascundere sunt alteraţi mai mulţi biţi, iar aceasta implică şi creşterea gradului de distorsionare a imaginii. Algoritmul presupune de astă dată înlocuirea primilor doi biţi cei mai puţini semnificativi ai pixelilor din imaginea considerată obiect de acoperire, cu primii doi biţi mai semnificativi ai mesajului secret. Următorii 2 biţi ai mesajului luaţi în ordinea semnificaţiei se înlocuiesc în biţii mai puţini semnificativi ai pixelului următor.

Metoda LSB pe 2 biţi poate prezenta un număr relativ mare de variante în funcţie de scopul urmărit. De exemplu, dacă se doreşte ascunderea unei cantităţi mai mare de informaţie pot fi neglijaţi biţii mai puţini semnificativi din mesaj, în schimb dacă se doreşte o recuperare cu o eroare cât mai mică a mesajului secret, trebuie încorporaţi toţi biţii acestuia. În acest caz cantitatea de informaţie ascunsă va scădea în mod evident. Varianta aleasă depinde şi de tipul obiectului de acoperire utilizat.

Procesul de înlocuire LSB pe 2 biţi este prezentat în figura 7.2:

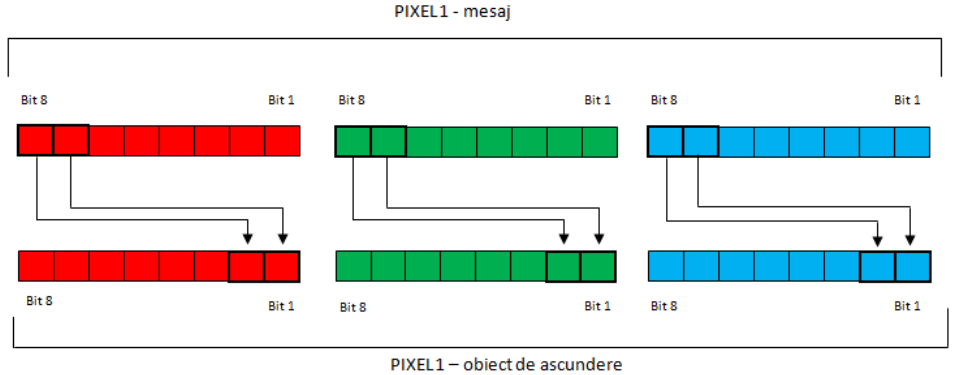


Figura 7.2. Algoritmul LSB pe 2 biţi

În cazul în care se lucrează cu imagini digitale color, unde fiecare pixel conţine 3 componente RGB, procesul de încorporare a mesajului în obiectul de acoperire se face pentru fiecare culoare în parte.

Dacă se consideră că obiectul de acoperire este o imagine reprezentată sub forma unei matrice de $m \times n$ (linii şi coloane) se constată că prin aplicarea acestui algoritm se poate ascunde o cantitate de informaţie de la $\frac{m \times n}{2}$ până la $\frac{m \times n}{4}$, care este practic de două ori mai mare decât în cazul LSB-ului pe 1 bit.

Avantajul acestei metode constă în faptul că obiectul de acoperire este afectat foarte puţin, astfel că eroarea relativă dintre obiectul de acoperire şi obiectul steganografic se reduce la 1,1% , menţinându-se eroarea relativă dintre mesajul original şi mesajul recuperat de la 0% la 6%, funcţie de varianta aleasă. Pentru a micşora eroarea relativă dintre mesajul iniţial şi mesajul recuperat se pot ascunde în obiectul de acoperire 6 biţi din mesaj sau chiar 8 biţi din mesaj.

Adaptarea acestui algoritm pentru microprocesoarele ARM şi ISAAC a condus în mod evident la îmbunătăţirea timpilor de obţinere a obiectului steganografic, cât şi la recuperarea mesajului ascuns. Din punct de vedere al erorilor relative nu s-a constatat o diferenţă semnificativă.

7.1.3 Algoritm de ascundere pe 4 biţi (LSB-P$_4$)

În figura 7.3 se prezintă modul de desfăşurare al procesului de înlocuire LSB pe 4 biţi.

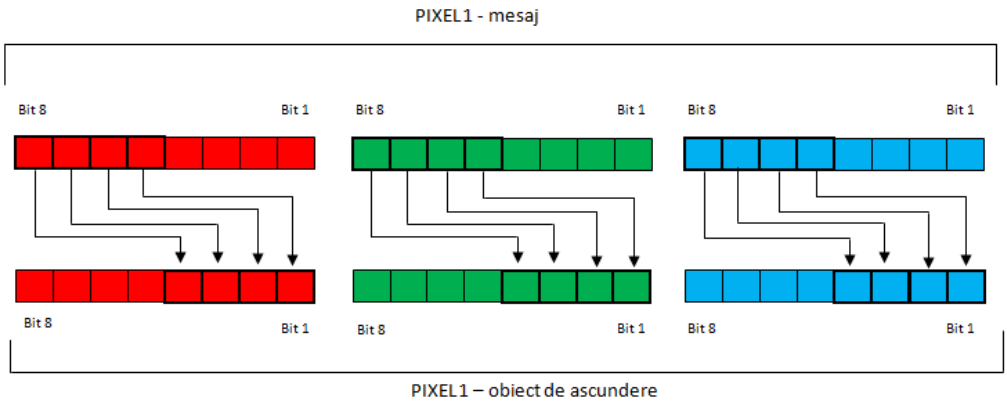


Figura 7.3. Algoritmul LSB pe 4 biţi

Algoritmul constă în înlocuirea celor 4 mai semnificativi biţi din mesaj cu cei 4 biţi mai puţini semnificativi din obiectul de acoperire. Şi aici se ţine cont de faptul că în cazul în care se lucrează cu imagini digitale color, procesul de încorporare a mesajului în obiectul de acoperire se face pentru fiecare culoare în parte. Această variantă a metodei LSB permite ascunderea unei capacităţi mari de

informaţie. Practic, un mesaj de capacitate $m \times n$ pixeli poate fi ascuns într-un obiect de acoperire de aceeaşi capacitate.

Dezavantajul acestei metode ar consta în faptul că atât obiectul de acoperire, cât şi mesajul secret vor fi degradate în raport cu valoarea biţilor cei mai puţini semnificativi. Mai mult, există posibilitatea să apară diferenţe vizibile între obiectul de acoperire iniţial şi obiectul steganografic rezultat, fapt ce ar putea permite unui atacator să fie atenţionat de prezenţa unui mesaj ascuns.

Se pot imagina variante ale acestui algoritm în funcţie de situaţia concretă ce trebuie rezolvată, fie crescând cantitatea de informaţie încorporată cu obţinerea unor erori mai mari de recuperare a mesajului, fie reducând cantitatea de informaţie ascunsă pentru a obţine o eroare cât mai mică la extragerea mesajului.

Un calcul simplu arată că eroarea relativă este de maxim 5,8% atât pentru diferenţa dintre obiectul de acoperire şi obiectul steganografic, cât şi pentru diferenţa dintre mesajul imagine iniţial şi cel recuperat.

În urma aplicării acestui algoritm, orice zgomot ce poate afecta transmiterea mesajului steganografic ar conduce la degradarea într-o măsură şi mai mare a mesajului recuperat, datorită faptului că atât din obiectul de acoperire, cât şi din mesaj sunt păstraţi doar 4 biţi mai semnificativi. Din acest motiv se poate considera că metoda LSB pe 4 biţi este cea mai puţin robustă. În procesul de extracţie cel mai puţin semnificativ bit este extras din subsetul în care a fost ascuns, urmând ca mesajul ascuns să fie reconstituit din biţii extraşi. În [SUK06] este propusă o metodă modificată pentru a combate problemele ce pot apărea în cazul în care datele încorporate nu pot fi extrase corect.

Dacă algoritmii de ascundere pe biţii cei mai puţini semnificativi ai obiectului de acoperire par la prima vedere relativ simplii, modalitatea lor de aplicare poate conduce la o diversitate foarte mare de cazuri de algoritmi particulari. În plus, modalitatea de utilizare a algoritmilor poate genera o diversificare mare de astfel de situaţii. Spre exemplu, încorporarea mesajului nu este obligatoriu să fie secvenţială. Ascunderea poate urmări diferite reguli pseudoaleatoare care să conducă la un proces de încorporare a mesajului secret.

În acest sens pot fi folosiţi algoritmii de inscripţionare a datelor pe CD. Aceşti algoritmi sunt astfel concepuţi încât doi biţi alăturaţi dintr-un cuvânt se găsesc în zone diferite, ceea ce face ca în momentul citirii CD-ului dacă se deteriorează suprafaţa acestuia există posibilitatea de a se pierde un şir de biţi succesivi. Cum aceştia nu fac parte din acelaşi cuvânt refacerea informaţiei se poate face fără pierderi semnificative. Sigur că ascunderea poate fi făcută în funcţie de puterea de creaţie a emiţătorului şi totodată de resursele pe care le are la dispoziţie acesta.

Pentru implementarea algoritmului pe microprocesoarele ARM şi ISAAC s-au folosit aceleaşi idei prezentate mai sus în scopul îmbunătăţirii timpului de execuţie al acestuia, iar rezultatele experimentale sunt evidenţiate în tabelele 5.1 şi 7.1.

7.1.4 Experimente

În scopul comparării performanţelor algoritmilor steganografici ce sunt executaţi pe platforma unui calculator personal, respectiv pe platformele microprocesoarelor ARM şi ISAAC au fost realizate o serie de experimente în care au fost utilizate imagini de acoperire de dimensiuni variabile, respectiv mesaje sub formă de imagini de capacităţi diferite.

Rezultatele experimentale au condus la observaţia că timpul de execuţie descreşte semnificativ, astfel că pentru microprocesorul ARM scade de 3 ori, iar pentru microprocesorul ISAAC de 20 de ori. Aceste performanţe au fost obţinute în condiţiile în care este cunoscut faptul că pentru un calculator problemele referitoare la memorie nu sunt stringent legate de executarea algoritmului.

În cazul microprocesoarelor ARM şi ISAAC care au memorie limitată, a fost necesară şi o gestionare suplimentară a resurselor de memorie internă care în mod evident implică consum de timp. În plus, procesul de paralelizare al algoritmului steganografic pentru microprocesor ISAAC implică şi el un timp de organizare internă. Cu toate acestea se poate constata că din punct de vedere al timpului de execuţie se obţin rezultate deosebit de bune pe cele două microprocesoare utilizate în telefonia mobilă. În tabelele 5.1 şi 7.1 sunt prezentate doar o parte din rezultatele experimentale prin care doresc să evidenţiez aspectele menţionate mai sus.

Tabel 7.1 Compararea timpului de execuţie pentru algoritmul *LSB-R*

Nr. Crt.	Obiect de acoperire		Mesaj secret		PC	ARM	ISAAC
	Nume	Dimensiune (bytes)	Nume	Dimensiune (bytes)	[ms]	[ms]	[ms]
1	camp_cu_flori.jpg	81.000	porumbel.jpg	33.930	64	25	5,38
2	camp_cu_flori.jpg	81.000	ceas_2.jpg	45.450	78	25	5,38
3	camp_cu_flori.jpg	81.000	ceas_3.jpg	81.000	68	25	5,38
4	lac_3.jpg	202.500	porumbel.jpg	33.930	161	63	12,8
5	lac_3.jpg	202.500	ceas_3.jpg	81.000	160	63	12,8
6	lac_3.jpg	202.500	ceas_4.jpg	182.700	180	63	12,8
7	lac_2.jpg	360.000	porumbel.jpg	33.930	286	112	22,5
8	lac_2.jpg	360.000	ceas_3.jpg	81.000	281	112	22,5
9	lac_2.jpg	360.000	ceas_4.jpg	182.700	291	112	22,5
10	lac_2.jpg	360.000	peisaj_1.jpg	360.000	278	112	22,5
11	lac_1.jpg	810.000	porumbel.jpg	33.930	611	253	33,6
12	lac_1.jpg	810.000	ceas_3.jpg	81.000	627	253	33,6
13	lac_1.jpg	810.000	ceas_4.jpg	182.700	600	253	33,6
14	lac_1.jpg	810.000	peisaj_1.jpg	360.000	605	253	33,6
15	lac_1.jpg	810.000	peisaj_2.jpg	562.500	610	253	33,6
16	lac_1.jpg	810.000	peisaj_1.jpg	810.000	609	253	33,6

O parte din rezultatele experimentelor au fost publicate în lucrarea [STA09] şi ca urmare a continuării cercetării în acest domeniu conform celor menţionate mai sus algoritmii de ascundere pe biţii cei mai puţini semnificativi au fost implementaţi şi pe microprocesorul ISAAC, ce momentan este în faza de a fi utilizat în noua generaţie de telefonie mobilă şi care printre alte aplicaţii va include şi unul dintre algoritmii steganografici experimentaţi în această lucrare. Varianta de algoritm ce urmează a fi implemetată va fi dependentă de solicitările clienţilor. În acest sens le putem pune la dispoziţie algoritmi steganografici cu timp de execuţie cât mai scurt sau varianta necesară pentru ascunderea unor cantităţi mari de informaţii (cum ar fi cei prezentaţi mai sus). Astfel de algoritmi pot permite practic şi lucrul în timp real.

Pentru a scoate în evidenţă caracteristicile de timp a celor trei platforme privind timpul de execuţie al algoritmului bazat pe ascunderea în biţii cei mai puţini

semnificativi, în figura 7.4 se reprezintă comparativ timpul necesar de execuţie exprimat în funcţie de capacitatea obiectului de acoperire. Menţionez că timpul este exprimat în milisecunde, iar capacitatea obiectului de acoperire în octeţi.

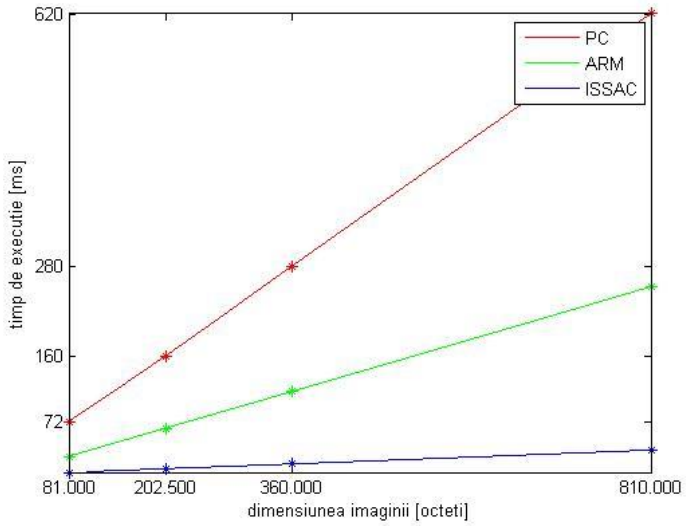


Figura 7.4 Reprezentarea grafică a timpului de execuţie pentru algoritmul *LSB-R*

În figura 7.5 este prezentat un exemplu de realizare a unui algoritm steganografic ce permite ascunderea unui mesaj secret în 1, 2, respectiv 4 biţi cei mai puţini semnificativi ai obiectului de acoperire ales.

Mesajul recuperat pe 2 biţi

Mesaj recuperat pe 4 biţi

Figura 7.5. Rezultate experimentale LSB pe 1, 2, respectiv 4 biţi pe microprocesorul ARM şi ISAAC.

În urma testelor se poate observa că indiferent de natura lor imaginile ascunse sunt extrase la o calitate mai superioară în cazul în care se ascund în obiecte de acoperire formate din imagini cu foarte multe nuanţe de culori şi la o calitate mai redusă (apar pixeli de zgomot) în cazul imaginilor ce prezintă puţine nuanţe de culori. Din punct de vedere al cantităţii de informaţie ascunsă se poate constata că aceasta depăşeşte în cazul meu rezultatele experimentale din lucrarea [CHE08a] în care este permisă ascunderea unei cantităţi de informaţii reprezentând 50% din obiectul de acoperire.

7.1.5 Concluzii privind algoritmii steganografici bazaţi pe ascunderea în biţii cei mai puţini semnificativi

În concluzie, algoritmii care folosesc tehnici de ascundere în biţii cei mai puţin semnificativi ai obiectului de ascundere prezintă avantajul că sunt relativ uşor de implementat şi permit ascunderea unor cantităţi mari de informaţii, iar din acest motiv i-am adaptat pentru generarea unor algoritmi steganografici performanţi în special din punct de vedere al timpului de rulare pe cele două microprocesoare amintite în acest paragraf. Menţionez că unul dintre microprocesoare este frecvent utilizat la ora actuală în telefonia mobilă, iar cel de-al doilea este în faza de testare finală constituind următoarea generaţie de microprocesoare ce vor fi folosite în telefonia mobilă modernă. Rezultatele testelor efectuate scot în evidenţă faptul că în condiţiile de funcţionare la frecvenţe de lucru asemănătoare ambele microprocesoare conduc la obţinerea unor timpi de execuţie net inferiori faţă de cazul utilizării unui calculator personal ce prezintă aceleaşi performanţe. Acest lucru a fost posibil datorită exploatării la maxim a arhitecturii interne a acestora şi confirmă faptul că modificările aduse algoritmilor au creat condiţii pentru executarea algoritmilor în timp real. Aceasta face posibilă includerea unor astfel de facilităţi în viitoarele echipamente de telefonie mobilă aşa cum se doreşte la ora actuală, ca urmare a unor cerinţe exprimate de beneficiarii echipamentelor mobile în ideea existenţei comunicărilor confidenţiale.

7.2 *Algoritmul steganografic YUV-P*

Având în vedere rapida dezvoltare a echipamentelor digitale, imaginile color au devenit un mediu comun în multe aplicaţii, inclusiv în domeniul steganografiei. Se cunoaşte că o imagine color poate fi reprezentată în diferite sisteme de coordonate, spre exemplu RGB, HSV, YUV. Cum în sistemele de transmisie TV frecvent este folosit domeniul spaţial YUV s-au căutat generarea unor algoritmi steganografici care să permită transmiterea de informaţii secrete prin intermediul canalelor TV.

În [CHO08] se propune modificarea culorii albastru cu scopul de a ascunde date secrete deoarece valoarea albastru este o culoare insensibilă ochiului uman. Pentru a mări şi mai mult complexitatea metodei de ascundere, autorii sugerează în lucrare o soluţie de ascundere a pixelilor în mod dinamic pentru a încorpora o cantitate cât mai mare de date secrete. Se menţionează că metoda propusă poate fi aplicată atât sistemelor color RGB, cât şi sistemelor YUV. În urma testelor efectuate s-a constatat că sistemele RGB permit o capacitate de încorporare a datelor cu o

distorsiune a imaginii mai mică, metoda steganografică fiind mai puţin vulnerabilă la algoritmi steganalitice.

În [CHA06b] se realizează transformarea unei imagini RGB într-o imagine YUV, iar încorporarea mesajului secret se realizează cu metoda bitului cel mai puţin semnificativ în componentele Y ai pixelilor imaginii secrete. Pentru a mări calitatea imaginii se adoptă un mecanism de prag care ia în considerare efectul vizual al omului. Se menţionează că diferenţa dintre imaginea steganografică şi obiectul de acoperire este aproape imperceptibilă. Metoda propusă poate insera mesaje secrete având capacitatea relativ mare cu condiţia ca mesajul secret să aibă formatul cerut în experimentele menţionate.

În general algoritmii steganografici folosiţi în domeniul spaţial YUV prezintă un mare dezavantaj în ceea ce priveşte cantitatea de informaţie ascunsă, în sensul că ascunderea mesajului se poate face doar într-una din cele trei componente fără a se pierde din informaţiile iniţiale ale obiectului de acoperire, ceea ce conduce la rate extrem de mici ale raportului dintre mesajul secret şi obiectul de acoperire. Se apreciază un rezultat mulţumitor la acest raport de circa 5%.

Algoritmul ar prezenta avantaje dacă metodele de ascundere ar putea fi combinate cu procedee de dispersare a informaţiei secrete şi/sau de comprimare a mesajului ascuns şi poate nu în ultimul caz, de o procesare iniţială, fie a obiectului de ascundere, fie a mesajului secret, fie a amândurora.

Bazat pe transformata YUV am implementat un algoritm care a fost executat pe un calculator personal, microprocesorul ARM şi microprocesorul ISAAC. Pentru cele două microprocesoare, datorită arhitecturii lor, a rezultat practic o nouă variantă de algoritm bazat pe transformarea YUV pe care l-am notat YUV-P. Algoritmul a fost dezvoltat pe baza celor prezentate în lucrarea [STA07c].

7.2.1 Transformare RGB-YUV-RGB

Algoritmul steganografic YUV se bazează pe ascunderea informaţiilor secrete în obiecte de acoperire tip imagini digitale reprezentate în domeniul spaţial YUV. În primă fază imaginea aleasă pentru ascunderea informaţiei secrete este reprezentată în domeniul spaţial RGB, dar trecerea acesteia în spaţiul YUV este relativ simplă. Practic trecerea de la un spaţiu la altul se face prin câteva înmulţiri de matrice, în modul următor [BUR08]:

$$\begin{bmatrix} Y \\ U \\ V \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ -0.14713 & -0.28886 & 0.436 \\ 0.615 & -0.51498 & 0.10001 \end{bmatrix} \times \begin{bmatrix} R \\ G \\ B \end{bmatrix} \tag{7.2}$$

Transformarea inversă se face după formula:

$$\begin{bmatrix} R \\ G \\ B \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1.13983 \\ 1 & -0.39465 & -0.58060 \\ 1 & 2.03211 & 0 \end{bmatrix} \times \begin{bmatrix} Y \\ U \\ V \end{bmatrix} \tag{7.3}$$

7.2.2 Etapele algoritmului steganografic YUV-P

Pentru ascunderea în domeniul YUV se folosesc practic aceiaşi algoritmi, de ascundere şi extragere ca cei prezentaţi la algoritmul steganografic LSB, cu menţiunea că procesarea datelor nu se face pe tabloul matricei de pixeli RGB, ci pe tabloul YUV ce se bazează pe proprietăţile vizuale ale ochiului uman [CHO06]. În general ascunderea se face în domeniul Y, deoarece ochiul uman nu este sensibil la variaţii mici de luminozitate. În principiu algoritmul de ascundere se bazează pe următoarele etape:

Algoritmul de ascundere

1) Se citeşte formatul imagine (TGA, JPEG, BMP, etc.) al obiectului de acoperire ales şi al mesajului secret după care se transformă în matrice de pixeli fiecare dintre ele. Mesajul secret este în principiu mai mic decât obiectul în care urmează a fi ascuns deoarece biţii ce formează mesajul secret trebuie distribuiţi în ultimii biţi ai pozei sau imaginii în care se va ascunde.
2) În cazul în care se ascunde o imagine color în altă imagine color reprezentate fiind în spaţiul RGB, se extrage din matricea de pixeli corespunzătoare obiectului de acoperire fiecare pixel şi i se aplică transformarea din spaţiul RGB în spaţiul YUV după formula (7.2).
3) Urmează transformarea Y-ul în întreg şi bitul cel mai puţin semnificativ se înlocuieşte cu un bit din mesaj rezultând astfel imaginea steganografică, ce este foarte asemanatoare cu obiectul de acoperire (imaginea iniţială).
4) Pentru a memora imaginea purtătoare în care s-a încorporat mesajul se face transformarea inversă, din spaţiul YUV în RGB prin aplicarea formulei (7.3).
5) Se reţin într-un fişier rezultatele procesului steganografic.

Pentru extragerea mesajului se pleacă de la obiectul steganografic asupra căruia se aplică algoritmul invers de ascundere pentru obţinerea mesajului secret. Paşii algoritmului sunt prezentaţi mai jos.

Algoritmul de extragere

1) Se citeşte imaginea originală care în acest caz este formată din obiectul steganografic.
2) Se transformă în matrice de pixeli.
3) Se face conversia din spaţiul RGB în spaţiul YUV aplicând formula (7.2).
4) Se extrag cei mai puţin semnificativi biţi şi sunt aliniaţi pentru reconstrucţia mesajului secret.
5) Se reţin într-un fişier datele obţinute în urma procesului steganografic.

În [STA07c] am aplicat acest algoritm şi am ascuns informaţia în canalul V deoarece am constatat că e mai bine să se ascundă în crominanţă. Rezultatele experimentului sunt prezentate în figura 7.6. Coeficientul folosit în transformarea YUV poate fi schimbat, ca de altfel şi matricea de transformare din RGB în YUV, precum şi matricea inversă (din YUV in RGB). După o astfel de transformare nu se mai obţine acelaşi spaţiu YUV, însă ceva asemănător notat cu Y'U'V'. În noua matrice pe baza unui algoritm asemenea celui prezentat mai sus, se va ascunde informaţia secretă. Alegerea coeficientului folosit în transformarea YUV este foarte importantă, deoarece este posibil ca atunci când se încorporează informaţie pe un

canal, să se distrugă imaginea în cazul în care se schimbă canalul. Odată ce un canal este compromis, devine vizibil faptul că ceva este ascuns acolo şi este posibil ca extragerea imaginii ascunse să fie compromisă. Acești coeficienți pot fi cheia secretă a datelor încorporate, şi odată cu schimbarea acestora scade şi rata de detecţie. Cheia secretă poate fi încorporată sau poate fi cunoscută.

În cazul algoritmului utilizat pot fi folosite toate cele trei canale de culoare pentru încorporarea mesajului secret sau se poate folosi unul singur. Totul depinde de raportul de ascundere şi de calitatea imaginii purtătoare. Se poate ascunde pixel cu pixel în toate cele trei canale simultan sau se poate ascunde într-un canal şi apoi în altul.

În [STA07c] am ascuns într-un singur canal pentru că am dorit să obţinem o calitate maximă. O calitate maximă a obiectului de acoperire implică o imagine greu de detectat. Am ascuns în primă fază în canalul V deoarece este cel mai potrivit să ascunzi în crominanţă, fiind mai flexibil pentru imaginile alese. Testând o serie de imagini, am observat că ascunderea informaţiei în canalele U sau V diferă de la imagine la imagine. Distrugând un anumit canal se poate distruge o culoare şi mesajul poate fi astfel detectat. Spre exemplu în figura 7.7 ascunderea informaţiei în componenta U conduce la deplasarea culorii de la albastru spre violet, ceea ce este nefiresc pentru o imagine în care se regăseşte un ochi de apă. Ascunderea informaţiei în canalul Y se obţine cu succes de fiecare dată, aşa cum se poate vedea în figura 7.8. În plus mesajul recuperat se obţine cu o eroare relativă foarte bună ($\varepsilon_{rel} = 0{,}76\%$). Această diferenţă foarte mică face dificilă detectarea de către ochiul uman a prezenţei unui mesaj secret în obiectul steganografic. Trebuie remarcat că algoritmul steganografic aplicat în spaţiul YUV nu este la fel de comun ca şi algoritmul bazat pe ascunderea în cei mai puţini semnificativi biţi aplicat în spațiul RGB, deci este mai greu de detectat.

7.2.3 Experimente YUV-P

În continuare voi prezenta câteva din experimentele efectuate în aplicarea algoritmului steganografic utilizat în spaţiul YUV, unde ascunderea mesajului s-a făcut pe unul din cele 3 canale: V – figura 7.6, U - figura 7.7, Y - figura 7.8.

Obiect de acoperire
Dimensiune 192x192 x 24biti

Obiect steganografic
Dimensiune 192x192 x 24biti

Mesaj secret
Dimensiune 32x48 x 24biti
Rata de ascundere:4,1%

Mesaj recuperat
Dimensiune 32x48x 24biti

Figura 7.6. Ascunderea in componenta V

Obiect de acoperire
Dimensiune 192x192 x 24biti

Obiect steganografic
Dimensiune 192x192 x 24biti

Mesaj secret
Dimensiune 32x48 x 24biti
Rata de ascundere 4,1%

Mesaj recuperat
Dimensiune 32x48x 24biti

Figura 7.7 Ascunderea in componenta U

Obiect de acoperire
Dimensiune 192x192 x 24biti

Obiect steganografic
Dimensiune 192x192 x 24biti

Mesaj secret
Dimensiune 32x48 x 24biti
Rata de ascundere:4,1%

Mesaj recuperat
Dimensiune 32x48x 24biti

Figura 7.8 Ascunderea in componenta Y

Pe baza testelor a rezultat faptul că ascunderea în componenta Y este uşor de realizat, diferenţa dintre imaginea obiectului de acoperire şi obiectul steganografic rezultat este imperceptibilă, dar este totodată posibil ca prin metode steganalitice să existe posibilitatea detecţiei şi eventual a distrugerii mesajului ascuns în eventualitatea cunoaşterii coeficienţilor de transformare. Ascunderea în componenta V prezintă rezultatele cele mai bune, obiectul steganografic este aproape imposibil de deosebit de obiectul de acoperire, iar metodele steganalitice sunt greu de aplicat. Ca dovadă a acestor afirmaţii în literatura de specialitate nu am identificat lucrări care să trateze astfel de probleme.

Algoritmul de ascundere ce utilizează reprezentarea imaginilor în domeniul YUV prezintă un grad mare de robusteţe şi este relativ uşor de implementat. De asemenea, încorporarea informaţiei în canalele Y, U sau V poate scădea riscul ca informaţia să fie detectată. Fiind o tehnică relativ simplă, ascunderea în domeniul YUV prezintă avantajul că algoritmii steganografici se pretează pentru a construi un

codor şi un decodor steganografic implementat cu ajutorul unui microprocesor. Rezultatele experimentale, pe o astfel de platformă, conduc la concluzia că această metodă oferă rezultate promiţătoare în protejarea informaţiilor prin ascundere.

În figura 7.9, se pot observa rezultatele experimentale obţinute pentru algoritmul ce utilizează reprezentarea în YUV ce este implementat pe microprocesoarele ARM şi ISAAC.

Obiect de acoperire
Dimensiune 600x450 x 24biti

Obiect steganografic
Dimensiune 600x450 x 32biti

Mesaj secret
Dimensiune 200x135 x 24biti
Rate de ascundere: 10%

Mesaj recuperat
Dimensiune 200x135x 24biti

Figura 7.9 Ascunderea YUV pe microprocesorul ARM7TDMI-S.

Adaptând algoritmul steganografic reprezentat în domeniul spaţial YUV la microprocesoarele ARM şi ISAAC am reuşit să îmbin proprietăţile acestui algoritm cu principalele caracteristici ale arhitecturii acestora pentru obţinerea unor performanţe maxime din această implementare. Aplicând această metodă de ascundere la microprocesoarele ARM şi ISAAC am constatat o îmbunătăţire substanţială în primul rând a ratei de ascundere, care a crescut de la 4,1% la 10%. Această îmbunătăţire s-a obţinut prin utilizarea mai bună a resurselor de care dispune algoritmul la nivel de bit, cât şi de exploatare corespunzătoarea a performanţelor microprocesoarelor ARM şi ISAAC [SLO04, HYU06].

În tabelul 7.2 prezint câteva rezultate comparative ale executării algoritmului YUV-P pe un calculator personal şi pe cele două microprocesoare ARM şi ISAAC. Menţionez că toate platformele sunt echivalente din punctul de vedere al performanţelor de timp specifice fiecăruia.

Plecând de la tabelul 7.2 se prezintă în figura 7.10 exprimarea grafică a raportului dintre timpul de execuţie pentru algoritmul YUV-P dezvoltat, verificat şi testat pe cele trei platforme : calculator personal şi microprocesoarele ARM, respectiv ISAAC. Menţionez faptul că timpii sunt exprimaţi în milisecunde, iar capacitatea obiectului de acoperire în octeţi.

Tabel 7.2 Compararea timpului de execuţie pentru algoritmul YUV-P

Nr. Crt.	Obiect de acoperire		Mesaj secret		PC	ARM	ISAAC
	Nume	Dimensiune (bytes)	Nume	Dimensiune (bytes)	[ms]	[ms]	[ms]
1	lac_1.jpg	810.000	porumbel.jpg	33.930	521	3162	420,47
2	lac_1.jpg	810.000	ceas_3.jpg	81.000	952	7550	1.006,6
3	peisaj_2.jpg	562.500	watch70x70.jpg	14.700	232	1369	182,04
4	peisaj_1.jpg	360.000	watch70x70.jpg	14.700	249	1371	182,32

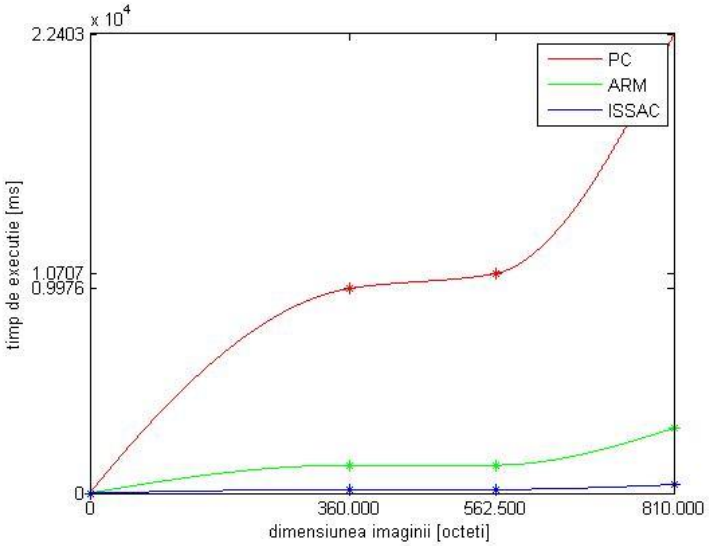


Figura 7.10 Reprezentarea grafică a timpul de execuţie pentru algoritmul YUV-P

Se poate constata că implementarea pe microprocesorul ARM conduce la îmbunătăţirea performanţelor legate de timpul de execuţie de aproximativ 7 ori, iar rularea pe microprocesorul ISAAC permite scăderea timpilor de execuţie cu o rată de până la 50 de ori. Aceste performanţe se obţin datorită folosirii cu succes a celor două arhitecturi, dintre care una exploatează proprietăţile bazate pe banda de asamblare şi cealaltă pe executarea în paralel a procesării imaginilor. Trebuie să precizăm faptul că dacă timpii executaţi pe cele două microprocesoare prezintă

valori constante la rulări diferite în timp, timpul de execuţie pe calculator prezintă diferenţe de la o rulare la alta în funcţie de modul de încărcare şi de execuţie al algoritmului, asupra căruia sistemul de operare al calculatorului joacă un rol hotărâtor. Chiar şi cu această rezervă pot spune că timpul de execuţie al algoritmului pe cele două microprocesoare este net mai mic decât în cazul rulării pe calculator.

Se poate remarca faptul că în literatura de specialitate o astfel de implementare pe microprocesor nu a fost încă realizată, din cele cunoscute de mine. Motivul lipsei unei astfel de abordări poate fi pusă pe seama dificultăţii implementării unor astfel de algoritmi steganografici pe un microprocesor existent, ce nu este adaptat unor astfel de prelucrări de semnale sau imagini. În eventualitatea utilizării unor procesoare grafice se ridică o altă problemă legată de implementarea algoritmilor steganografici. În primul rând trebuie să se ţină cont de numărul limitat de instrucţiuni de altă natură decât cele grafice pe care le au astfel de echipamente.

Algoritmii steganografici în domeniul YUV îşi pot găsi aplicaţii în domeniul transmiterilor TV prin plasarea unor informaţii utile doar acelor persoane sau abonaţi care deţin codoare, respectiv decodoare steganografice. Datorită faptului că Y are ponderea cea mai mare în formula de transformare a spaţiului RGB -YUV, modificările care se fac la nivelul lui se vor propaga liniar în toate canalele RGB. Din acest motiv rezultă o uşoară detectabilitate în cazul unui atac. Ascunderea informaţiilor secrete în componentele U sau V duc la o detectabilitate mai scăzută, dar rezultatele ascunderii diferă de la imagine la imagine (la unele este mai indicat ca ascunderea să se facă în U, iar la altele în V)

7.2.4 Concluzii YUV-P

În concluzie, utilizarea algoritmului YUV-P prezintă avantajul robusteţii în cazul unui atac prin prisma faptului că într-o primă etapă atât imaginea purtătoare, cât şi mesajul secret sunt imagini RGB. În etapa a doua, imaginea considerată obiect de acoperire este convertită din RGB în YUV, după care biţii mesajului secret sunt încorporaţi unul câte unul cu ajutorul algoritmului bazat pe ascunderea în biţii cei mai puţini semnificativi în fiecare canal al fiecărui pixel din imaginea purtătoare, rezultând astfel o imagine steganografică YUV care va fi convertită, la rândul ei în RGB şi abia apoi transmisă printr-un canal de comunicaţie unui anumit receptor. În cazul în care obiectul steganografic astfel rezultat ar fi interceptat, atacatorul va încerca să decodifice algoritmul de ascundere folosind o procedură caracteristică unui algoritm bazat pe ascunderea în biţii cei mai semnificativi aplicat unei imagini RGB. El nu are acces la obiectul de acoperire iniţial şi astfel nu ştie că mesajul secret a fost de fapt ascuns în imaginea convertită în YUV. Pentru a extrage mesajul are nevoie de această conversie inversă, de care nu are cunoştinţă. Din acest motiv creşte gradul de rezistenţă în cazul unui atac inoportun.

Trebuie remarcat faptul că în cazul algoritmului YUV-P adaptat pentru a fi executat pe cele două microprocesoare se constată că datorită multiplelor prelucrări, atât asupra obiectului de acoperire, cât şi asupra mesajului secret timpul de execuţie creşte în comparaţie cu algoritmii bazaţi pe biţii cei mai puţini semnificativi. Mai mult, timpul de execuţie depinde atât de mărimea obiectului de acoperire, cât şi de cantitatea de informaţii ascunse, ceea ce face ca acest algoritm prezintă şi dezavantajul timpului de execuţie. Din acest motiv acest algoritm se recomandă a fi

utilizat pentru ascunderea unor cantităţi mai mici de informaţii, cât şi în cazul ascunderii unei informaţii ce nu necesită transmiterea ei în timp real. În acest sens, ca viitor obiectiv voi încerca aducerea unor noi îmbunătăţiri în vederea scăderii timpului de execuţie.

7.3 *Algoritmi steganografici bazaţi pe complexitatea planurilor de biţi*

Algoritmii steganografici bazaţi pe complexitatea planurilor de biţi, denumiţi pe scurt BPCS (Bit-Plane Complexity Segmentation Steganography) se află printre cei mai utilizaţi algoritmi de ascundere deoarece au proprietatea de a include o cantitate relativ mare de informaţii de aproximativ 30% din capacitatea obiectului de ascundere, iar imaginea steganografică rezultată prezintă o vizibilitate redusă. În plus aceşti algoritmi sunt relativ robuşti la încercările de atac datorită faptului că utilizează o mască de conjugare aleasă de către autorul algoritmului şi care poate juca rolul unei chei de acces.

În [NOD02a, NOD02b, NOD04, FUR03] sunt prezentate metode steganografice ce folosesc combinarea unui algoritm de tip BPCS cu o soluţie de comprimare a imaginilor video. Ideile propuse permit un grad relativ mare de ascundere fără degradarea vizibilă a calităţii imaginilor video implicate în procesul steganografic. Este de remarcat faptul că autorii acestor articole şi-au direcţionat eforturile pentru creşterea cantităţii de informaţie ce poate fi ascunsă ajungând să crească această cantitate de la 15% la 28% din capacitatea obiectului de ascundere.

Niimi şi colaboratorii săi dezvoltă în [NII02a, NII02b] metode de ascundere a informaţiilor secrete bazate pe complexitatea planurilor de biţi (BPCS) în domeniul spaţial reprezentat în RGB prin memorarea vectorilor de informaţie.

[TOR06] introduce în algoritmii de tip BPCS coduri de control a erorii (ECC) ce au ca scop reducerea ratei de eroare BER (bit error rate) la extragerea datelor din imaginea steganografică chiar şi în cazul apariţiei unor distorsiuni pe canalele de transmitere. Folosirea codurilor de control al erorilor a condus la o creştere a capacităţii de ascundere cu mai mult de doi biţi pe pixel faţă de lucrările de referinţă luate de către autori.

Se dovedeşte că algoritmii ce folosesc tehnica BPCS sunt şi rezistenţi la atacuri concepute prin steganaliză. În lucrarea [ZHA06] autorii propun algoritmul BPCS pentru ascunderea mesajului secret deoarece aceştia se dovedesc a fi deosebit de rezistenţi la analiza statistică folosită în procesul de steganaliză. Mai mult, acest algoritm permite şi obţinerea unor contramăsuri în cazul unor atacuri [NII04].

Algoritmul de ascundere BPCS este util şi în alte domenii. Spre exemplu în medicină este propus în [SRI04] spre a fi folosit pentru protecţia înregistrărilor medicale în vederea asigurării confidenţialităţii datelor pacienţilor.

7.3.1 Conceptele de bază ale algoritmilor steganografici bazaţi pe complexitatea planurilor de biţi

Algoritmul steganografic BPCS ascunde o informaţie secretă într-un obiect de acoperire tip imagine digitală, iar pentru aceasta se foloseşte tehnica domeniului spaţial care înglobează informaţia direct în biţii imaginii digitale. BPCS este o tehnică care profită de proprietatea sistemului vizual uman [KAW98], [KAW02].

Tehnica presupune divizarea imaginii de preferat în blocuri de dimensiune 8x8, însă pot fi concepute şi alte dimensiuni. Fiecare imagine este descompusă în regiuni de 8x8, care la rândul lor sunt descompuse în 8 planuri de biţi. Pentru implementarea algoritmului este necesară calcularea complexităţii binare pentru fiecare plan de biţi.

În general nu există o definiţie standard a complexităţii planurilor de biţi. Spre exemplu Kawaguchi a propus trei tipuri de măsuri ale complexităţii în [KAW86], [KAW89], [KAM95]. Pentru determinarea complexităţii şi înglobarea datelor în aceste regiuni individuale se foloseşte pentru calculul acesteia o măsură a complexităţii binare a planurilor de biţi individuale din fiecare regiune.

În mod frecvent complexitatea imaginii se defineşte prin lungimea graniţei dintre alb şi negru. Lungimea totală a graniţei între alb şi negru este egală cu însumarea numărului de schimbări negru/alb în lungul liniilor şi al coloanelor dintr-o imagine.

Complexitatea imaginii este definită în [KAW86] prin relaţia :

$$\alpha = \frac{k}{M} \qquad (7.4.)$$

În relaţia (7.4), k este lungimea totală a graniţei dintre negru şi alb sau numărul total de treceri de la 0 la 1 a imaginii şi M este numărul maximum posibil de schimbări între alb şi negru. Desigur, valoarea complexităţii variază între limitele [0,1]. Pentru ca un bloc să fie considerat complex şi a putea fi înlocuit cu mesajul de ascuns, trebuie ca acesta să aibă de obicei complexitatea mai mare decât o complexitate de prag, notată α_t = 0.3.

Codificarea binară a planurilor de biţi poate crea generarea pe anumite regiuni a unor complexităţi foarte mari cu toate că din punct de vedere valoric planurile de biţi nu se deosebesc semnificativ. Una din soluţiile propuse în [KAW86] constă în transformarea codului binar în cod Gray.

În procesul de ascundere la început se realizează o descompunere a imaginii în planuri de biţi după care se calculează complexitatea fiecărei regiuni locale din fiecare plan de biţi. Dacă o regiune are complexitatea mai mică decât complexitatea de prag, atunci regiunea este lăsată aşa cum e, însă dacă complexitatea este mai mare sau egală cu pragul, atunci regiunea este înlocuită cu informaţia care se doreşte a fi ascunsă.

La extragerea informaţiei înglobate din imagine steganografică, procesul este inversat. Se realizează o descompunere a imaginii în planuri de biţi şi se calculează complexitatea fiecărei regiuni din fiecare plan de biţi. Regiunile cu o complexitate mai mică decât complexitatea de prag sunt presupuse ca fiind informaţie din imaginea originală şi sunt sărite. Regiunile cu complexitatea mai mare sau egală cu complexitatea de prag vor conţine informaţia ascunsă.

Problema acestei metode după cum a fost prezentată este aceea că este posibil ca informaţia ascunsă, deşi în general aleatoare prin natură, ar putea avea o complexitate mai mică decât complexitatea de prag. O astfel de regiune ar fi sărită în mod greşit în procesul de extragere deoarece având o complexitate scăzută este plasată în categoria informaţiei simplu structurate din imagine.

Pentru a rezolva această problemă se utilizează o operaţie de conjugare, ce poate fi privită ca o operaţie sau-exclusiv a pixelilor din regiune cu un tipar în formă de tablă de şah. În acest fel are loc convertirea unei imagini cu complexitate mai mică decât pragul ales într-una cu o complexitate mai mare. Este posibil ca în funcţie de caracteristicile sistemului vizual uman ca pragul ales să difere de la un plan de biţi la altul. Se cunoaşte că ochiul uman este mai sensibil la regiuni cu

degradări mai mari. Avându-se în vedere acest aspect se pot selecta praguri care să satisfacă această caracteristică, lucru ce a fost încercat în [ZHA06].

7.3.2 Etapele algoritmul steganografic bazat pe complexitatea planurilor de biţi

Pe baza principiilor de bază enumerate mai sus am dezvoltat un algoritm bazat pe complexitatea planurilor în scopul efectuării unei analize privind caracteristicile acestui gen de algoritm, cât şi performanţele lui. Algoritmul constă în următoarele etape:

Algoritmul de ascundere

1. Se realizează conversia obiectului de acoperire în codul Gray canonic.
2. Se descompune imaginea în planuri de biţi. Imaginea alb negru prezintă 1×8 planuri de biţi, iar imaginea color 3×8 planuri de biţi.
3. Se partiţionează fiecare plan de biţi în regiuni de 8x8 blocuri.
4. Se generează masca de conjugare.
5. Se parcurge, într-o ordine prestabilită, fiecare bloc în parte şi se calculează complexitatea planului de biţi.
6. Primul plan de biţi care are complexitatea mai mare decât complexitatea de prag este rezervat pentru a fi completat atât cu lungimea (exprimată în octeţi) a mesajului ascuns, cât şi cu numele fişierului ce are complexitate. Acesta se va complecta la sfârşitul operaţiei de ascundere şi constituie antetul obiectului steganografic.
7. Se parcurge următorul bloc care a mai rămas în secvenţa regiunilor imaginii. Pentru fiecare regiune se calculează complexitatea acesteia.

a) Dacă complexitatea este mai mică decât complexitatea de prag, atunci se ignoră regiunea curentă şi se trece la regiunea următoare. În acest caz blocul rămâne nemodificat.

b) Dacă complexitatea blocului este mai mare sau egală cu complexitatea de prag atunci regiunea este considerată complexă şi planul de biţi a obiectului de acoperire este înlocuit cu planul de biţi al mesajului, după care se conjugă.

8. Blocul conjugat este marcat printr-un bit indicator.
9. Se continuă pasul 7, 8 până la terminarea blocurilor.
10. Se completează primul bloc complex, pasul 6, cu datele menţionate.
11. Se realizează conversia planurilor de biţi în codul Gray canonic înapoi în formatul imagine binară RGB care constituie imaginea steganografică.

Algoritmul de extragere.

1. Imaginea steganografică se converteşte în imagini în codul Gray canonic urmată de descompunerea acesteia în planuri de biţi.
2. Se partiţionează fiecare plan de biţi în regiuni de 8x8 blocuri şi se recreează secvenţa imaginii acestor regiuni folosite în procesul de ascundere.
3. Se parcurg regiunile imaginii în aceeaşi secvenţă până când se găseşte prima care are complexitatea mai mare sau egală cu cea de prag. Aceasta este regiunea antet.
4. Se conjugă regiunea antet dacă bitul său indicator este unu. De aici se extrage lungimea fişierului mesajului.
5. Se parcurge secvenţa regiunilor imaginii începând cu regiunea următoare după antet. Pentru fiecare regiune se calculează complexitatea. Dacă aceasta este mai mică decât complexitatea de prag, atunci regiunea curentă se ignoră şi se trece la următoarea regiune.
6. Dacă complexitatea este mai mare sau egală cu complexitatea de prag atunci regiunea conţine informaţie secretă şi aceasta va fi extrasă.

7. Dacă bitul indicator este ”1” atunci informaţia extrasă se conjugă şi apoi urmează plasarea ei în fluxul de informaţie secretă.
8. Operaţia continuă până s-a extras cantitatea de informaţie specificată de dimensiunea fişierului găsită în pasul 4.

7.3.3 Rezultate experimentale - BPCS

În figurile 7.11, 7.12, 7.13 sunt prezentate câteva rezultate experimentale obţinute în urma aplicării algoritmului bazat pe complexitatea planurilor de biţi, iar în tabelul 7.3 sunt prezentate comparaţii între eroarea relativă rezultată şi cantitatea de informaţie ascunsă cu acest algoritm.

Obiect de acoperire - Dimensiuni: 900,1kbiţi

Obiect steganografic 900,1kbiţi

Mesaj secret Dimensiuni: 317k biţi

Mesaj recuperat 317kbiţi

Figura 7.11 Algoritmul BPCS - Experimentul a

$\propto = 0{,}3$

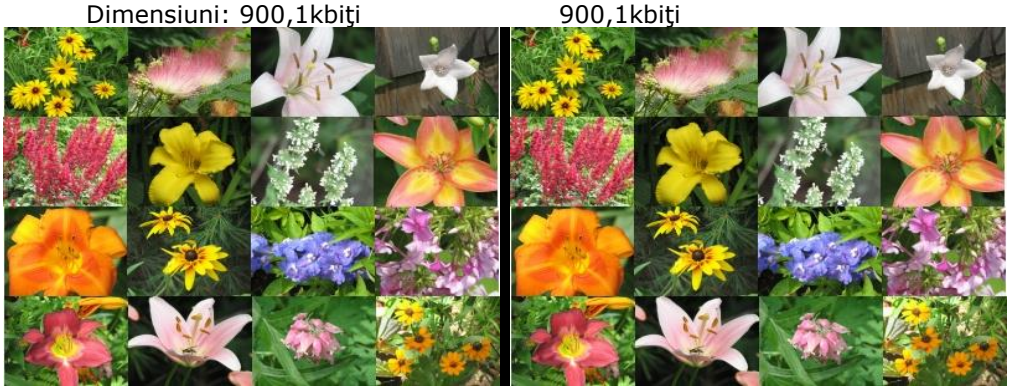
Raport de ascundere : mesaj/obiect de acoperire: 0.3521

Eroarea relativă dintre imaginea obiect de acoperire şi imaginea steganografică:0,92%

Eroarea relativă dintre mesajul secret şi mesajul extras: 1,59%

Obiect de acoperire
Dimensiuni: 900,1kbiţi

Obiect steganografic
900,1kbiţi



Mesaj secret
Dimensiuni: 265kbiţi

Mesaj recuperat
265kbiţi

Figura 7.12 Algoritmul BPCS - Experimentul b

$\propto = 0{,}3$

Raport de ascundere : mesaj/obiect de acoperire: 0.293

Eroarea relativă dintre imaginea obiect de acoperire şi imaginea steganografică:0,92%

Eroarea relativă dintre mesajul secret şi mesajul extras: 0,80%

Obiect de acoperire
Dimensiuni: 900,1kbiţi

Obiect steganografic
900,1kbiţi

Mesajul secret
Dimensiuni: 96,2kbiţi

Mesajul recuperat
96,2k biţi

Figura 7.13 Algoritmul BPCS - Experimentul c

$\alpha = 0{,}3$

Raport de ascundere : mesaj/obiect de acoperire:0,107

Eroarea relativă dintre imaginea obiect de acoperire şi imaginea steganografică:0,92%

Eroarea relativă dintre mesajul secret şi mesajul extras: 0,17%

Pentru efectuarea testelor în tabelul 7.3 se prezintă unul dintre experimentele efectuate având următoarele date: complexitatea pragului ales este de 0,2, respectiv 0,3, capacitatea mesajului ascuns este aleasă variabil, iar ca rezultat în ultima coloană se prezintă eroarea relativă dintre imaginea de acoperire şi imaginea steganografică rezultată. Capacitatea obiectului de acoperire folosit în experimente este de 700 kbiţi. Din tabel se constată că raportul maxim de ascundere este de 0,34% din imaginea de acoperire, în cazul când $\alpha = 0{,}3$, respectiv 0,43% pentru cazul $\alpha = 0{,}2$.

Tabel 7.3 Comparaţii eroare relativă şi cantitate ascunsă BPCS

alfa	Capacitatea maxima de informaţie ce se poate ascunde [kbiți]	Capacitate a mesajului ascuns [kbiți]	Eroarea relativă dintre obiect de acoperire/ obiect steganografic
0.3	244	20	0.0004
		40	0.0009
		60	0.0013
		80	0.0018
		100	0.0025
		120	0.0031
		140	0.0038
		180	0.0050
		200	0.0081
		220	**0.0105**
		240	0.0157
0.2	313 k	40	0.0009
		80	0.0018
		120	0.0031
		160	0.0045
		200	0.007
		240	**0.0103**

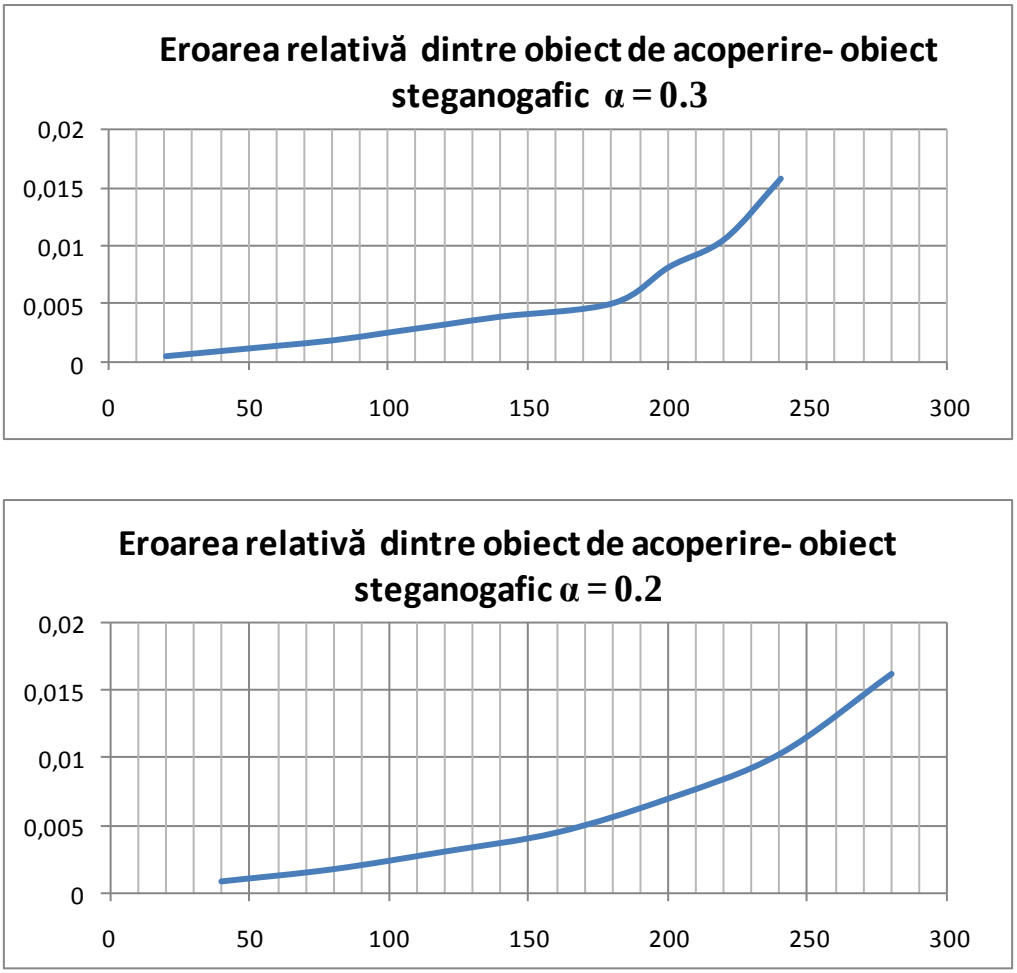


Figura 7.14 Eroare relativă – BPCS

În figura 7.14 se prezintă raportul dintre cantitatea de informaţii ascunsă şi eroarea relativă dintre obiectul de acoperire şi obiectul steganografic. Pe axa orizontală este reprezentată cantitatea informaţiei ascunse exprimată în kbiţi, iar pe verticală se regăseşte eroarea relativă. Consider că obţinerea unei erori relative mai mici de 1% implică reducerea cantităţii de informaţii ascunse, aşa cum se remarcă în figura 7.14 unde se observă o creştere exponenţială a erorii pentru o capacitate de ascundere mărită, ceea ce poate afecta în mod evident şi degradarea obiectului steganografic.

7.3.4 Concluzii - BPCS

În concluzie este de remarcat faptul că prelucrările multiple efectuate în cadrul procesul de generare a obiectului steganografic implică timpi de execuţie cu atât mai mari cu cât procesul de prelucrare este mai complex. Din acest motiv

algoritmul bazat pe complexitatea planurilor de biţi este inoperant în executarea lui în timp real.

Pe de altă parte algoritmul poate prezenta avantajul că prelucrările multiple nu sunt cunoscute de către un eventual atacator, ceea ce face dificilă recuperarea neautorizată a acestuia.

Mai mult, dacă ascunderea se face doar în planurile de biţi mai puţin semnificative, calitatea imaginii steganografice este deosebit de bună, neatrăgând atenţia celui care doreşte analiza obiectului steganografic. Astfel de algoritmi pot implica o mare varietate de soluţii care să conducă la creşterea rezistenţei unui eventual atac.

Algoritmul bazat pe complexitatea planurilor de biţi a constituit pentru mine un bun exemplu ca studiu de caz permiţându-mi totodată realizarea unei comparaţii în ceea ce priveşte calitatea sistemului steganografic vis-à-vis de timpul de execuţie al acestuia. În acest sens se poate constata faptul că multiplele prelucrări pot îmbunătăţii calitatea obiectului steganografic, ceea ce confirmă încă o dată valabilitatea modelului steganografic propus în capitolul 6. Totodată efectuarea prelucrărilor multiple duce la ridicarea unor noi bariere în calea eventualilor atacatori.

Ca direcţie de cercetare viitoare doresc sa adaptez şi această implementare pentru a face posibilă ascunderea informaţiilor prin intermediul unui microprocesor în ideea găsirii altor variante de procesare care să reducă timpul de execuţie fără a afecta avantajele câştigate până în prezent. Identificarea unor noi metode de procesare ar putea conduce la utilizarea şi a acestui algoritm în scopul propus. În plus, este de aşteptat ca următoarele generaţii de microprocesoare mai performante din punct de vedere al frecvenţei de lucru şi al capacităţii memoriei să permită şi adaptarea acestui algoritm în condiţii optime.

7.4 *Concluzii - Algoritmi steganografici aplicaţi în domeniul spaţial*

Algoritmii de ascundere ce utilizează imagini reprezentate în domeniul spaţial prezintă avantajul că au un timp relativ redus de generare a imaginii steganografice, pot recupera mesajul secret cu o eroare relativ mică şi sunt uşor de implementat. Ca dezavantaj al acestor algoritmi se poate aminti faptul că ar putea fi vulnerabili la anumite tipuri de atacuri, cum ar fi încercarea introducerii unor zgomote pe canalul de transmitere a mesajului steganografic. În general introducerea zgomotelor pe canalul de transmitere este o problemă care nu ţine de generarea unei imagini steganografice de bună calitate, ci este legată de securitatea canalelor de transmisie care reprezintă un alt domeniu, de care nu mă ocup în această lucrare.

Prin calitatea generării unui mesaj steganografic bun şi prin repetitivitatea etapelor de generare a imaginii steganografice, așa cum am arătat mai sus, astfel de algoritmi se pretează foarte bine pentru a fi implementaţi hard.

Făcând o comparaţie între cei trei algoritmi steganografici realizaţi în domeniul spaţial se pot desprinde următoarele observaţii:

- Cantitatea cea mai mare de informaţii ce poate fi încorporată se poate obţine cu algoritmi steganografici bazaţi pe ascunderea în biţii cei mai puţini semnificativi, putându-se ajunge chiar la un raport dintre obiectul de acoperire şi mesaj de 100%.

- Cantitatea cea mai mică de informaţii ce poate fi ascunsă se obţine cu algoritmi bazaţi pe transformata YUV.
- Algoritmii care ar putea prezenta cele mai dificile posibilităţi de detecţie a mesajului sunt algoritmii bazaţi pe complexitatea planurilor de biţi care implică multiple prelucrări atât asupra mesajului ascuns, cât şi a obiectului de acoperire. De asemenea şi algoritmii bazaţi pe transformata YUV implică o serie de prelucrări ale mesajului. Mai mult, modul de transformare poate fi considerat ca o cheie suplimentară de protecţie.
- Eroarea relativă sub 1% se obţine practic cu toţi algoritmii implementaţi de mine în domeniul spaţial, dar bineînţeles având câteva elemente specifice. Astfel că: algoritmul bazat pe transformata YUV nu în toate experimentele generează eroarea menţionată, iar algoritmul bazat pe complexitatea planurilor de biţi impune în mod obligatoriu reducerea cantităţii informaţiei ascunse pentru obţinerea unei astfel de erori.
- Din punctul de vedere al timpului de rulare algoritmii bazaţi pe ascunderea informaţiilor în biţii cei mai puţini semnificativi ai obiectului de acoperire prezintă valori minime. Comparativ cu acesta, algoritmul bazat pe transformata YUV implică un timp de execuţie de 40 de ori mai mare, iar algoritmul bazat pe complexitatea planului de biţi un timp de 30 pană la 40 de ori mai mare.

În concluzie consider că algoritmii bazaţi pe ascunderea datelor în cei mai puţini semnificativ biţi prezintă un raport optim între cantitatea de informaţie ce poate fi ascunsă, timpul de execuţie şi calitatea obiectului steganografic obţinut. Din acest motiv am ales acest algoritm pentru a fi experimentat şi pe microprocesoarele ARM şi ISAAC ce sunt sau vor fi folosite în telefonia mobilă.

În continuare voi încerca să aduc noi îmbunătăţiri schemei de implementare, prin mărirea capacităţii memoriei alocate, o paralelizare mai accentuată a algoritmului, pentru a scădea timpul de execuţie. Mă gândesc că un astfel de algoritm ar putea fi implementat şi pe alte tipuri de microprocesoare folosite în telefoanele mobile fără prea mari modificări, pentru a asigura securitatea transmiterii mesajelor SMS şi de ce nu a convorbirilor, care la ora actuală au un grad de securitate redus.

8 STEGANOGRAFIA ÎN DOMENIUL FRECVENŢĂ

Din cele prezentate anterior se poate constata faptul cã tehnicile bazate pe modificări ale celor mai puþini semnificativi biþi reprezintã modalitãți uºoare de a încorpora informaþii secrete, însã acestea ar putea fi vulnerabile dacã nu se iau în considerare tehnici de protejare a informaþiei. În multe cazuri chiar ºi schimbările mici rezultate în urma comprimărilor cu pierderi pot duce la o degradare parþialã sau totalã a informaþiei ascunse [JOH01]. Aceste afirmaţii la ora actuală pot fi combătute relativ simplu deoarece există foarte multe metode de contracarare a atacurilor aşa cum am arătat în capitolul precedent.

S-a observat de-a lungul timpului cã prelucrarea informaþiilor în domeniul frecvenþei conduce la micºorarea timpului de procesare, ceea ce face ca multe dintre sistemele steganografice cunoscute azi sã opereze în domeniul frecvenþei folosind diferite transformate specifice acestuia [YUA08].

Metodele bazate pe domeniul transformatelor ascund mesaje în zone semnificative ale imaginii de acoperire ceea ce le poate face mai puternice împotriva atacurilor. Astfel de metode sunt: comprimarea, decuparea ºi alte procesări ale imaginii, acestea fiind diferite de cele abordate în procesarea efectuatã în algoritmi bazaþi pe ascunderea în biþii cei mai puþini semnificativi ai obiectului de acoperire. Totodatã, în timp ce ele sunt mai viguroase faþã de alte procesări ale semnalului, rãmân imperceptibile sistemului senzorial uman. Există numeroase variaþii ale domeniului transformatelor.

Există numeroase metode bazate pe domeniul transformatei, acestea fiind independente faþã de formatul imaginii. Pot de asemenea apărea conversii între formate cu pierdere ºi fără pierdere. Cele mai utilizate metode de ascundere în domeniul frecvenþei se bazează pe transformări de tipul DCT (Discret Cosinus Transform), FFT(Fast Fourier Transform), DFT(Discret Fourier Transform), cu menþiunea cã prima transformatã este cea mai frecvent utilizatã.

8.1 *Algoritm steganografic bazat pe transformata cosinus discretă DCT*

Se dovedeşte că steganografia este o arie importantă dezvoltată în ultimii ani în securizarea informaţiilor în încorporarea unui mesaj ascuns într-un obiect de acoperire rezultând un obiect steganografic ce este imperceptibil simţurilor umane şi /sau unor algoritmi de steganaliză. Astfel obiectul de acoperire devine purtătorul unor mesaje secrete.

Pe baza acestor afirmaţii la ora actuală s-a dezvoltat steganografia modernă ce-şi propune ca sarcină de bază încorporarea mesajelor într-un obiect de ascundere fără posibilitatea de detecţie. Ca urmare a acestui obiectiv în [RAJ05] sunt prezentate mai multe metode steganografice care combinã algoritmii steganografici LSB ºi DCT ºi alte tehnici de comprimare ale imaginilor în vederea creºterii securitãþii imaginii steganografice. Într-o primã etapã algoritmul LSB este folosit pentru a încorpora biþii mesajului secret, iar în etapa următoare imaginea

steganograficã rezultatã este transformatã din domeniul spaþial în domeniul frecvenþã utilizând transformata DCT.

Un numãr mare de programe steganografice comerciale folosesc ca metode de ascundere metoda LSB, atât a imaginilor color (24 biþi), cât ºi a imaginilor alb negru (8 biþi). În general se constatã cã modificãrile fãcute în cel mai puþin semnificativ bit nu pot fi detectate datoritã zgomotului care este prezent tot timpul în imaginile digitale. Pentru a mãri ºi mai mult gradul de rezistenþã la atacuri [HAS05] descrie o tehnicã LSB, combinatã cu o tehnicã de inserare DCT.

Transformata discretã a cosinusului este una dintre cele mai populare sisteme de comprimare a imaginilor digitale folosite în ziua de azi. Una din provocãrile majore ale steganografiei este rezistenþa informaþiei la transmiterea imaginii steganografice pe canale afectate de zgomot. Cu ajutorul algoritmilor de ascundere ce folosesc transformata DCT sunt permise modificãri imperceptibile ale imaginilor steganografice în cazul recepþionãrii ei, iar recuperarea datelor se poate face complet în absenþa zgomotelor. Un astfel de exemplu se prezintã în lucrãrile [AGR09] şi [TAN08].Transformatele pot fi aplicate asupra întregii imagini dar ºi asupra anumitor blocuri din imagine [SAJ08]. Influenþa celor mai înalþi coeficienþi DCT este redusã, deoarece de obicei ei sunt acoperiþi de zgomot ºi nu se aºteaptã sã contribuie semnificativ la alcãtuirea detaliilor imaginilor. Pasul urmãtor presupune aplicarea transformatei DCT inverse cu scopul de a reconstrui datele. În acest fel, imaginea reconstruitã va fi foarte aproape de cea originalã, însã nu identicã cu ea. Dacã valorile cuantizãrii sunt stabilite în mod corespunzãtor, nu ar trebui sã existe diferenþe observabile de cãtre un eventual atacator [SAR07].

Pentru creºterea securitãþii imaginii steganografice sunt utilizaþi algoritmi prin intermediul cãrora mesajul secret este comprimat de aºa manierã încât pierderile sã fie nesemnificative. În acest mod poate creºte capacitatea de ascundere cunoscând faptul cã utilizarea unor astfel de transformate implicã cantitãþi mici de informaþii ce pot fi încorporate. În [YAH08] este propus un algoritm de ascundere bazat pe transformata cosinus discretă DCT în vederea creşterii capacităţii de ascundere, dar şi a robusteţii.

O metodă eficientă de ascundere bazată pe strategii de încorporare a datelor pe nivele este descrisă în [CHI09]. Autorii afirmă că această soluţie ce utilizează transformata DCT este superioară altora citate în lucrare pentru majoritatea imaginilor testate.

Practic, în transformarea JPEG mai întâi se converteºte imaginea care trebuie comprimatã în spaţiul culorii YC_bC_r ºi împarte fiecare zonã de culoare în blocuri 8x8 pixeli [XIA08c]. Apoi pentru toate blocurile se aplicã transformata cosinus discretã. În urmãtorul pas al cuantizãrii toţi coeficienþii DCT sunt împãrþiþi cu ajutorul unor valori de cuantizare predefinite, ºi rotunjite spre cel mai apropiat întreg. După declaraþia autorilor, metoda propusă se dovedeşte a fi eficientă în steganaliză.

Pentru a contracara eventualele atacuri asupra obiectelor steganografice, Koksheik propune în [KOK07] o metodă steganografică ce foloseşte transformata DCT şi un set de operaţii aritmetice modulo 4 pentru a încorpora o pereche de biţi în imaginea de ascundere. Algoritmul se dovedeşte a fi deosebit de rezistent metodelor de atac prin steganaliză.

[RUF04] prezintă un algoritm steganografic care se bazează pe similaritatea ce există între coeficienţii DCT ce aparţin blocurilor adiacente ale imaginii. Pe baza acestor observaţii distorsiunile apărute se împrăştie spre blocurile adiacente ale imaginii. Rezultatele obţinute demonstrează rezistenţa la atacurile tipice. Este

cunoscut faptul că scopul principal al metodelor steganografice este de a încorpora o imagine secretă într-o imagine purtătoare în aşa fel încât imaginea rezultată să rămână cât mai asemănătoare cu versiunea originală. Pe lângă aceasta, imaginea purtătoare ar trebui să rămână robustă la atacurile clasice. În [KER05] este prezentată o metodă ce încearcă să acopere toate aceste preocupări.

În lucrările [CRU06, CAI07] au fot implementate în imagini video în format MPEG-2 şi MPEG-4 metode de ascundere pentru imagini video cu rezultate bune privind imaginile steganografice. Cele două lucrări utilizează ca şi modalitate de ascundere algoritmi bazaţi pe transformata cosinus discretă DCT.

Pentru testarea şi validarea performanţelor algoritmilor steganografici bazaţi pe transformata cosinus discretă am implementat două soluţii prezentate în lucrările [STA07b] şi [STA08a].

Un prim algoritm realizat de mine în [STA07b] a condus la încorporarea datelor în cadrele unor imagini video. Datorită caracteristicilor sale în timp real transmiterea cadrelor de date reprezintă un subiect înrudit cu constrângerile impuse de lărgimea benzii de frecvenţă. Pornind de la principiul de funcţionare al algoritmului MPEG – 2 am propus un algoritm ce utilizează ascunderea de date pentru a transmite informaţii adiţionale fără a necesita o lărgime de bandă suplimentară rezultând astfel o degradare aproape de neperceput a imaginii. Datele adiţionale transmise pot fi subtitrări, semnale de corecţie sau watermarking. Astfel, în articol s-a aplicat algoritmul bazat pe transformata cosinus discretă pentru compresia unor imagini MPEG2 si generarea unor imagini steganografice. Folosind cadre de mărimi 720×576 pixeli au fost încorporate un text generând astfel imagini steganografice fără a avea diferenţe semnificative faţă de obiectul de acoperire iniţial.

În [STA08a] am prezentat tehnici steganografice referitoare la watermarking punându-se accent pe robusteţe şi cantitatea de informaţie ascunsă. Robusteţea este obţinută utilizând o transformare optimă, iar rata biţilor este obţinută procesând înainte semnalul de watermark. Se aplică totodată şi transformata KLT cu ajutorul căreia se transformă obiectul de acoperire, după care se pregăteşte watermark-ul pentru încorporarea sa. Acest lucru se realizează prin utilizarea unor tehnici folosite în comprimarea JPEG: separarea blocurilor, transformata cosinus discretă şi cuantificarea. Imaginea watermark este divizată în $n \times n$ blocuri, utilizându-se aceeaşi valoare pentru n ca şi pentru imaginea purtătoare. Având un mare grad de concentrare a energiei, KLT este ales ca fiind potrivit pentru ascunderea datelor.

De asemenea, în [STA08a] s-a arătat ºi faptul cã metoda propusã este foarte robustã împotriva atacurilor severe precum filtrul trece jos, codarea comprimatã, având o performanþã foarte bunã. Mai mult, transformarea cosinus discretã permite încorporarea watermark-urilor dintr-o singurã culoare, ºi implicã sporirea cantitãþii de date ce pot fi ascunse. Mai multe amãnunte în legãturã cu capacitatea sa de rezistenþã împotriva atacurilor se aflã sub investigaþie, de exemplu utilizarea unui model partiþionat al imaginii, ºi nu un bloc fix $n \times n$. Precizez cã imaginea steganograficã rezultatã prezintã o robusteþe ridicatã satisfãcând scopul urmãrit, putându-se astfel recupera în întregime mesajul ascuns, chiar în cazul aplicării unor zgomote puternice pe imaginea steganograficã.

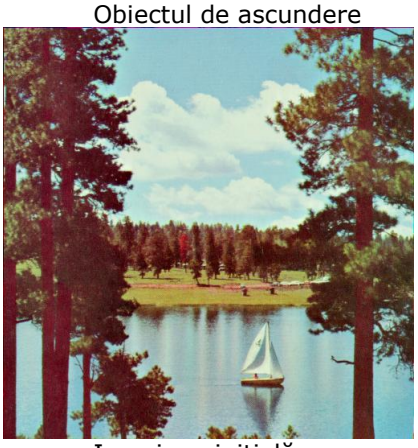
8.1.1 Experimente DCT

În figura 8.1. se prezintă un exemplu de ascundere a unui mesaj folosind transformata cosinus discretă. Menţionez că asupra acestui algoritm nu voi insista în această lucrare fiind descris în [STA08a]. Se constată că imaginea recuperată în

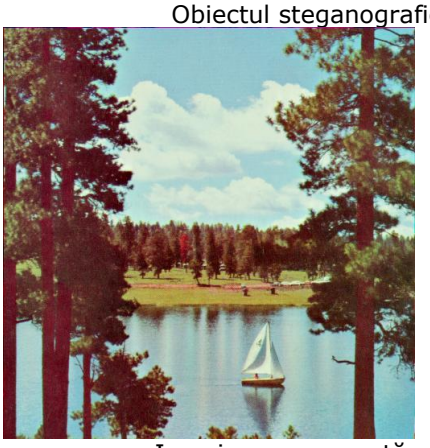
cazul aplicării unui semnal de zgomot este afectată într-o proporţie foarte mică fiind relativ simplu de recunoscut imaginea iniţială.

Obiectul de ascundere

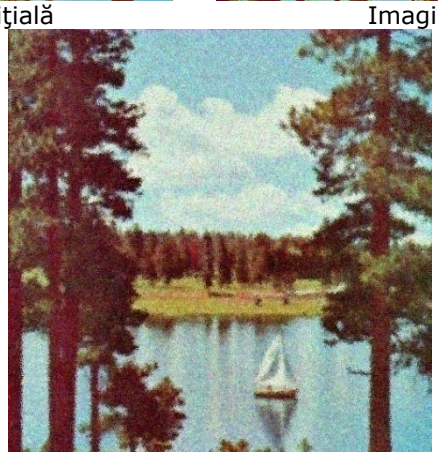
Obiectul steganografic



Imaginea iniţială



Imaginea recuperată



Imaginea recuperată în cazul aplicării unui semnal de zgomot

Figura 8.1 DCT – Rezultate experimentale

Datorită caracteristicilor algoritmilor ce se bazează pe transformata cosinus discretă cantitatea de informaţii ascunse a fost cu 3 ordine de mărime mai mică decât în cazul utilizării algoritmilor bazaţi pe ascunderea în bitul cel mai puţin semnificativ, respectiv algoritmii bazaţi pe complexitatea planurilor de biţi, şi cu 2 ordine de mărime mai mic decât în cazul utilizării algoritmilor bazaţi pe transformata YUV. În plus, erorile relative obţinute depăşesc de 1 până la 5 ori erorile relative obţinute cu algoritmii implementaţi în domeniul spaţial.

Sigur că obiectivele algoritmilor menţionaţi au urmărit proprietăţi legate de robusteţea obiectului steganografic, însă am ţinut cont şi de faptul că unul din algoritmi a fost implementat pe un mediu relativ rar folosit în steganografie, şi anume imagini video.

Rezultatele comparative ale algoritmilor ce folosesc transformata DCT se regăsesc în tabelul 10.1 din capitolul 10. Se poate constata că acest algoritm este unul dintre cei mai puţini performanţi în ceea ce priveşte cantitatea de informaţie ascunsă. Din acest motiv, acest algoritm l-am implementat doar în dorinţa de a constitui un studiu de caz privind compararea performanţelor lui faţă de alţi algoritmi prezentaţi în această lucrare. Utilizarea transformatei cosinus discretă este utilă în prelucrări de imagini şi comprimarea acestora, în schimb nu prezintă aceleaşi rezultate şi în steganografie, fiind utilizat cu precădere în watermarking pentru protecţia proprietăţii intelectuale.

8.1.2 Concluzii

Algoritmii care utilizează domeniul frecvenþă, datoritã capacitãþii de compactare a imaginilor au fost în atenþia numeroºilor autori de algoritmi steganografici. Ceea ce dezavantajează aceºti algoritmi constituie rata micã de ascundere, în schimb prezintã o robustețe sporitã, ceea ce îi fac utili la generarea semnãturilor digitale sau la încorporare de watermak-uri.

În domeniul frecvenþei au loc diferite transformări ale imaginilor bazate pe modificarea anumitor coeficienþi specifici transformatei aplicate, fapt ce permite ascunderea de informaþii secrete în aceºtia. Acest domeniu poate fi utilizat pentru a creºte rezistenþa la detectarea informaþiei ascunse. De asemenea astfel de transformate permit obþinerea unor imagini digitale sau video cu un anumit grad de comprimare, ceea ce poate fi benefic în cazul sistemelor steganografice.

O concluzie legată de aplicarea algoritmului bazat pe transformata cosinus discretă constă în faptul că timpul de execuţie este relativ redus şi cu rezultate bune în ceea ce priveşte obţinerea unei imagini steganografice corespunzătoare. Utilitatea acestui algoritm prin combinarea cu alte tehnici cum ar fi LSB, YUV ar putea rămâne ca direcţie viitoare de cercetare.

9 STEGANOGRAFIA ÎN DOMENIUL VECTORIAL

Unul dintre cele mai importante atribute ale steganografiei îl constituie alegerea unei tehnici potrivite pentru ascunderea unor informaţii secrete. Gradul de reuşită a unui proces steganografic constă în abilitatea unei astfel de alegeri. În situaţia în care o altă persoană decât cele implicate direct în procesul steganografic (emiţătorul şi receptorul) poate să observe existenţa unor date ascunse într-un obiect steganografic la care are acces, atunci tehnica steganografică utilizată este inutilă.

Atunci când oamenii utilizează o anumită tehnologie într-un scop propriu, urmarea firească este ca în continuare aceştia să ceară diferite îmbunătăţiri. Astfel că în permanenţă are loc dezvoltarea de noi tehnologii în domeniul steganografiei. Deoarece lumea a devenit în mare parte digitală şi tehnicile steganografice dezvoltate în ultimii au necesitat anumite modificări pentru a fi aplicate în acest domeniu.

În marea lor majoritate tehnologiile existente prezintă anumite limitări, iar procesul de îmbunătăţire a acestora constă în înţelegerea lor şi luarea unor măsuri în vederea minimalizării impactului acestora în procesul steganografic.

Sistemele steganografice existente permit încorporarea unei anumite cantităţi de informaţie secretă fără a degrada obiectul de acoperire astfel încât să nu trezească suspiciuni unui eventual interceptor. La ora actuală steganografia are tendinţa de a ascunde o cantitate cât mai mare de date, ceea ce necesită în permanenţă dezvoltarea unor astfel de algoritmi care să permită comprimarea unei cantităţi mari de date, iar stocarea acesteia să fie în fişiere cât mai mici. Aşadar, capacitatea de a ascunde cantităţi mari de date cu ajutorul tehnicilor steganografice este un domeniu care poate fi îmbunătăţit.

Pentru sporirea securizării o soluţie ar fi codarea mesajului secret cu o cheie cunoscută doar de emiţător şi receptor, similar ca în criptografie. Aceasta ar putea constitui o tehnică de combinare a metodelor steganografice cu cele criptografice. Dacă nu este aleasă o tehnică potrivită pentru a ascunde date, iar obiectul steganografic trezeşte suspiciune atunci este posibil ca informaţia secretă să fie depistată. În cazul în care informaţiile secrete sunt protejate suplimentar cu o anumită cheie, la o detecţie se poate obţine conţinutul mesajului, însă acesta va fi de neînţeles atacatorului, datorită prezenţei cheii suplimentare. Ca atare, cu cât steganografia devine mai sofisticată, rezistenţa sa împotriva analizării sau chiar a recunoaşterii sale devine din ce în ce mai puternică. Astfel că se vor face în permanenţă eforturi considerabile pentru a face steganografia să fie de nedetectat pentru oricine în-afara celor care au realizat-o.

Pornind de la reprezentarea imaginilor în diferite domenii sunt într-o continuă dezvoltare şi algoritmi steganografici ce pot fi aplicaţi în domeniile respective. Astfel că, pe lângă domeniul spaţial şi frecvenţă există şi un alt spaţiu în care imaginile pot fi reprezentate, cunoscut sub numele de spaţiu vectorial [HOG06]. Conceptul de spaţiu vectorial este bazat pe ideea de vectori. Cel mai simplu exemplu de vector care se poate imagina este desenarea unei săgeţi într-un plan fix de două sau trei coordonate, care începe dintr-un punct fix. Vectorii sunt utilizaţi în general pentru obiecte asupra cărora se pot aplica două tipuri de operaţii,

şi anume adunarea, respectiv înmulţirea vectorilor cu un scalar. O mare parte dintre algoritmii steganografici care utilizează într-un mod sau altul vectori şi valori proprii prezintă un grad ridicat în ceea ce priveşte robusteţea, datorită faptului că vectorii şi valorile proprii păstrează foarte bine informaţia.

Cele mai cunoscute aplicaţii în domeniul steganografiei bazate pe domeniul vectorial sunt cele care utilizează transformatele SVD, respectiv KLT. Ambele transformate prezintă proprietăţi ce pot fi exploatate în algoritmi steganografici, atât pentru obţinerea comprimării imaginii, cât şi pentru generarea unor procesări suplimentare asupra obiectelor ce sunt folosite în sistemele steganografice. Procesarea asupra acestor obiecte conduce la îmbunătăţirea erorilor rezultate în urma ascunderii prin generarea unui obiect steganografic de calitate superioară. Mai mult, se obţine îmbunătăţirea procesului de recuperare cu mai multă acurateţe a mesajului secret, cât şi creşterea robusteţii obiectului steganografic.

9.1 *Transformata SVD aplicată în steganografie*

Tehnicile de ascundere ce folosesc transformata SVD urmăresc să facă recuperarea mesajului secret cât mai dificilă de către terţe persoane. În acest scop algoritmii bazaţi pe transformata SVD implică obţinerea unui obiect steganografic care să nu trezească suspiciune, ceea ce presupune o procesare suplimentară asupra obiectelor participante în sistemul steganografic. Cunoscând faptul că transformata SVD implică un grad mic de încorporare de date, tendinţa care se manifestă în ultimul timp constă în mărirea capacităţii de ascundere. O soluţie în acest sens ar fi compactarea fără pierderi a informaţiilor din mesajul secret.

În [GOR03] se prezintă un studiu experimental al proprietăţilor unei noi tehnici de ascundere a informaţiei bazate pe imagini ce sunt critice pentru comunicarea ascunsă. Tehnica presupune aplicarea transformatei SVD asupra unei imagini digitale şi foloseşte inserarea unui bit de date prin mici modificări a unei combinaţii liniare ale unei valori dintr-un bloc de dimensiuni mici aparţinând imaginii de acoperire. Ideea principală a acestui studiu constă în găsirea unei dependenţe între rata de încorporare a datelor invizibile şi robusteţea obiectului steganografic. Un alt obiectiv urmărit constă în realizarea unor recomandări practice referitoare la ajustarea atributelor controlabile ale procedurii de încorporare de date bazată pe transformata SVD. Rezultatele studiului oferă informaţii privind modalitatea abordării procesului steganografic.

Pentru creşterea capacităţii de încorporare a datelor secrete şi obţinerea unui obiect steganografic robust în [BAB07] este propus un algoritm ce utilizează transformata SVD şi se bazează pe două proprietăţi importante ale acesteia, şi anume: valorile singulare reprezintă luminozitatea sau energia imaginii digitale, iar perechea relevantă a vectorilor singulari reprezintă geometria imaginii, astfel că mici variaţii ale transformatei SVD nu pot afecta perceperea vizuală a imaginii. Pe baza acestor observaţii obiectul de acoperire este transformat, iar mesajul secret ce urmează a fi transmis se încorporează în valorile singulare ale acestuia. Din punctul de vedere al performanţelor algoritmul prezintă caracteristici superioare faţă de algoritmii luaţi în calcul de autori.

Pe baza transformatei SVD bazându-se şi pe proprietăţile sistemului auditiv uman folosind ca obiect de acoperire formatul MP3 utilizat în domeniul audio, în

[BAO04] se descrie un sistem steganografic deosebit de robust cu o recuperare sigură a datelor.

Se remarcă faptul că folosirea transformatei SVD îndepărtează dependenţa liniară relativă dintre rândurile şi coloanele unei imagini [GUL08b]. Cunoscând faptul că imaginile care prezintă asemenea dependenţe pot crea suspiciuni că ar conţine informaţii secrete, rezultă că prin folosirea transformatei SVD la astfel de imagini s-ar putea creşte gradul de robusteţe în cazul unor atacuri.

Prin schimbarea valorilor singulare a unei imagini se constată că acest lucru nu afectează calitatea imaginii prea mult. În [YAV07] se dezvoltă unele metode bazate pe SVD prin care informaţia secretă este încorporată în valorile singulare ale imaginii de acoperire. În situaţia unui atac, dacă vectorii singulari ai altei imagini sunt folosiţi în detrimentul imaginii originale acest lucru ar genera un fals, ceea ce ar permite detectarea dreptului de proprietate a originalului.

9.1.1 Algoritm steganografic bazat pe descompunerea în valori singulare

În [STA08b] prezint un algoritm bazat pe descompunerea matricei corespunzătoare obiectului de acoperire, cât şi pe compresia mesajului folosind un algoritm ce cuantizează valorile acestuia. Paşii algoritmului sunt următorii:

Algoritm de ascundere

1) Din fişierul obiectului de acoperire tip imagine se formează matricea M cu valorile corespunzătoare pixelilor. Dacă imaginea este alb-negru se va construi o singură matrice, iar dacă este color pentru fiecare culoare R,G,B se vor forma 3 matrice.
2) Matricea (matricele) M se împarte în sub-blocuri de dimensiune 8×8, notate A . Submatricele rezultate sunt împărţite la rândul lor în matrice pare A_1, respectiv impare A_2. Dacă matricea M nu poate fi împărţită exact în submatrice A_i atunci surplusul de linii şi coloane se poate ignora.
3) Folosind transformata SVD se determină matricele U , S , V pentru fiecare bloc.
4) Asupra mesajului secret care este format din biţi ce au valori 0 sau 1 se face o conversie prin care valorile [0,1] sunt convertite în valori de [-1,1] folosind următoarea formulă de calcul: „0" se va înlocui cu 2×0-1=-1; „1" se va înlocui cu 2×-1=1
5) Mesajul secret este împărţit în blocuri de 4×4, iar fiecare bloc este comprimat folosind o compresie DXT [KRA07]. Ca urmare, prin cuantizarea fiecărei valori din bloc obţinută cu relaţia:
$$c = \alpha \times low + (1 - \alpha) \times high \quad (9.1)$$
6) Pentru încorporarea mesajului secret se va folosi numai matricea U , care este împărţită în 3 regiuni, aşa cum se constată în figura 9.1.

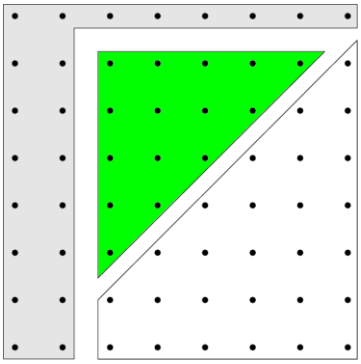


Figura 9.1 Regiunile de bază ale matricei U

Informaţia secretă va fi încorporată numai în zona de deasupra diagonalei secundare (regiunea verde). În total pot fi ascunşi 15 biţi în blocul par şi 15 biţi în blocul impar.

7) Formula folosită pentru ascunderea datelor secrete este:

$$u'_{ij} = p_k \times |u_{ij}| \quad (9.2)$$

Unde, i = 3...8, iar j = 2...9 – i

p_k reprezintă biţii din informaţia secretă,

u_{ij} reprezintă elementele matricei A .

De menţionat că valorile lui p_k vor fi +1 sau – 1 în funcţie de valoarea bitului ascuns. Ca urmare efectul produs de relaţia (9.2) determină ca valorile lui u'_{ij} să genereze o nouă matrice U' diferită de cea originală U numai prin semn (+ sau -). Semnul elementului u'_{ij} din matricea U' va fi de fapt informaţia ascunsă. Din cauză că elementele ce se află deasupra diagonalei secundare sunt modificate şi având în vedere că U' trebuie să fie ortogonală, rezultă că este necesară şi modificarea elementelor de sub diagonala secundară. Ortogonalitatea presupune calcularea unui sistem de ecuaţii liniare ce foloseşte algoritmul de eliminare Gauss – Jordan [STR03]. În felul acesta matricea U' va fi ortogonală.

8) Se calculează matricele de forma : $A' = U' \times S \times V^T$. Acest pas presupune reconstituirea blocurilor de pixeli, dar de data aceasta sunt incorporate şi informaţiile secrete.

9) Se reconstituie matricea M' folosind noile submatrici A' determinate în pasul anterior. Matricea M' constituie de fapt obiectul steganografic.

Algoritmul de extragere

1) Matricea obiectului steganografic M' se descompune în submatrice $\bar{A}$ de dimensiune 8×8.

2) Folosind transformata SVD se determină matricele $\bar{U}, \bar{S}$, $\overline{V^T}$.

3) Se extrag biţii cu informaţia ascunsă din $\bar{U}$ din semnul elementelor de deasupra diagonalei principale folosind formula:

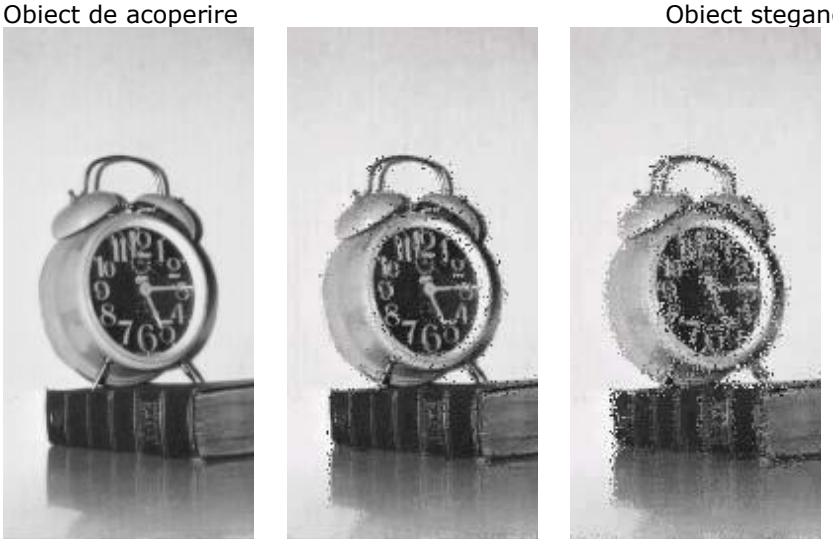
$$p_k = \frac{\overline{u_{ij}}}{\left|\overline{u_{ij}}\right|} \tag{9.3}$$

4) Se concatenează toţi biţii rezultaţi în urma extragerii informaţiei ascunse din matricele $\bar{A}$ obţinându-se în final mesajul secret.

9.1.2 Experimente SVD

Pentru experimentarea algoritmului bazat pe descompunerea în valori singulare pentru unul din experimente, prezentat în figura 9.2 s-a folosit ca obiect de acoperire o imagine alb negru, de dimensiune 512 × 512 pixeli (72,7Kbiţi, în format JPEG). Mesajul secret este o imagine alb negru, de dimensiune 128 × 256 pixeli (9Kbiţi, în format JPEG).

Obiect de acoperire Obiect steganografic



Mesaj secret Mesaj recuperat Mesaj recuperat în prezenţa zgomotului

Figura 9.2 Rezultate algoritm steganografic bazat pe transformata SVD

Se constată din figura 9.2 că imaginea recuperată chiar şi în prezenţa unor zgomote poate fi recunoscută comparativ cu imaginea iniţială, ceea ce dovedeşte caracteristicile de robusteţe ale algoritmului steganografic bazat pe transformata SVD.

9.1.3 Concluzii

Am constatat în urma implementării algoritmului menţionat mai sus la care am adus unele modificări legate de compactarea mesajului secret că raportul de ascundere este $\frac{1}{8}$ din imaginea de acoperire, ceea ce este mult inferior algoritmilor bazaţi pe bitul cel mai puţin semnificativ, cât şi cei bazaţi pe complexitatea planurilor de biţi, fiind doar comparabili cu algoritmii bazaţi pe transformata YUV şi pe cei bazaţi pe transformata cosinus discretă. O statistică privind compararea algoritmilor bazaţi pe descompunerea în valori singulare se prezintă în tabelul 10.1 din capitolul 10. Se poate constata pe baza comparaţiilor unor performanţe legate de cantitatea de informaţie ascunsă, calitatea imaginii steganografice şi raportul de recuperare al mesajului că astfel de algoritmi se clasează printre algoritmii cu performanţe relativ reduse din punct de vedere steganografic. Pe de altă parte datorită prelucrărilor multiple efectuate asupra obiectului de acoperire astfel de algoritmi permit creşterea gradului se securizare a datelor ascunse, precum şi o robusteţe sporită la eventualele atacuri. Din acest motiv astfel de algoritmi sunt recomandaţi în domeniul watermarking-ului pentru protejarea proprietăţii intelectuale. Algoritmul constituie un studiu de caz pentru eventualele dezvoltări ulterioare.

Legat de timpul de execuţie se poate constata că algoritmul bazat pe transformata SVD necesită un număr relativ mare de operaţii care în mod evident sunt consumatoare de timp, ceea ce conduce la faptul că timpul de execuţie a unui astfel de algoritm devine relativ mare în cazul în care obiectul de acoperire şi mesajul secret au dimensiuni mai mari. Din acest motiv este de presupus că un astfel de algoritm nu poate satisface condiţiile de lucru în timp real, fiind puţin probabil că poate fi utilizat în prezent în telefonia mobilă. O soluţie de viitor legată de astfel de algoritmi ar consta în proiectarea unei scheme cablate pentru executarea algoritmilor. Interesul pentru astfel de algoritmi este firesc la ora actuală deoarece se caracterizează printr-o robusteţe mare chiar şi în cazul unui atac.

9.2 *Transformata KLT aplicată în steganografie*

După cum am arătat în paragrafele anterioare, transformata KLT este considerată ca fiind o prelucrare optimă a semnalelor pentru reprezentarea, compresia, analiza şi procesarea datelor. Această transformată este utilizată în foarte multe domenii unde apar secvenţe sau procese aleatoare, fiind optimă din punct de vedere statistic, în sensul că oferă cea mai bună compactare în raport cu recorelarea datelor şi păstrarea celor mai importante informaţii din acestea. Prezintă însă o problemă, şi anume faptul că necesită un număr mare de prelucrări de date, unele de capacitate mare ceea ce face ca timpul de execuţie să fie mare [HOG06]. Dar în cazul unor divizări pe blocuri a imaginii digitale, așa cum se va vedea în

continuare, aceste costuri de timp se pot reduce semnificativ, iar rezultatele generării unor algoritmi steganografici foarte puternici sunt de apreciat.

În [WUZ96] este realizat un studiu ce utilizează histograma imaginii pentru a identifica locul unde trebuie ascunse datele secrete. În acest sens se pune accentul pe proprietăţile transformatei KLT aplicate unei imagini pentru a identifica histograma cea mai potrivită pentru încorporarea datelor astfel încât să se obţină imagini de o calitate cât mai bună.

Rata de distorsiune a imaginilor în urma unui proces steganografic şi complexitatea transformatelor liniare pentru comprimarea datelor cu pierderi sunt două probleme importante ce sunt analizate în [FEN02]. Scopul urmărit în lucrare este o mai bună înţelegere a aspectelor legate de performanţă/complexitate asociate transformatei KLT şi aproximărilor sale imediate.

Prin aplicarea transformatei KLT asupra unei imagini rezultă o nouă imagine ale cărei componente (pixelii) sunt într-un mod ideal independente din punct de vedere statistic. Utilizarea transformatei KLT poate fi luată în considerare şi pentru generarea unui algoritm steganografic fie prin modul de procesare a imaginii, fie prin comprimarea mesajului secret, ceea ce implică în mod normal realizări multiple ale unei imagini. Pornind de la aceasta, în [DAF03] se propune o metodă pentru ascunderea unei imagini monocrome digitale, folosind transformarea Karhunen-Loeve (KLT).

Pentru creşterea capacităţii de ascundere şi mărirea robusteţii imaginii ascunse în [PIV00] se prezintă o metodă de ascundere în domeniul RGB bazată pe transformata KLT. Această transformată se aplică componentelor RGB, iar ascunderea se face în domeniul transformatei Fourier discretă.

În [CHE07] este prezentat un cadru pentru realizarea unei monitorizări vizuale robuste folosind proprietăţile transformatei KLT, deoarece este foarte importantă pentru multe aplicaţii vizuale.

O soluţie interesantă de transmitere a unui mesaj secret în timp real este dezvoltată în lucrarea [MOU03] prin care se propune o metodologie de joc teoretic la care participă doi sau mai mulţi adversari / aliaţi. Mesajul secret este încorporat in imagini în prezenţa adversarilor fără ca aceştia să sesizeze schimbul de informaţii. Este de precizat faptul că transformata KLT joacă un rol central în distribuţia optimă a mesajului. Mai mult, la atacurile adversarilor pentru sustragerea informaţiei ascunse metoda s-a dovedit deosebit de eficientă la astfel de situaţii.

O analiză a transformatelor discrete ortogonale este făcută în lucrarea [CAN08] unde se face o paralelă a proprietăţilor imaginilor digitale ce urmează a fi ascunse cu ajutorul transformatelor DCT şi KLT. Comparând cele două metode de ascundere a imaginilor digitale se constată că în cazul compresiei imaginii are loc o pierdere de informaţie. S-a constat că aceste pierderi sunt mai semnificative în cazul folosirii transformatei DCT. Pierderile rezultate la folosirea transformatei KLT sunt imperceptibile.

În [STA07a] şi [STA08a] am implementat două aplicaţii utilizând transformata KLT, în care s-a evidenţiat robusteţea imaginii steganografice.

În continuare voi prezenta alţi trei algoritmi ce se bazează pe proprietăţile transformatei KLT prin care voi scoate în evidenţă, în funcţie de caz: robusteţea mesajului steganografic, capacitatea lui de ascundere, respectiv timpul de execuţie. Pentru realizarea obiectivelor propuse, au fost adoptate anumite artificii de calcul, spre exemplu: folosind soluţii de comprimare a mesajului secret prin aplicarea transformatei KLT, combinate cu metode de ascundere a acestuia în biţii cei mai puţini semnificativi ai obiectului de acoperire. Alte soluţii posibile ar fi dispersia mesajului secret în obiectul de acoperire pe baza unor algoritmi pseudoaleatori ce pot fi consideraţi ca o cheie de acces în recuperarea acestuia. Pentru inducerea în eroare a unui eventual atacator în obiectul de ascundere se pot adăuga zgomote

care la rândul lor să conţină mesajul secret. Toate aceste soluţii pot utiliza cu succes transformata KLT.

9.2.1 Algoritm steganografic pentru ascundere prin comprimare - ASAC

Pentru a mări capacitatea de ascundere a unui mesaj secret am dezvoltat un algoritm în care procesul de ascundere se realizează în biţii cei mai puţini semnificativi ai obiectului de acoperire reprezentat în domeniul spaţial RGB prin comprimarea datelor folosind proprietăţile transformatei KLT. Prin combinarea celor două proceduri am urmărit practic trei direcţii de cercetare: creşterea capacităţii de ascundere a unor mesaje de capacitate mare, obţinerea unui obiect steganografic de o calitate foarte bună astfel încât deosebirea faţă de obiectul de acoperire să fie imperceptibilă şi îmbunătăţirea timpului de execuţie a programului prin segmentarea procesării imaginilor în ideea implementării acestui algoritm pe un microprocesor cu mai multe unităţi de procesare. Scopul final în realizarea acestui algoritm constă în paralelizarea procesului de execuţie în ideea implementării lui pe unul din telefoanele mobile ce urmează a fi lansate pe piaţă.

9.2.1.1 Descrierea algoritmului ASAC

În acest paragraf transformata KLT este utilizată pentru a comprima un mesaj ce urmează a fi încorporat într-un obiect de acoperire cu ajutorul algoritmului bazat pe ascunderea în biţii cei mai puţini semnificativi ai acestuia. În cele ce urmează se face o prezentare mai detaliată a paşilor urmaţi în algoritmul propus:

Compactarea mesajului secret

1.a.) Se consideră mesajul secret ca fiind exprimat printr-o matrice RGB notată cu M formată din m linii şi n coloane:

$$M = \begin{bmatrix} m_{1,1} & \cdots & m_{1,n} \\ & & \\ m_{m,1} & \cdots & m_{m,n} \end{bmatrix} \tag{9.4}$$

Unde $m_{i,j}$ reprezintă un pixel în cadrul imaginii. Fiecare pixel este compus din cele 3 culori de bază: roşu (R), verde (G) şi albastru (B).

$$m_{i,j} = \left(R_{i,j}, G_{i,j}, B_{i,j}\right) \tag{9.5}$$

1.b) Se împarte matricea M în blocuri de submatrice de dimensiunea $(5 \times n)$, unde (5 reprezintă numărul de linii, iar n numărul de coloane) rezultând o matrice de (3×5) linii şi n coloane, unde 3 reprezintă cele trei componente R,G,B ale unui pixel.

$$M^* = \begin{bmatrix} r_{1,1} & & r_{1,n} \\ g_{1,1} & \cdots & g_{1,n} \\ b_{1,1} & & b_{1,n} \\ r_{2,1} & & r_{2,n} \\ \vdots & \ddots & \vdots \\ r_{5,1} & & r_{5,n} \\ g_{5,1} & \cdots & g_{5,n} \\ b_{5,1} & & b_{5,n} \end{bmatrix} \tag{9.6}$$

2) Se construieşte matricea de covarianţă a submatricei M^* corespunzătoare mesajului secret M pentru cele ($15 \times n$) linii şi coloane, obţinându-se:

$$Cov(M^*) = \begin{bmatrix} a_{1,1} & \cdots & a_{1,15} \\ \cdot & & \\ a_{15,1} & \cdots & a_{15,15} \end{bmatrix} \quad (9.7)$$

3) Se calculează polinomul caracteristic, din care se determină valorile proprii $\lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_{15}$ care constituie de fapt şi rădăcinile polinomului caracteristic.

4) Se calculează vectorii proprii $\overrightarrow{v_1}, \overrightarrow{v_2}, \ldots, \overrightarrow{v_{15}}$ şi se formează astfel matricea Q, care este matricea vectorilor proprii a matricei de covarianţă exprimată în relaţia următoare :

$$Q = \overrightarrow{v_1}, \overrightarrow{v_2}, \ldots, \overrightarrow{v_{15}} \quad (9.8)$$

5) Se ordonează valorile proprii în ordine descrescătoare.

6) Se calculează coeficientul de calitate q, după relaţia:

$$q = \frac{\lambda_1 + \lambda_2 + \lambda_3 + \cdots + \lambda_k}{\lambda_1 + \lambda_2 + \lambda_3 + \cdots + \lambda_{15}} \quad ; \quad k \text{ se alege astfel încât } q < 99 \quad (9.9)$$

Numărul 0.99 reprezintă un coeficient prin care se exprimă gradul de compactare astfel încât diferenţa între imaginea iniţială şi cea compactată să fie mai mică decât 1%.

a) Obiect de acoperire

b) Obiect steganografic, unde mesajul s-a compactat cu reţinerea a 99% din datele iniţiale

c)
Obiect steganografic, unde mesajul s-a compactat cu reţinerea a 97% din datele iniţiale

d)
Obiect steganografic, unde mesajul s-a compactat cu reţinerea a 95% din datele iniţiale

e)
Obiect steganografic, unde mesajul s-a compactat cu reţinerea a 90% din datele iniţiale

Figura 9.3 Prezentarea obiectului de acoperire si a obiectelor steganografice pentru diferite grade de reţinere a mesajului secret

a) Mesaj secret original

b) Mesaj recuperat, obţinut în urma compactării cu reţinerea a 99% din datele iniţiale

c) Mesaj recuperat obţinut în urma compactării cu reţinerea a 97% din datele iniţiale

d) Mesaj recuperat obţinut în urma compactării cu reţinerea a 95% din datele iniţiale

e) Mesaj recuperat, obţinut în urma compactării cu reţinerea a 90% din datele iniţiale

Figura 9.4 Mesajul original si mesajele recuperate pentru diferite grade de reţinere a mesajului secret

În figura 9.3 şi 9.4 am prezentat un exemplu cu privire la obţinerea obiectului steganografic sau a mesajului recuperat pentru diferite valori ale coeficientului q, atribuindu-i acestuia valorile de 0,99 până la 0,90. Pe baza experimentelor rezultate se constată că în cazul unei valori mai mici pentru q, calitatea mesajului recuperat se degradează vizibil, dar acesta nu este afectat din punctul de vedere al recunoaşterii lui. Apar diferenţe doar în zonele cu suprafeţele mari de aceeaşi culoare. Avantajul unei valori mici pentru q, conduce la posibilitatea creşterii gradului de încorporare. Pe de altă parte, în urma experimentelor efectuate am constatat că între obiectele steganografice nu există diferenţe vizibile. Din acest motiv în continuare am utilizat pentru q valoarea de 0,99. În situaţii extreme în care se doreşte o compactare mai mare, se poate alege un coeficient chiar mai mic pentru q.

În urma experimentelor efectuate, coeficientul k a rezultat a fi cuprins între $1/4$ şi $1/3$ din numărul de linii $m = 15$. În funcţie de blocul de imagine prelucrat se constată că parametrul k este cuprins între valoarea 4 şi maxim 7.

7) Se păstrează primele k coloane ale matricii Q formată din vectorii proprii rezultând astfel o matrice de vectori proprii Q^* de dimensiune m linii şi n coloane. În cazul acestui algoritm $m = 15$.
8) Se calculează transpusa matricei Q^* rezultând matricea $\text{QUOTE } Q^{*T}$ de dimensiuni k linii şi m coloane.
9) Se aplică transformata KLT:

$$Y = \text{QUOTE } Q^{*T} \times M \quad (9.10)$$

Unde, matricea Y este formată din k linii şi n coloane.

Paşii 1.b – 9 se repetă până la comprimarea întregii imagini. Procesarea se poate executa atât secvenţial în cazul existenţei unei singure unităţi de prelucrare, dar şi în paralel în cazul în care procesorul are la dispoziţie mai multe unităţi de procesare.

Ascunderea mesajului secret

10.a) Mărimile Y, Q^*, k se ascund în obiectul de acoperire care este o imagine în format RGB. Ascunderea se realizează în ordinea menţionată, cu precizarea că asupra obiectului de acoperire nu se fac prelucrări în acest caz. Pentru a efectua procesul de ascundere s-a ales utilizarea algoritmului bazat pe încorporarea în cei mai puţini semnificativi biţi, respectiv 1, 2 şi 4 biţi.

Pentru a testa valabilitatea modelelor prezentate în capitolul 6 am efectuat câteva prelucrări atât asupra obiectului de acoperire, cât şi asupra mesajului secret. Menţionez că asupra obiectului de acoperire s-a efectuat o scalare spre negru a fiecărui pixel, respectiv spre alb. Rezultatele prelucrării au fost descrise în capitolul 6. Precizez că astfel de deplasări a fiecărui pixel conduce la constatarea că deplasarea spre negru a imaginii de acoperire conduce la îmbunătăţirea erorii relative dintre obiectul de acoperire şi obiectul steganografic cu o valoare medie de 6%. Asupra mesajului secret înaintea procesului de comprimare am efectuat de asemenea o scalare a fiecărui pixel spre negru, respectiv spre alb, obţinându-se şi în acest caz îmbunătăţiri ale erorii relative dintre mesajul secret iniţial şi cel recuperat, în medie de 16%. În urma compresiei se constată că este posibilă încorporarea unei cantităţi mai mari de informaţii ce poate fi ascunsă fără a pierde din calitatea obiectului steganografic şi a mesajului secret recuperat, deoarece vectorii proprii şi proiecţia au încorporată o cantitate de 99% din imaginea iniţială.

10.b) Întregul algoritm se repetă de atâtea ori până se parcurg toate blocurile matricei mesaj de 5 linii. Dacă matricea mesaj are m linii, numărul de cicluri va fi $\overline{\frac{m}{5}}$.

11) În final se obţine imaginea steganografică, notată cu S care este o imagine în format RGB:

$$S = \begin{bmatrix} s_{1,1} & \cdots & s_{1,m} \\ s_{n,1} & \cdots & s_{n,m} \end{bmatrix} \quad (9.11)$$

Unde $s_{i,j}$ reprezintă pixelul i, j din imaginea steganografică: $i = \overline{1,n}$ si $j = \overline{1,m}$

Extragerea mesajului secret

12) La recepţie din imaginea steganografică S se aplică algoritmul de recuperare invers, prin care se extrag biţii cei mai puţini semnificativi, din care se obţin mărimile: Y - proiecţia matricei iniţiale în noile coordonate, vectorii proprii Q^* şi mărimea k. Precizez că pentru fiecare ciclu mărimea k are valori diferite ce dimensionează matricea de vectori proprii Q^*, care este de dimensiune 15 linii şi k coloane.

13) Se extrage mesajul secret aplicând relaţiile:

$$Y = \text{QUOTE}\ Q^{*T} \times \mathbf{M} \tag{9.12}$$

Relaţia (9.12) se înmulțește cu Q^{*} şi rezultă:

$$Y \times \text{QUOTE}\ Q^{*} = \text{QUOTE}\ Q^{*T} \times Q^{*} \times M = M_R \tag{9.13}$$

Unde: $\text{QUOTE}\ Q^{*T} \times Q^{*} = 1$.

Calitatea mesajului ascuns este calculată în funcţie de eroarea relativă ce constituie diferenţa dintre mesajul iniţial şi mesajul recuperat. În urma testelor efectuate a rezultat că eroarea relativă este cuprinsă între 0,8% şi 4,5%, depinzând atât de tipul imaginii utilizate în procesul steganografic, cât şi de dimensiunea acestora. Eroarea relativă dintre obiectul de acoperire şi obiectul steganografic rezultat în urma ascunderii mesajului secret variază între 0,2% în cazul ascunderii în cel mai puţin semnificativ bit, creşte la 0,5% în cazul ascunderii în ultimii 2 biţi mai puţini semnificativi, până la 2% în situaţia utilizării ultimilor 4 biţi mai puţini semnificativi. În paragraful următor vor fi date câteva exemple în acest sens.

9.2.1.2 *ASAC* - Experimente

În figurile 9.5, 9.6, 9.7, 9.8 sunt arătate câteva exemple de imagini prelucrate cu algoritmul $ASAC$ pe 1 bit.

Obiect de acoperire - C Obiect steganografic - S

Mesajul secret ascuns M Mesajul secret recuperat M_R

Figura 9.5 $ASAC$ pe 1 bit

Mărimea obiectului de acoperire C şi a obiectului steganografic S : 1600 x 1200 x 24 biţi
Mărimea mesajului: 640 x 480 x 24 biţi
Eroarea relativă dintre C şi S : 0.195%
Eroarea relativă dintre mesajul ascuns şi mesajul recuperat: 1.668%
Raport mesaj secret/ obiect de acoperire C : 0.16

Obiect de acoperire - C Obiect steganografic - S

Mesajul secret ascuns M Mesajul secret recuperat M_R

Figura 9.6 ASAC pe 1 bit

.

Mărimea obiectului de acoperire C şi a obiectului steganografic S : 1600 x 1200 x 24 biţi
Mărimea mesajului: 800 x 600 x 24 biţi
Eroarea relativă dintre C şi S : 0.195%
Eroarea relativă dintre mesajul ascuns şi mesajul recuperat: 4.644%
Raport mesaj secret / obiect de acoperire C: 0.25

Obiect de acoperire - C Obiect steganografic - S

Mesajul secret ascuns M Mesajul secret recuperat M_R

Figura 9.7 $ASAC$ pe 1 bit

Mărimea obiectului de acoperire C şi a obiectului steganografic S : 1024 x 1024 x 24 biţi
Mărimea mesajului: 512 x 512x 24 biţi
Eroarea relativă dintre C şi S : 0.195%
Eroarea relativă dintre mesajul ascuns şi mesajul recuperat: 1.421%
Raport mesaj secret / obiect de acoperire C: 0.25

Obiect de acoperire - C Obiect steganografic - S

Mesajul secret ascuns M Mesajul secret recuperat M_R

Figura 9.8 $ASAC$ pe 1 bit

Mărimea obiectului de acoperire C şi a obiectului steganografic S : 1024 x 1024 x 24 biţi
Mărimea mesajului: 640x 480x 24 biţi
Eroarea relativă dintre C şi S : 0.195 %
Eroarea relativă dintre mesajul ascuns şi mesajul recuperat: 0.800%
Raport mesaj secret / obiect de acoperire C : 0.29

Din cele câteva exemple prezentate în figurile anterioare se pot trage câteva concluzii de bază în ceea ce priveşte algoritmul steganografic $ASAC$ pe 1 bit, şi anume: calitatea obiectului steganografic este obţinută cu o eroare extrem de mică (0,195%), ceea ce practic este de nesesizat de către ochiul uman. În acest sens, se poate constata făcând o analiză comparativă dintre obiectul de acoperire şi obiectul steganografic din figura 9.5 că şi unele elemente de detalii practic nu pot fi sesizate (ex. scrisul din dreapta sus), dar nu numai atât, toate elementele de detalii sunt deosebit de clare, ceea ce conferă obiectului steganografic o calitate indiscutabilă. Mai mult, şi eroarea dintre mesajul secret original şi cel recuperat este relativ mică având o medie de1,25, însă existând şi situaţii în care poate scădea chiar sub 1% (ex. figura 9.8). În mare parte timpul de execuţie a acestui algoritm este dependent în mare parte de mărimea obiectului de acoperire, fiind puţin influenţat de mărimea obiectului ce urmează a fi încorporat. O altă observaţie ce trebuie remarcată constă în faptul că timpul de extragere al mesajului secret este aproape la jumătate faţă de timpul de încorporare a lui. Acest lucru poate fi benefic în cazul în care mesajul secret trebuie recuperat într-un timp real. Este cunoscut faptul că încorporarea unui mesaj nu implică o astfel de funcţie.

În figurile 9.9, 9.10, 9.11, 9.12 sunt arătate câteva exemple de imagini prelucrate cu algoritmul ASAC pe 2 biţi.

Obiect de acoperire - C Obiect steganografic - S

Mesajul secret ascuns M Mesajul secret recuperat M_R

Figura 9.9 $ASAC$ pe 2 biţi

Mărimea obiectului de acoperire C şi a obiectului steganografic S : 256 x 256 x 24 biţi
Mărimea mesajului: 128 x 128 x 24 biţi
Eroarea relativă dintre C şi S : 0.545 %
Eroarea relativă dintre mesajul ascuns şi mesajul recuperat: 1.119 %
Raport mesaj secret / obiect de acoperire C : 0.25

Obiect de acoperire - C Obiect steganografic - S

Mesajul secret ascuns M Mesajul secret recuperat M_R

Figura 9.10 ASAC pe 2 biţi

Mărimea obiectului de acoperire C şi a obiectului steganografic S : 1024 x 1024 x 24 biţi
Mărimea mesajului: 800 x 600 x 24 biţi
Eroarea relativă dintre C şi S : 0.526 %
Eroarea relativă dintre mesajul ascuns şi mesajul recuperat: 4.644%
Raport mesaj secret / obiect de acoperire C: 0.45

Obiect de acoperire - C Obiect steganografic - S

Mesajul secret ascuns M Mesajul secret recuperat M_R

Figura 9.11 $ASAC$ pe 2 biţi

Mărimea obiectului de acoperire C şi a obiectului steganografic S : 1600 x 1200 x 24 biţi
Mărimea mesajului: 1024 x 1024 x 24 de biţi
Eroarea relativă dintre C şi S : 0.556 %
Eroarea relativă dintre mesajul ascuns şi mesajul recuperat: 1.038 %
Raport mesaj secret / obiect de acoperire C : 0.54

Obiect de acoperire - C Obiect steganografic - S

Mesajul secret ascuns M Mesajul secret recuperat M_R

Figura 9.12 $ASAC$ pe 2 biţi

Mărimea obiectului de acoperire C şi a obiectului steganografic S : 1600 x 1200 x 24 Mărimea mesajului: 1024 x 1036 x 24 de biţi
Eroarea relativă dintre C şi S : 0.534 %
Eroarea relativă dintre mesajul ascuns şi mesajul recuperat: 1.231%
Raport mesaj secret / obiect de acoperire C : 0.55

În cazul algoritmului $ASAC$ pe 2 biţi, din exemplele prezentate mai sus se poate constata că eroarea dintre obiectul de acoperire şi obiectul steganografic este de asemenea relativ mică (0,5%) şi foarte greu de sesizat de ochiul uman, în schimb spre deosebire de algoritmul $ASAC$ pe 1 bit se dublează cantitatea de

informaţie ce poate fi ascunsă (de la 29% la 55% din mărimea obiectului de acoperire). Pe de altă parte calitatea mesajului recuperat se îmbunătăţeşte în mod vizibil (figura 9.9). Menţionez că imaginile au fost mărite pentru a se constata cu mai multă acurateţe asemănarea dintre mesajul secret ascuns şi cel recuperat.

În figurile 9.13, 9.14, 9.15, 9.16 sunt arătate câteva exemple de imagini prelucrate cu algoritmul ASAC pe 4 biţi.

Obiect de acoperire - C Obiect steganografic - S

Mesajul secret ascuns M Mesajul secret recuperat M_R

Figura 9.13 $ASAC$ pe 4 biţi

Mărimea obiectului de acoperire C şi a obiectului steganografic S : 1600 x 1200 x 24 Mărimea mesajului: 1600 x 1200 x 24 de biţi
Eroarea relativă dintre C şi S : 2.353 %
Eroarea dintre mesajul secret si mesajul recuperat: 1.091 %
Raport mesaj secret / obiect de acoperire C : 1,00

Obiect de acoperire - C Obiect steganografic - S

Mesajul secret ascuns M Mesajul secret recuperat M_R

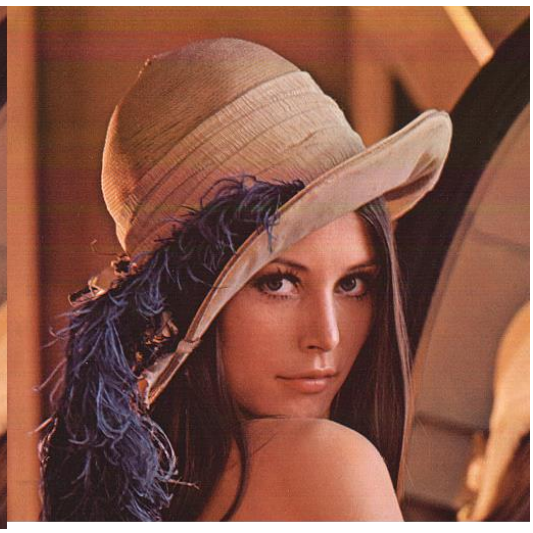
Figura 9.14 $ASAC$ pe 4 biţi

Mărimea obiectului de acoperire C şi a obiectului steganografic: 1024 x 1024 x 24 biţi
Mărimea mesajul: 1024 x 1036 x 24 biţi
Eroarea relativă dintre C şi S : 2.4165 %
Eroarea dintre mesajul secret si mesajul recuperat: 1.71 %
Raport mesaj secret / obiect de acoperire C : 1.01

Obiect de acoperire - C

Obiect steganografic - S

Mesajul secret ascuns M



Mesajul secret recuperat M_R

Figura 9.15 $ASAC$ pe 4 biţi

Mărimea obiectului de acoperire C şi a obiectului steganografic S : 512 x 512 x 24 biţi

Mărimea mesajul: 512 x 512 x 24 biţi

Eroarea relativă dintre C şi S : 2.199 %

Eroarea dintre mesajul secret si mesajul recuperat: 1.686 %

Raport mesaj secret / obiect de acoperire C : 1,00

Obiect de acoperire - C Obiect steganografic - S

Mesajul secret ascuns M Mesajul secret recuperat M_R

Figura 9.16 $ASAC$ pe 4 biţi

Mărimea obiectului de acoperire C şi a obiectului steganografic: 200 x 135 x 24 biţi

Mărimea mesajului secret: 200 x 135 x 24 de biţi

Eroarea relativă dintre C şi S : 2.102 %

Eroarea dintre mesajul secret si mesajul recuperat: 0.778 %

Raport mesaj secret / obiect de acoperire C : 1,00

În cazul utilizării variantei algoritmului $ASAC$ pe 4 biţi se constată o creştere semnificativă a cantităţii de informaţie ce poate fi ascunsă, aceasta ajungând la valoarea de 100% din mărimea obiectului de acoperire, fără pierderea semnificativă din calitatea obiectului steganografic a cărei eroare atinge erori ce nu depăşesc 2,4% comparat cu obiectul de acoperire. În schimb mesajul recuperat este foarte asemănător cu mesajul original, chiar şi în cazul analizării unor detalii. Singurele modificări ce pot apărea sunt cele legate de mici schimbări ale nuanţelor regăsite în fundalul imaginilor dacă acestea sunt de dimensiuni mari.

Cantitatea mare de informaţii ce poate fi ascunsă cu algoritmul creat de mine $ASAC$ pe 1, 2 sau 4 biţi, respectiv de la 29% la 100% din mărimea obiectului de acoperire este superioară cantităţii de informaţii ce poate fi ascunsă de algoritmii

dezvoltaţi în [CHA08] unde raportul de ascundere este cuprins între 6% şi 18% (1,5 biţi per pixel - bpp) în funcţie de imaginea folosită ca obiect de acoperire, respectiv în [CHI08] unde se atinge o cantitate maximă de ascundere de 41,37% (3,31 bpp). Practic, cu algoritmul *ASAC* pe 4 biţi pot ascunde o cantitate de 2,5 ori mai mare, iar calitatea imaginii steganografice din cele câteva exemple prezentate se poate observa că este superioară.

Ceea ce defineşte acest algoritm constă în faptul că înainte de ascundere se realizează o compactare a mesajului fără pierderi semnificative datorită utilizării transformatei KLT, ceea ce rezultă şi din exemplele prezentate mai sus. Totodată această compactare are şi un rol de a îngreuna posibilitatea de extragere a mesajului, în sensul modelului prezentat în capitolul 6 prin care se propune ca pe calea de generare a mesajului steganografic să existe o prelucrare a mesajului de ascundere. Această cerinţă este realizată în algoritmul prezentat.

Având în vedere calitatea algoritmului prezentat în acest capitol mi-am propus ca acesta să fie implementat pe un microprocesor în vederea creşterii vitezei de procesare şi de a micşora timpul de generare a mesajului steganografic, respectiv de scădere a timpului de extragere a mesajului secret. În acest sens, în cadrul algoritmului propus se constată că timpul de extragere e de două ori mai mic decât timpul de încorporare al mesajului. Astfel s-a urmărit că prin implementarea cu ajutorul unui microprocesor performant să atribui algoritmului şi proprietăți de timp real.

În vederea măsurării performanţelor algoritmului *ASAC* am utilizat două platforme de comparare constituite dintr-un calculator personal şi un suport de dezvoltare prevăzut cu un microprocesor ARM. În tabelul 9.1 sunt prezentate câteva exemple mai semnificative dovedind faptul că timpul de execuţie pe microprocesorul ARM scade de cel puţin 4 ori. Această scădere se datorează valorificării superioare a facilităţilor algoritmului pe o astfel de platformă, deoarece este pusă în valoarea întreaga arhitectură a acestuia bazată pe banda de asamblare, a cărei exploatare implică o regândire a întregului algoritm în vederea beneficierii la maxim a acestor proprietăţi.

Tabel 9.1 Compararea timpului de execuţie pentru algoritmul *ASAC*

Nr. Crt.	Obiect de acoperire		Mesaj secret		PC	ARM
	Nume	Dimensiune (bytes)	Nume	Dimensiune (bytes)	[ms]	[ms]
1	camp_cu_flori.jpg	81.000	porumbel.jpg	33.930	124	1243
2	camp_cu_flori.jpg	81.000	ceas_2.jpg	45.450	135	1340
3	camp_cu_flori.jpg	81.000	ceas_3.jpg	81.000	156	1370
4	arthas.jpg	120.000	gryphon.jpg	120.000	204	2040
5	arthas.jpg	120.000	ceas_3.jpg	81.000	187	2097
6	lac_3.jpg	202.500	porumbel.jpg	33.930	254	1283

În figura 9.17 se prezintă sub formă grafică modul cum variază timpul de execuţie al algoritmului *ASAC* pe 4 biţi pe un calculator personal, respectiv pe microprocesorul ARM. Menţionez că algoritmul *ASAC* s-a comportat foarte bine şi pe

simulatorul microprocesorului ISAAC, însă datorită faptului că timpii de execuţie nu sunt reali nu i-am menţionat în tabelul 9.1, respectiv în figura 9.17.

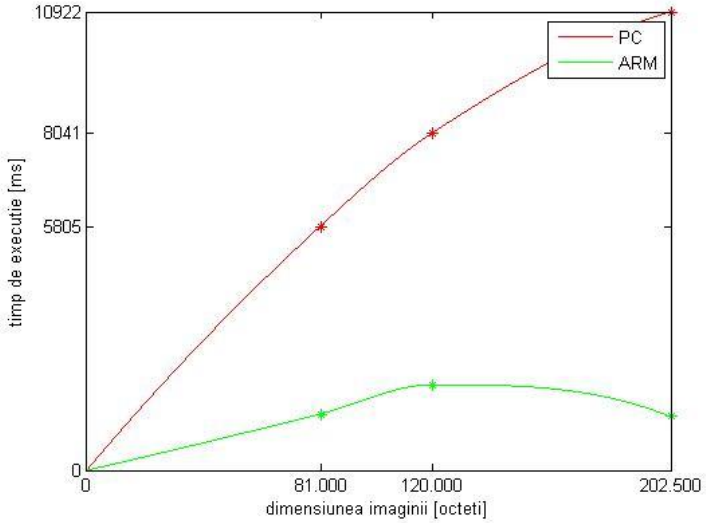


Figura 9.17 Reprezentarea grafică a timpilor de execuţie pentru algoritmul *ASAC*

Din figura 9.17 se poate observa o îmbunătăţire a timpului de execuţie între 4 până la 9 ori, totul depinzând în mare parte de dimensiunea obiectului de acoperire şi mai puţin de dimensiunea mesajului secret. Îmbunătăţirea timpului de execuţie este de aşteptat să fie mai semnificativă în situaţia utilizării unui microprocesor cu mai multe unităţi de prelucrare.

9.2.1.3 ASAC – Concluzii

Teoretic cu algoritmul descris mai sus se poate ascunde în condiţii foarte bune fără degradarea imaginii steganografice o cantitate de informaţii foarte mare ce poate atinge valori de 100% din cantitatea informaţiilor deţinută de obiectul de acoperire. Acest aspect este confirmat de cele câteva exemple prezentate în acest capitol, cât şi de numărul mare de teste efectuate. Din punct de vedere calitativ am constatat faptul că imaginea steganografică este foarte asemănătoare cu imaginea purtătoare, putând atinge diferenţe minime de 0,19 %. Imaginea recuperată prezintă în schimb o diferenţă ce poate atinge valori minime de 0,8 % raportată faţă de mesajul original. Este de specificat că în realizarea unei imagini steganografice de bună calitate, respectiv în obţinerea unui mesaj recuperat foarte asemănător cu cel original un rol important îl joacă tipologia imaginilor alese şi utilizate în algoritm.

Referitor la timpul de execuţie al algoritmului obţinut în urma adaptării pe un microprocesor utilizat în telefonia mobilă se poate observa că acesta prezintă valori relativ mici. Consider că în urma experimentării acestui algoritm pe un microprocesor mult mai performant decât cel utilizat să poată fi realizată şi posibilitatea executării în timp real a acestuia. Astfel, microprocesorul ISAAC prezentat în capitolul 5, a cărui arhitectură se bazează pe existenţa mai multor

nuclee ce pot lucra în paralel poate fi un candidat în acest sens. Trebuie menţionat că algoritmul $ASAC$ a fost astfel conceput încât să permită o procesare în paralel în vederea generării obiectului steganografic prin faptul că mesajul secret este divizat în mai multe blocuri ce pot fi ascunse în mod simultan dacă arhitectura microprocesorului permite acest lucru. Apreciez că timpul de execuţie pe un astfel de microprocesor poate scădea semnificativ.

Ca viitoare cercetare îmi propun implementarea algoritmului $ASAC$ pe noua variantă a microprocesorului ISAAC. Menţionez că în urma rulării algoritmilor steganografici dezvoltaţi în domeniul spaţial, cum ar fi algoritmul bazat pe ascunderea în cei mai puţini semnificativi biţi, respectiv algoritmul bazat pe transformata YUV au fost depistate câteva neconcordanţe de proiectare. Pe lângă acestea compania producătoare a mai adus şi alte modificări impuse de cerinţele beneficiarilor, astfel că în momentul în care cea mai mare parte din problemele sesizate vor fi rezolvate voi putea continua studiului în domeniul steganografiei folosind această nouă variantă a microprocesorului.

9.2.2 Algoritm steganografic pentru ascundere în zgomot – *ASAZ*

Creşterea gradului de robusteţe se poate obţine prin realizarea unor prelucrări suplimentare prin care atacatorului să i se pună o serie de piedici în depistarea mesajului secret, însă toate acestea conduc la scăderea cantităţii de informaţie ce poate fi ascunsă. Bazându-mă pe acest principiu am dezvoltat un algoritm steganografic ce utilizează ca obiect de acoperire imagini color, iar mesajul ascuns îl constituie o imagine binară ce urmează să fie încorporată în zgomotele generate artificial pe obiectul de acoperire. Ideea acestui principiu constă în inducerea în eroare a unui eventual atacator cunoscând faptul că pe canalele de transmisie astfel de zgomote se regăsesc în orice caz. Algoritmul se bazează în mare parte pe transformata KLT şi pe o serie de prelucrări ce au drept scop distragerea atenţiei unui eventual intrus.

9.2.2.1 *ASAZ* – Algoritmul de ascundere

Procesarea obiectului de acoperire

Procesul steganografic urmat în acest algoritm presupune ca o primă etapă prelucrarea obiectului de acoperire, urmată de ascunderea, respectiv extragerea mesajului secret.

1) Imaginea obiectului de acoperire în format RGB e reprezentată printr-o matrice de n linii şi m colane, în care fiecare element al matricei reprezintă un pixel format din elementele RGB :

$$C = \begin{bmatrix} c_{1,1} & \cdots & c_{1,m} \\ c_{n,1} & \cdots & c_{n,m} \end{bmatrix}; \quad c_{i,j} = \left(R_{i,j}, G_{i,j}, B_{i,j}\right) \tag{9.14}$$

2) Se transformă fiecare componentă a matricei C într-o matrice de 1 linie şi $n \times m$ coloane de forma:

$$\begin{aligned} C_R &= [R_{11}, R_{12}, \ldots, R_{1m}, R_{21}, \ldots, R_{nm}] \\ C_G &= [G_{11}, G_{12}, \ldots, G_{1m}, G_{21}, \ldots, G_{nm}] \\ C_B &= [B_{11}, B_{12}, \ldots, B_{1m}, B_{21}, \ldots, B_{nm}] \end{aligned} \tag{9.15}$$

3) Se începe prelucrarea obiectului de acoperire calculând prima dată media celor trei matrice din relaţiile (9.15) cu formulele:

$$M(C_R) = \frac{1}{n*m}\sum_{i,j}^{n,m} R_{ij}$$
$$M(C_G) = \frac{1}{n*m}\sum_{i,j}^{n,m} G_{ij}$$
$$M(C_B) = \frac{1}{n*m}\sum_{i,j}^{n,m} B_{ij} \quad (9.16)$$

4) Se generează o matrice diferenţă dintre matricele C_R, C_G, C_B şi matricele obţinute cu relaţiile (9.16).

$$C^* = \begin{bmatrix} C_R \\ C_G \\ C_B \end{bmatrix} - \begin{bmatrix} M(C_R) & \cdots & M(C_R) \\ M(C_G) & \cdots & M(C_G) \\ M(C_B) & \cdots & M(C_B) \end{bmatrix} = \begin{bmatrix} c^*_{R_{11}} & \cdots & c^*_{R_{nm}} \\ c^*_{G_{11}} & \cdots & c^*_{G_{nm}} \\ c^*_{B_{11}} & \cdots & c^*_{B_{nm}} \end{bmatrix} \quad (9.17)$$

Unde fiecare element al matricei C^* se obţine cu ajutorul relaţiilor:

$$c^*_{R_{i,j}} = c^*_{R_{i,j}} - M(C_R)$$
$$c^*_{G_{i,j}} = c^*_{G_{i,j}} - M(C_G)$$
$$c^*_{B_{i,j}} = c^*_{B_{i,j}} - M(C_B) \quad (9.18)$$

Pentru $i = 1 \ldots n, j = 1 \ldots m$

5) Se generează matricea de covarianţă notată Cov a matricei C^*, rezultând o matrice de 3 linii şi 3 colane:

6) Se determină valorile proprii: $\lambda_1, \lambda_2, \lambda_3$

7) Se determină vectorii proprii ai matricei Cov : $\overrightarrow{v_1}, \overrightarrow{v_2}, \overrightarrow{v_3}$.

8) Se formează matricea Q care are drept linie componentele fiecărui vector propriu: $\overrightarrow{v_1}, \overrightarrow{v_2}, \overrightarrow{v_3}$, unde matricea Q are 3 linii şi 3 coloane.

Aceasta reprezintă exprimarea matricei C a obiectului de ascundere în baza formată de vectorii proprii. Se remarcă la această bază faptul că fiecare dintre cei 3 vectori ai bazei corespund unei valori proprii, iar cu cât valoarea proprie este mai mare cu atât va fi mai mare domeniul în care variază proiecţia "norului" de pixeli (fiecare pixel are 3 coordonate) pe vectorul corespunzător acelei valori proprii. Ceea ce urmăreşte algoritmul este ca ascunderea mesajului să altereze cât mai puţin obiectul de ascundere. Din acest motiv ascunderea se poate face în proiecţia care corespunde valorii proprii minime, această proiecţie fiind cea mai omogenă, în sensul că are cele mai mici abateri de la media sa.

Se ordonează valorile proprii în ordine descrescătoare. În cazul de faţă valoarea proprie cu indicele 3 presupunem ca are valoarea minimă, iar acesteia îi corespunde vectorul propriu $\overrightarrow{v_3}$.

9) Se construieşte matricea Y :

$$Y = Q \times C^* \quad (9.19)$$

În matricea Y se va înlocui a 3-a linie, pe baza comentariilor făcute la punctul (8), cu mesajul secret conform punctului (17) al acestui algoritm.

10) Pe baza transformatei KLT se generează o nouă matrice de o linie şi $n \times m$ coloane notată I_K :

$$I_K = \overrightarrow{v_3} \times C^* \tag{9.20}$$

Prelucrarea mesajului secret

11) Mesajul ce urmează a fi ascuns, notat cu M este o imagine binară ("0" pentru alb şi "1" pentru negru) şi are aceeaşi dimensiune ca şi obiectul de acoperire: n linii şi m coloane:

$$M = \begin{bmatrix} m_{1,1} & \cdots & m_{1,m} \\ \cdot & & \\ m_{n,1} & \cdots & m_{n,m} \end{bmatrix} \text{; unde } m_{i,j} = \{0,1\} \tag{9.21}$$

12) Se formează matricea linie M_L :

$$M_L = [m_{1,1} \dots m_{1,m}, m_{2,1} \dots \dots m_{n,m}] \tag{9.22}$$

13) Din M_L se formează o matrice prin care se înlocuieşte valoarea "0" cu "-1" şi "1" cu "1". În acest fel se doreşte să se introducă un zgomot în care se va ascunde mesajul secret.

$$M^* = [m^*_{1,1}, m^*_{1,2}, \dots m^*_{n,m}] \tag{9.23}$$

Unde fiecare element al matricei se calculează cu formula:

$$m^*_{1,1} = 2m_{i,j} - 1 \tag{9.24}$$

14) Se construieşte matricea P_S ce se generează pseudoaleator, astfel încât modul de generare este cunoscut doar de către emiţător şi receptor. În acest fel, chiar dacă mesajul va putea fi interceptat de către un eventual atacator, acesta nu va putea descifra mesajul fără cunoaşterea modului de generare a matricei P_S .

$$P_S = \begin{bmatrix} s_{1,1} & \cdots & s_{1,m} \\ \cdot & & \\ s_{n,1} & \cdots & s_{n,m} \end{bmatrix} \tag{9.25}$$

Unde $s_{i,j} = \{-1,1\}$ se generează pseudoaleator cu probabilitatea:

$$P(s_{i,j} = 1) = P(s_{i,j} = -1) = \frac{1}{2} \tag{9.26}$$

15) Se construieşte matricea linie W formată din $n \times m$ coloane, ce are rolul de a scunde mesajul în zgomot.

$$W = [w_{1,1} \dots w_{1,m}, w_{2,1} \dots \dots w_{n,m}] \tag{9.27}$$

Unde fiecare element se obţine ca un produs de 2 termeni, astfel:

$$w_{i,j} = s_{i,j} \times m^*_{i,j} \text{ ; pentru } i = \overline{1,n} \text{ si } j = \overline{1,m} \tag{9.28}$$

Dacă se notează:

$$P(m^*_{i,j} = 1) = \beta \tag{9.29}$$

Rezultă în acest caz că:

$$P(w_{i,j} = 1) = P(s_{i,j} * m_{i,j} = 1) = P((s_{i,j} = 1, m_{i,j} = 1) \cup (s_{i,j} = -1, m_{i,j} = -1)) = P(s_{i,j} = 1, m_{i,j} = \tag{9.30}$$

La fel şi:

$$P(w_{i,j} = -1) = \frac{1}{2} \tag{9.31}$$

16) Pe baza matricei corespunzătoare imaginii I_K şi a matricei W se generează o nouă matrice linie de forma:

$$I_W = I_K + \alpha w \tag{9.32}$$

Unde $\alpha = \overline{1,10}$.

În această etapă se încorporează mesajul secret cu zgomot în linia vector propriu corespunzător celor mai mici valori proprii.

Coeficientul α s-a luat prin încercări pentru a permite creşterea calităţii imaginii steganografice obţinute. Pentru $\alpha = 1$ rezultă o calitate mai bună, iar pentru $\alpha = 10$ se obţine o calitate mai slabă atât a imaginii steganografice, precum şi a mesajului recuperat. Valoarea lui $\alpha = 1$ se va alege în funcţie de tipul imaginii digitale, a obiectului de acoperire. Cea mai bună valoare pentru o gamă mare de imagini este $\alpha = 4$.

Ascunderea mesajului secret

17) În matricea Y obţinută la punctul (9) se înlocuieşte a 3-a linie cu I_W şi se obţine matricea Z care are 3 linii si $n \times m$ coloane.

18) Se generează imaginea steganografică exprimată intermediar sub forma unei matrice de 3 linii şi $n \times m$ coloane şi se consideră în continuare ca fiind imagine steganografică linie:

$$I_{S_1} = Q^T * Z + \begin{bmatrix} M(C_R) & \cdots & M(C_R) \\ M(C_G) & \cdots & M(C_G) \\ M(C_B) & \cdots & M(C_B) \end{bmatrix} \tag{9.33}$$

Unde matricea Q^T are 3 linii şi 3 coloane, matricea Z este de 3 linii şi $n \times m$ coloane, iar matricea mediilor este de 3 linii şi $n \times m$ coloane. Rezultă că matricea I_{S_1} este de 3 linii şi $n \times m$ coloane şi este de forma:

$$I_{S_1} = \begin{bmatrix} s1^R_{1,1} & \cdots & s1^R_{1,n}, s1^R_{2,1} & \cdots & s1^R_{n,m} \\ s1^G_{1,1} & \cdots & s1^G_{1,n}, s1^G_{2,1} & \cdots & s1^G_{n,m} \\ s1^B_{1,1} & \cdots & s1^B_{1,n}, s1^B_{2,1} & \cdots & s1^B_{n,m} \end{bmatrix} \tag{9.34}$$

19) Pe baza matricei I_{S_1} se obţine imaginea steganografică S care este de forma RGB:

$$S = \begin{bmatrix} s_{1,1} & \cdots & s_{1,m} \\ \cdot & & \\ s_{n,1} & \cdots & s_{n,m} \end{bmatrix} \tag{9.35}$$

Unde $s_{i,j} = \left(s1^R_{i,j}, s1^G_{i,j}, s1^B_{i,j}\right)$ reprezintă pixelul i,j din imaginea steganografică: pentru $i = \overline{1,n}$ si $j = \overline{1,m}$.

20) Obiectul steganografic S exprimat sub forma unei imagini RGB se trimite în continuare pe canalele de transmisie.

9.2.2.2 *ASAZ*– Algoritmul de extragere

1) Se recepţionează imaginea steganografică S , exprimată în relaţia (9.35).
2) Se transformă matricea S în trei matrice linie de $n \times m$ coloane, una pentru fiecare componentă RGB, sub următoarea formă:

$$\begin{aligned} S_R &= [R_{11}, R_{12}, \dots, R_{1m}, R_{21}, \dots, R_{nm}] \\ S_G &= [G_{11}, G_{12}, \dots, G_{1m}, G_{21}, \dots, G_{nm}] \\ S_B &= [B_{11}, B_{12}, \dots, B_{1m}, B_{21}, \dots, B_{nm}] \end{aligned} \tag{9.36}$$

3) Se calculează media elementelor celor 3 matrice linie:

$$M(S_R) = \frac{1}{n*m}\sum_{i,j}^{n,m} R_{ij}, \quad M(S_G) = \frac{1}{n*m}\sum_{i,j}^{n,m} G_{ij}, \quad M(S_B) = \frac{1}{n*m}\sum_{i,j}^{n,m} B_{ij} \tag{9.37}$$

unde: $i = \overline{1,n}$ şi $j = \overline{1,m}$

4) Se calculează o matrice diferenţă dintre matricele S_R, S_G, S_B şi media obţinută cu relaţia (9.37) pentru fiecare culoare şi se obţine o matrice S^* formată din 3 linii şi $n \times m$ coloane:

$$S^* = \begin{bmatrix} S_R \\ S_G \\ S_B \end{bmatrix} - \begin{bmatrix} M(S_R) & \cdots & M(S_R) \\ M(S_G) & \cdots & M(S_G) \\ M(S_B) & \cdots & M(S_B) \end{bmatrix} \tag{9.38}$$

5) Se generează matricea de covarianţă a matricei S^*, formată din 3 linii şi 3 coloane, cu relaţia:

$$Cov(S^*) = S^* \times S^{*T} \tag{9.39}$$

6) Se determină valorile proprii şi vectorii proprii corespunzători matricei $Cov(S^*)$:

$\lambda_1, \lambda_2, \lambda_3$ si $\overrightarrow{v_1}, \overrightarrow{v_2}, \overrightarrow{v_3}$

Valorile proprii sunt ordonate descrescător, iar vectorul propriu corespunzător valorii proprii cu valoarea cea mai mică corespunde proiecţiei mesajului ascuns, ce urmează a fi extras. Fie acest vector $\overrightarrow{v_3}$

7) Se aplică transformata KLT asupra imaginii steganografice S^* şi a vectorului propriu $\overrightarrow{v_3}$ (exprimat pe linie).

$$K = \overrightarrow{v_3} * S^* \tag{9.40}$$

Rezultă în acest mod o matrice transformată sub următoarea formă:

$$K = \begin{bmatrix} k_{1,1} & \cdots & k_{1,m} \\ & & \\ k_{n,1} & \cdots & k_{n,m} \end{bmatrix} \tag{9.41}$$

8) Pentru a asigura o anumită corelaţie între valori, se aplică o funcţie de uniformizare ce are ca rezultat următoarea matrice de uniformizare K_S a matricii K:

$$K_S = \begin{bmatrix} k_{s\,1,1} & \cdots & k_{s\,1,m} \\ k_{s\,n,1} & \cdots & k_{s\,n,m} \end{bmatrix} \quad (9.42)$$

Unde termenii k_s se obţin cu relaţiile:

$$k_{s_{i,j}} = \left(k_{i-1,j-1} + k_{i-1,j} + k_{i-1,j+1} + k_{i,j-1} + k_{i,j} + k_{i,j+1} + k_{i+1,j-1} + k_{i+1,j} + k_{i+1,j+1}\right)$$

Pentru $i = \overline{2, n-1}$ şi $j = \overline{2, m}$;

$k_{s_{i,j}} = k_{i,j}$ pentru $i = 1$ si $j = \overline{1, m}$;

$k_{s_{i,j}} = k_{i,j}$ pentru $j = 1$ si $j = \overline{1, m}$;

$k_{s_{i,j}} = k_{i,j}$ pentru $j = m$ si $i = \overline{1, n}$;

$k_{s_{i,j}} = k_{i,j}$ pentru $i = n$ si $j = \overline{1, m}$; (9.43)

9) Se calculează matricea diferenţă D dintre matricea K şi matricea K_S rezultând o imagine diferenţă de forma:

$$D = K - K_S,$$

sau:

$$D = \begin{bmatrix} d_{1,1} & \cdots & d_{1,m} \\ \cdot & & \\ d_{n,1} & \cdots & d_{n,m} \end{bmatrix}; \text{ unde: } d_{i,j} = d_{i,j} - k_{s_{i,j}} \quad (9.44)$$

Prin diferenţă se recuperează practic mesajul şi zgomotul introdus.

10) Se generează matricea P_S într-un mod pseudoaleator fiind identică cu cea generată la emisie.

$$P_S = \begin{bmatrix} s_{1,1} & \cdots & s_{1,m} \\ \cdot & & \\ s_{n,1} & \cdots & s_{n,m} \end{bmatrix}; \text{ unde: } s_{i,j} \in \{-1,1\} \quad (9.45)$$

11) Cu ajutorul matricei diferenţă D şi a matricei pseudoaleatoare P_S se obţine mesajul secret recuperat M_R în format RGB de dimensiune n linii şi m coloane:

$$M_R = \begin{bmatrix} m_{r\,1,1} & \cdots & m_{r\,1,m} \\ m_{r\,n,1} & \cdots & m_{r\,n,m} \end{bmatrix} ; \text{ unde : } m_{r\,i,j} = s_{i,j} * d_{i,j} \quad (9.46)$$

În acest pas se elimină zgomotul şi se recuperează mesajul.

9.2.2.3 *ASAZ*– Experimente

Este de consemnat faptul că mesajul extras la recepţie este de bună calitate în special pentru imagini purtătoare de dimensiuni mari. În acest fel diferenţele existente sunt nesemnificative faţă de mesajul ascuns iniţial de către emiţător. Conform modelului prezentat în capitolul 6 în vederea creşterii siguranţei sistemului steganografic s-a propus şi aplicat o funcţie de procesare f_m asupra mesajului original.

Funcţia de procesare constă în introducerea unor zgomote în mesajul secret ce urmează a fi ascuns. Acestea sunt obţinute cu ajutorul unui generator pseudoaleator. În cazul unei eventuale interceptări, atacatorul ar trebui să aibă cunoştinţe atât despre algoritmul de ascundere steganografic, cât şi despre modelul de procesare aplicat la prelucrarea realizării obiectului de acoperire. Probabilitatea ca un atacator să reuşească obţinerea unor astfel de informaţii este foarte mică, ceea ce duce în mod evident la îmbunătăţirea siguranţei sistemului steganografic şi confirmă propunerea făcută pentru modelul steganografic amintit.

În continuare vor fi prezentate câteva experimente şi rezultatele obţinute. În primele două figuri 9.18 şi 9.19 s-a adoptat pentru parametrul α valori mari constatându-se că între obiectul de acoperire şi obiectul steganografic sunt diferenţe nesemnificative, eventualele diferenţe apar în zonele ce conţin culori unice, iar pentru o mai bună analiză obiectul de acoperire şi obiectul steganografic au fost mărite. Pe de altă parte se constată că recuperarea mesajului nu se face în condiţii bune.

Se poate remarca în experimentele prezentate în figurile 9.20, 9.21, 9.22 că prin metoda propusă de mine, mesajul secret ascuns este recuperat la recepţie într-o formă apropiată de cea originală pentru cazul în care $\alpha = 4$, iar eroarea mesajului recuperat se îmbunătăţeşte vizibil pe măsură ce mărimea obiectului de acoperire este mai mare.

Toate experimentele prezentate dovedesc că obiectul steganografic nu diferă semnificativ de obiectul de acoperire, ceea ce în mod evident nu va trezi suspiciuni unui eventual atacator.

Obiect de acoperire - C

Obiect steganografic - S

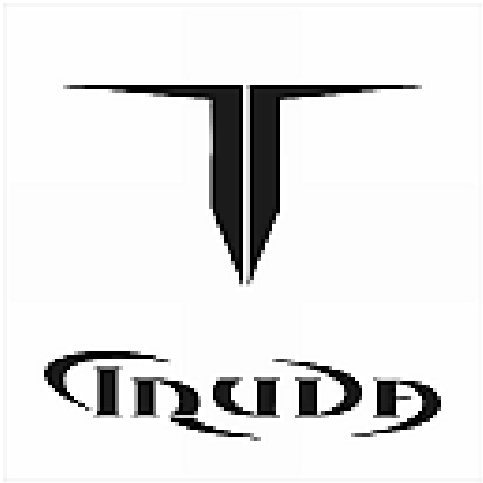
Mesajul secret ascuns M Mesajul secret recuperat M_R

Figura 9.18 ASAZ Ascundere şi recuperare mesaj

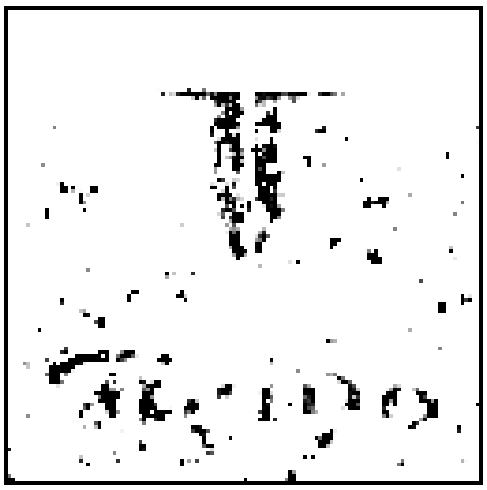
Mărimea obiectului de acoperire C şi a obiectului steganografic S : 64 x 64 x 24 biţi
Mărimea mesajului: 64 x 64 x 1 bit (imagine binară)
Eroarea relativă dintre C şi S : 4.3%
Eroarea relativă dintre mesajul ascuns şi mesajul recuperat: 76.5%
$\alpha = 16.0$

Obiect de acoperire - C

Obiect steganografic - S



Mesajul secret ascuns M



Mesajul secret recuperat M_R

Figura 9.19 ASAZ Ascundere şi recuperare mesaj

Mărimea obiectului de acoperire C şi a obiectului steganografic S : 128 x 128 x 24 biţi

Mărimea mesajului: 128 x 128 x 1 bit (imagine binară)

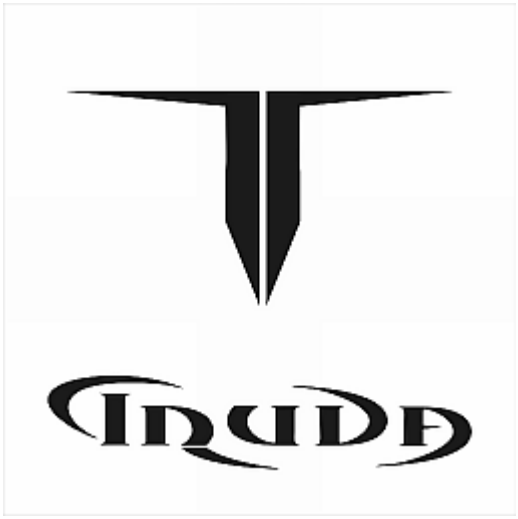
Eroarea relativă dintre C şi S : 2.28%

Eroarea relativă dintre mesajul ascuns şi mesajul recuperat : 44.56%

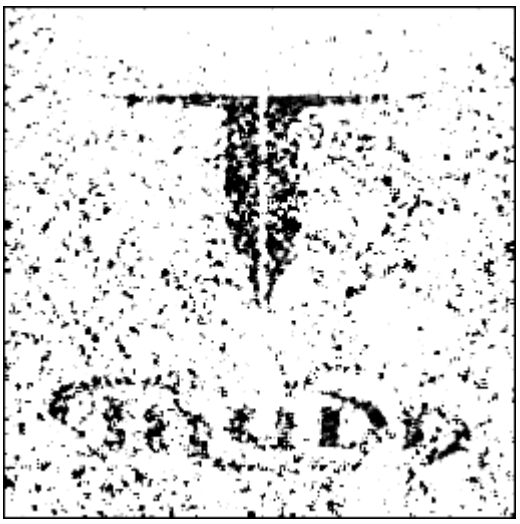
$\alpha = 8.0$

Obiect de acoperire - C

Obiect steganografic - S



Mesajul secret ascuns M



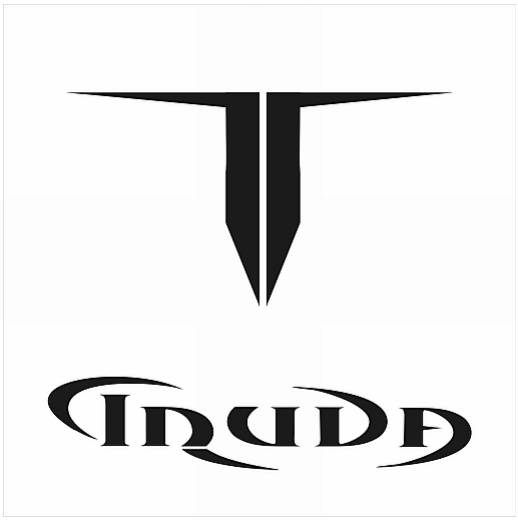
Mesajul secret recuperat M_R

Figura 9.20 ASAZ Ascundere şi recuperare mesaj

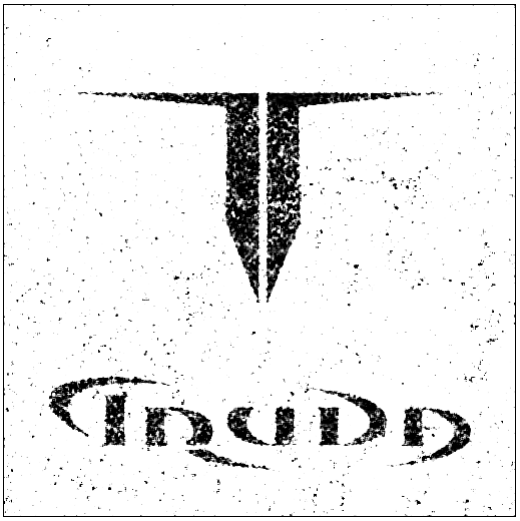
Mărimea obiectului de acoperire C şi a obiectului steganografic S : 256 x 256 x 24 biţi
Mărimea mesajului: 256 x 256 x 1 bit (imagine binară)
Eroarea relativă dintre C şi S : 0.88%
Eroarea relativă dintre mesajul ascuns şi mesajul recuperat: 7.41%
$\alpha = 4.0$

Obiect de acoperire - C

Obiect steganografic - S



Mesajul secret ascuns M



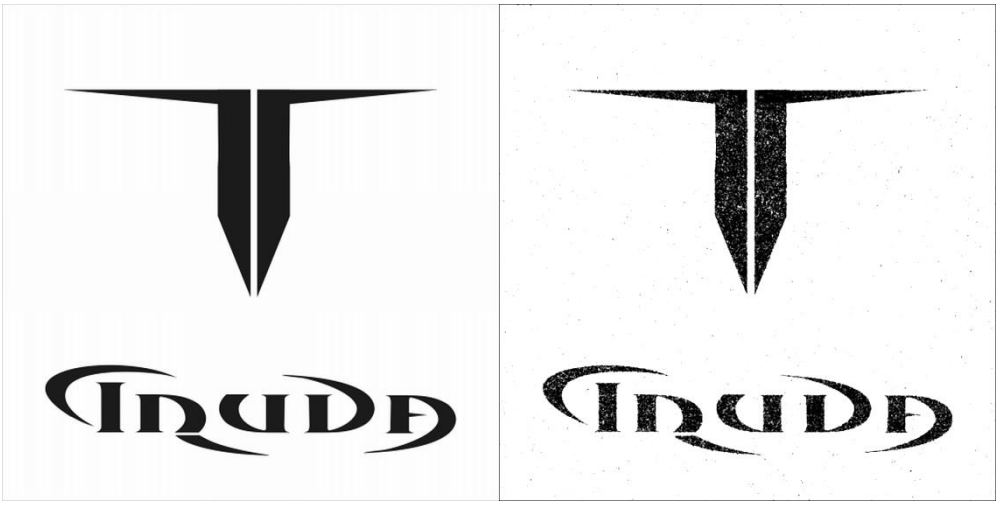
Mesajul secret recuperat M_R

Figura 9.21 ASAZ Ascundere şi recuperare mesaj

Mărimea obiectului de acoperire C şi a obiectului steganografic S : 512 x 512 x 24 biţi
Mărimea mesajului: 512 x 512 x 1 bit (imagine binară)
Eroarea relativă dintre C şi S : 0.88%
Eroarea relativă dintre mesajul ascuns şi mesajul recuperat: 1.8%
$\alpha = 4.0$

Obiect de acoperire - C

Obiect steganografic - S



Mesajul secret ascuns M Mesajul secret recuperat M_R

Figura 9.22 ASAZ Ascundere şi recuperare mesaj

Mărimea obiectului de acoperire C şi a obiectului steganografic S : 1024 x 1024 x 24 biţi
Mărimea mesajului: 1024 x 1024 x 1 bit (imagine binară)
Eroarea relativă dintre C şi S: 0.89%
Eroarea relativă dintre mesajul ascuns şi mesajul recuperat: 0.88%
$\alpha = 4.0$

9.2.2.4 ASAZ- Concluzii

Teoretic cu algoritmul ASAZ descris mai sus se pot ascunde în condiţii foarte bune de securitate fără degradarea imaginii steganografice o cantitate relativ mică de informaţii egală cu 1 bpp din cantitatea de informaţii corespunzătoare obiectului de acoperire.

La prima vedere acest algoritm are o capacitate mai mică de ascundere decât algoritmul $ASAC$, însă prezintă un alt avantaj şi anume faptul că datorită modului de ascundere a mesajului în semnalele de zgomot, îl face foarte greu de depistat de un eventual atacator, ceea ce îi conferă acestuia o robusteţe mare.

Procesarea efectuată asupra obiectului de acoperire generează un obiect steganografic de foarte bună calitate aşa cum se constată în figurile prezentate în acest subcapitol, cât şi din faptul că eroarea relativă dintre obiectul de acoperire şi obiectul steganografic este extrem de bună, respectiv 0,8%.

Alegerea corespunzătoare a parametrului α ce poate fi ales în funcţie de tipul imaginii digitale permite obţinerea unei recuperări în condiţii foarte bune a mesajului ascuns. În acest sens eroarea relativă dintre mesajul ascuns şi mesajul recuperat poate scădea sub 1%. Mai mult, fiind un algoritm vectorial probabilitatea ca imaginea ascunsă să fie degradată de un eventual atacator este mai mică.

Algoritmul ASAZ dezvoltat de mine valorifică în condiţii foarte bune transmiterea unor mesaje secrete exprimate sub formă de imagini binare. Algoritmul poate fi util totodată şi în telefonia mobilă în vederea ascunderii unor mesaje text într-o imagine digitală color. Consider că acest algoritm prezintă calităţi deosebite în ceea ce priveşte recuperarea mesajului de către un eventual atacator, deoarece acesta este inclus într-un semnal de zgomot folosind o metodă pseudoaleatoare cunoscută doar de emiţător şi receptor. În acest fel chiar dacă mesajul ar putea fi interceptat de către un eventual atacator, el nu va putea fi şi descifrat de către acesta. Adăugând faptul că şi obiectul de acoperire prezintă câteva prelucrări şi transformări este greu de presupus că astfel de procesări vor putea fi cunoscute de cei ce nu deţin în detaliu modalitatea de desfăşurare a algoritmului, ceea ce îngreunează şi mai mult tentativa de descifrare a informaţiei ascunse.

Algoritmul ASAZ constituie un bun exemplu de validare a modelului propus în capitolul 6 rezultând în felul acesta un sistem steganografic sigur cu generarea unui obiect steganografic de o calitate foarte bună şi cu posibilitatea de recuperare a mesajului secret cu eroare foarte mică.

În concluzie consider că acest algoritm este deosebit de util şi în watermarking pentru protecţia dreptului de autor, respectiv a semnăturilor digitale. Ca şi cercetare viitoare îmi propun să adaptez acest algoritm pentru a fi rulat pe unul sau mai multe microsisteme cu arhitecturi diferite în vederea îmbunătăţirii timpului de execuţie.

Algoritm steganografic pentru ascundere prin codarea mesajului secret $ASAC_{MS}$

Algoritmul steganografic bazat pe ascunderea mesajului secret prin codarea acestuia constă în prelucrarea atât a obiectului de acoperire cu ajutorul transformatei KLT, cât şi a mesajului secret prin distribuirea acestuia în mod pseudoaleator folosind generatorul Mersenne-Twister [MAK98]. De menţionat că rata de repetiţie a şirului pseudoaleator obţinut pe baza generatorului menţionat este de 2^{19937}-1. Scopul utilizării distribuirii mesajului în obiectul de acoperire folosind şirul pseudoaleator constă în faptul că se pot obţine două avantaje majore. Un prim avantaj ar consta în faptul că recuperarea mesajului secret de către un atacator este imposibil de realizat în lipsa cunoaşterii cifrei de plecare a şirului, ce poate fi considerată ca şi o cheie secretă. Al doilea avantaj constă în faptul că pixelii alăturaţi ai mesajului secret nu mai sunt încorporaţi succesiv, ceea ce conduce la obţinerea unei imagini steganografice mai puţin distorsionate din punct de vedere al percepţiei umane.

9.2.2.5 *$ASAC_{MS}$* - Algoritm de ascundere

Prelucrarea obiectului de acoperire

Paşii 1- 7 parcurşi se referă la prelucrarea obiectului de acoperire şi sunt identici ca la algoritmul de ascundere ASAZ .

8) Se formează matricea Q care are drept linii vectorii proprii obţinuţi anterior.
9) Cu ajutorul matricei Q şi a imaginii de acoperire, folosind transformata KLT se construieşte matricea imagine notată cu I_K :

$$I_K = Q^T \times C^* \tag{9.47}$$

Matricea I_K este formată din 3 linii şi $n \times m$ coloane şi reprezintă exprimarea imaginii RGB în baza formată de vectorii proprii. Este de remarcat faptul că fiecare din cei 3 vectori ai bazei, corespunde unei valori proprii, iar cu cât această valoare proprie este mai mare, cu atât va fi mai mare domeniul în care variază proiecţia pixelilor (fiecare pixel are 3 coordonate date de o coloană din matricea C^* pe vectorul corespunzător acelei valori).

Algoritmul urmăreşte ca la ascunderea mesajului, acesta să altereze cât mai puţin obiectul de acoperire, din acest motiv ascunderea se va face în proiecţia care corespunde valorii proprii minime. Această proiecţie este considerată cea mai omogenă în sensul că are cele mai mici abateri faţă de media sa. Se notează indicele valorii proprii cu valoarea cea mai mică, ind .

10) Se află domeniul între care variază coordonatele proiecţiei pe vectorul propriu minim, notat la punctul 9) cu ind . În continuare voi numi acest domeniu ca $domeniu\ de\ acoperire$. Pentru simplitate considerăm acest domeniu ca fiind ultima linie a matricei I_K. Precizez că domeniul de acoperire poate fi orice linie a matricei menţionate depinzând de valoarea proprie minimă calculată anterior.

Prelucrarea mesajului secret

11) Mesajul secret reprezentat printr-o matrice M are ca elemente valorile pixelilor alb – negru cuprinse între (0,..,255). În continuare matricea M se transformă dintr-o matrice de n linii şi m coloane într-o matrice linie M^* de dimensiune $n \times m$ coloane, ca în relaţiile ce urmează:

$$M = \begin{bmatrix} m_{1,1} & \cdots & m_{1,m} \\ \cdot & & \\ m_{n,1} & \cdots & m_{n,m} \end{bmatrix} \tag{9.48}$$

$$M^* = [m_{1,1}, m_{1,2}, \ldots, m_{1,m}, m_{2,1}, \ldots, m_{n,m}] \tag{9.49}$$

12) Folosind generatorul Mersenne-Twister ce furnizează numere aleatoare, se va construi un şir pseudoaleator cu valori cuprinse între 1 şi $n \times m$ (inclusiv) având $n \times m$ elemente. Numărul de plecare al acestui şir reprezintă o cheie de criptare care va permite reconstituirea acestui şir la extragerea mesajului, şi este cunoscut atât de emiţător cât şi de receptor.

13) În urma acestei prelucrări, matricea M^* se transformă într-o altă matrice codificată, pe care am notat-o cu S_C.

$$S_C = [s_{c_1}, s_{c_2}, \ldots, s_{c_{n \times m}}]; \tag{9.50}$$

14) Din fiecare element al matricei mesaj criptat S_C se scade media elementelor matricei S_C notată med , obţinându-se o nouă matrice S_m : $S_m = [s_{m_1}, s_{m_2}, \ldots, s_{m_{n \times m}}]$; unde $s_{m_i} = s_{m_i} - med$ (9.51)

Media elementelor matricei S_C se obţine cu relaţia:

$$med = \frac{1}{n \times m} \sum_{i}^{n \times m} S_{c_i} \tag{9.52}$$

15) Se scalează S_m în domeniul dat de $domeniu - acoperire$ şi se obţine S_f. Scalarea se face cu media termenilor vectorilor ce urmează a fi ascunşi.
16) În continuare se trece la ascunderea mesajului astfel prelucrat, iar pentru aceasta s-au încercat două variante, fiecare cu propriile avantaje şi dezavantaje:

Metoda de ascundere ASAC$_{MS}$-A$_1$

a) Se înlocuieşte în matricea I_K din relaţia (9.47), linia corespunzătoare indicelui valorii proprii ind cu S_f înmulţit cu un coeficient subunitar, notat $coef$. Cu cât acest coeficient este mai aproape de valoarea "1", cu atât mesajul va fi recuperat mai bine, iar cu cât acesta e mai aproape de "0", cu atât imaginea steganografică seamănă mai mult cu imaginea obiectului de acoperire original. Ca urmare, coeficientul se adaptează la caracteristicile imaginilor folosite. Algoritmul de extragere este independent de acest coeficient.

$$S_f^* = S_f \times coef \tag{9.53}$$

Dacă matricea I_K are forma:

$$I_K = \begin{bmatrix} k_{\mathbf{1}_{1,1}} & k_{\mathbf{1}_{1,m}} & k_{\mathbf{1}_{n,m}} \\ k_{\mathbf{2}_{1,1}} \cdots & k_{\mathbf{2}_{1,m}} \cdots & k_{\mathbf{2}_{n,m}} \\ k_{\mathbf{3}_{1,1}} & k_{\mathbf{3}_{1,m}} & k_{\mathbf{3}_{n,m}} \end{bmatrix} \tag{9.54}$$

Şi dacă se presupune că indicele $ind = \mathbf{3}$, prin înlocuirea liniei ind cu S_f^* rezultă o nouă matrice I_{K_1} din 3 linii şi $n \times m$ coloane, de forma:

$$I_{K_1} = \begin{bmatrix} k_{\mathbf{1}_{1,1}} & \cdots & k_{\mathbf{1}_{n,m}} \\ k_{\mathbf{2}_{1,1}} & \cdots & k_{\mathbf{2}_{n,m}} \\ s_{f_1}^* & & s_{f_{n \times m}}^* \end{bmatrix} \tag{9.55}$$

Metoda de ascundere ASAC$_{MS}$-A$_2$

b) Se calculează matricea linie S_f^* cu relaţia:

$$S_f^* = coef \times S_f + (1 - coef) \times \mathbf{linia}\ ind\ \mathbf{a\ matricii}\ I_K \tag{9.56}$$

Şi din nou se formează matricea I_{K_1}.

În metoda de ascundere a algoritmului $\mathbf{ASAC_{MS}} - A_1$ mesajul este încorporat ca atare. Prin această metodă este posibil ca imaginea steganografică să fie afectată

într-o proporţie mai mare. În schimb, la extragere mesajul recuperat este mai asemănător cu mesajul ascuns iniţial.

În metoda de ascundere a algoritmului $\mathbf{ASAC_{MS}}$ - A_2 ascunderea mesajului se face doar într-o anumită proporţie exprimată prin coeficientul ales, combinat cu imaginea de acoperire. Această variantă are avantajul că oferă o imagine steganografică mult mai apropiată de obiectul de acoperire, în special dacă se ia un coeficient cu valoare mică. Dezavantajul acestei metode constă în faptul că poate duce la o distorsionare mai mare a mesajului extras.

17) Se exprimă matricea I_{K_1} dinnou în baza RGB, rezultând imaginea steganografică sub forma unei matrice linie notată I_{S_1} construită după relaţia:

$$I_{S_1} = I_{K_1} \times Q \tag{9.57}$$

Matricea I_{S_1} este o matrice cu 3 linii si $n \times m$ coloane.

18) La matricea I_{S_1} se adună la fiecare coloană media, notată cu med şi se obţine astfel o matrice asemănătoare cu cea din relaţia (9.34)

19) Se redimensionează matricea linie I_{S_1} într-o matrice ce are dimensiunea de n linii şi m coloane şi 3 culori de bază R, G, B. Aceasta reprezintă de fapt imaginea steganografică S (9.35) ce urmează a fi transmisă unui receptor.

9.2.2.6 $\mathbf{ASAC_{MS}}$-$\mathbf{E_1}$ Algoritm de extragere

Acest algoritm de extragere a mesajului ascuns foloseşte doar imaginea steganografică transmisă receptorului.

Paşii algoritmului:

1) Pornind de la imaginea steganografică S se formează o matrice care are pe fiecare linie elementele unei culori. Aceasta va avea 3 linii şi $n \times m$ coloane, având pe linii reprezentate proiecţiile imaginii RGB.

$$I_{S_1} = \begin{bmatrix} R_{1,1} & \dots & R_{1,m}, R_{2,1} & \dots & R_{n,m} \\ G_{1,1} & \dots & G_{1,m}, G_{2,1} & \dots & G_{n,m} \\ B_{1,1} & \dots & B_{1,m}, B_{2,1} & \dots & B_{n,m} \end{bmatrix} \tag{9.58}$$

2) Se calculează media pe fiecare linie şi se scade din fiecare element al liniei corespunzătoare matricei I_{S_1}, rezultând astfel o nouă matrice $I_{S_1}^*$ ce are aceeaşi dimensiune ca I_{S_1}.

3) Se determină matricea de covarianţă:

$$Cov = I_{S_1}^* \times I_{S_1}^{*T} \tag{9.59}$$

Unde $I_{S_1}^{*T}$ este transpusa matricii $I_{S_1}^*$. Matricea Cov rezultată va avea dimensiunea de 3 linii şi 3 coloane.

4) Se determină vectorii proprii $\overrightarrow{v_1}, \overrightarrow{v_2}, \overrightarrow{v_3}$ şi valorile proprii $\lambda_1, \lambda_2, \lambda_3$ ale matricei de covarianţă.

5) Se formează matricea P care are drept coloane vectorii proprii obţinuţi la pasul 4. Matricea P va avea 3 linii şi 3 coloane.

6) Aplicând transformata KLT se construieşte matricea K, după formula:

$$K = P^T \times I_{S_1}^{\bullet} \quad (9.60)$$

Matricea rezultată reprezintă matricea imaginii steganografice în baza dată de vectorii proprii.

7) Având în vedere că ascunderea mesajului secret s-a făcut în proiecţia care corespundea valorii proprii minime a matricei de covarianţă a imaginii de acoperire, şi ţinând cont că a fost scalat mesajul în domeniul său de variaţie, ca şi proiecţia în care s-a făcut ascunderea, rezultă în mod evident că obiectul de acoperire se încadrează în acelaşi domeniu ca şi obiectul steganografic. Fiecare pixel din imaginea gazdă, de acoperire, respectiv din imaginea steganografică are trei coordonate RGB care pot fi privite drept coordonatele unui punct intr-un reper ortogonal din spaţiu, astfel încât totalitatea pixelilor poate forma un aşa-zis "nor de puncte". Rezultă că direcţia de variaţie minimă a norului de puncte (ce corespunde imaginii steganografice) va fi aproximativ egală cu direcţia de variaţie minimă a norului iniţial. Prin urmare şi proiecţia pe această direcţie va aproxima vectorul ascuns în obiectul de acoperire. Dacă direcţiile sunt aceleaşi, mesajul extras va fi mai aproape de mesajul ascuns. În acest sens se caută valoarea proprie minimă din cel determinat la punctul 4 şi se notează cu un indice, ind .
8) Din matricea K se extrage linia ce corespunde indicelui ind , iar acesta este vectorul care este ascuns în mesajul secret. Operaţia este inversa punctului 16 din algoritmul de ascundere $ASAC_{MS}$.
9) Se scalează această matrice liniară, ce are o linie şi $n \times m$ coloane, între 0 şi 255 pentru obţinerea contrastului maxim şi se generează matricea linie A_1. Scalarea se face cu media termenilor vectorului extras. Prin scalare nu trebuie să se depăşească valoarea 255.
10) Se generează un şir pseudoaleator de numere întregi cuprinse între 1 şi $n \times m$ identic ca la algoritmul de ascundere, punctul 12. De asemenea se utilizează aceleaşi cifre de plecare cu rol de cheie de codare, iar şirul este generat cu algoritmul Mersenne-Twister [MAK98].
11) Se permută pe rând în cadrul matricei A_1 elementul din fiecare poziţie (începând cu ultimul) cu un alt element din A_1 având indicele dat de valoarea elementului din şirul pseudoaleator aflat pe aceeaşi poziţie cu elementul permutat. Se obţine un nouă matrice A_f .
12) Se aranjează elementele matricei liniare A_f într-o matrice de dimensiunea n linii şi m coloane şi se obţine matricea mesajului extras în forma finală M_R în format RGB.

Algoritmul de extragere $ASAC_{MS} - E_1$ are ca avantaj faptul că la extragerea mesajului utilizează doar imaginea steganografică.

Ca dezavantaj îl constituie faptul că imaginea steganografică poate prezenta diferenţe faţă de imaginea de acoperire. Aceste diferenţe depind de tipologia mesajului ce se doreşte a fi ascuns precum şi de imaginea de acoperire. În situaţia în care imaginea de acoperire este luată aleator dintr-un şir de imagini necunoscute, acest dezavantaj este foarte greu de sesizat. Spre exemplu, imaginea de acoperire poate fi o fotografie făcută în vacanţă, care este o

imagine unicat, privată şi a cărei structură iniţială nu este cunoscută de către un eventual atacator. Din acest motiv este puţin probabil ca acesta să aibă termeni de comparaţie ce ar putea sa-i trezească suspiciuni, în sensul că imaginea respectivă conţine un mesaj ascuns.

9.2.2.7 ASAC$_{MS}$-E$_2$ - Algoritm de extragere

Acest algoritm de obţinere a mesajului ascuns foloseşte atât imaginea steganografică, cât şi imaginea de acoperire originală a imaginii steganografice.

Paşii algoritmului:

1) Plecând de la imaginea steganografică exprimată prin matricea S se formează o matrice care are pe fiecare linie elementele unei culori. Această nouă matrice notată cu I_{S_1} este formată din 3 linii şi $n \times m$ coloane. Fiecare linie reprezintă prezintă proiecţiile imaginii RGB.
2) Pentru fiecare linie se calculează media, după care se scade din fiecare element al matricei I_{S_1}. Se obine astfel matricea $I^{\bullet}_{S_1}$.

3) Se aplică transformata KLT asupra matricei $I^{\bullet}_{S_1}$, reprezentând exprimarea imaginii steganografice în baza dată de vectorii proprii ai imagini de acoperire şi se obţine matricea I_{S_K}.

$$I_{S_K} = Q^T * I^{\bullet}_{S_1} \tag{9.61}$$

Unde:

$$I_{S_K} = \begin{bmatrix} s_{k_{1,1}} & \cdots & s_{k_{1,n,1}} \\ s_{k_{2,1,1}} & & s_{k_{2,n,1}} \\ s_{k_{3,1,1}} & & s_{k_{3,n,1}} \end{bmatrix} \tag{9.62}$$

4) Se ia coeficientul care exprimă procentual cantitatea de mesaj secret încorporată în proiecţia de vectori proprii corespunzători valorilor proprii minime Acest coeficient
s-a notat cu $coef$ în algoritmul de ascundere C_{MS}.

Din matricea I_{S_K} se alege linia indicată de indicele ind şi se generează matricea liniară A, în care este ascuns mesajul, sub forma:

$$A = coef \times linia(ind)a\ matricii\ I_{S_K} - (1 - coef) \times linia(ind)a\ matricii\ I_K \tag{9.63}$$

Matricea liniară A este constituită atât din imaginea steganografică, cât şi din imaginea de acoperire într-o proporţie identică, folosită în procesul de ascundere. Această matrice va înlocui linia specificată de indicele ind din matricea I_{S_K}. În cazul în care se consideră $ind = 3$, atunci matricea rezultată, notată $I^{\bullet}_{S_K}$ va fi:

$$I^{\bullet}_{S_K} = \begin{bmatrix} s_{k_{1,1,1}} & \cdots & s_{k_{1,n,1}} \\ s_{k_{2,1,1}} & & s_{k_{2,n,1}} \\ a_{1,1} & & a_{n,m} \end{bmatrix} \tag{9.64}$$

5) Se calculează media elementelor din matricea A după care se scade din fiecare element a acesteia.

6) Din matricea $I\overset{\bullet}{s}_K$ nou rezultată se ia linia ind , care reprezintă totodată şi matricea liniară în care este ascuns mesajul. Se scalează această matrice linie, formată din $n \times m$ coloane, între 0 şi 255 pentru a obţine contrastul maxim şi se generează astfel matricea A_1 .

7) Pornind de la numărul de plecare utilizat în algoritmul de ascundere $ASAC_{MS}$, se generează acelaşi şir pseudoaleator de întregi cuprins între "1" şi $n \times m$, obţinut cu ajutorul algoritmului Messenne-Twister. În final se obţine matricea mesajului final recuperat A_f.

8) Se aranjează elementele matricei linie A_f într-o matrice de n linii şi m coloane şi se obţine matricea mesajului extras în format RGB, care se notează cu M_R şi reprezintă matricea mesajului recuperat.

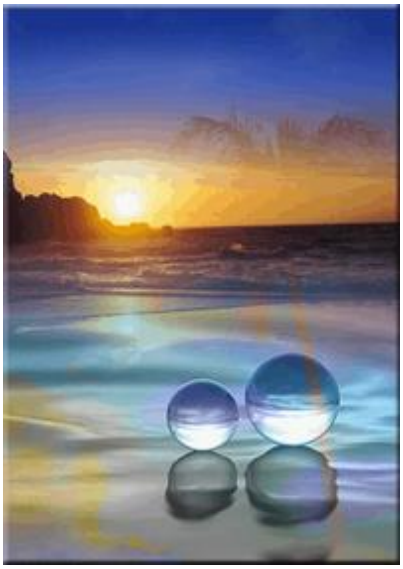
Algoritmul de extragere care necesită atât imaginea steganografică, cât şi imaginea de acoperire se pretează pentru watermarking, deoarece în acest caz trebuie ca receptorul să deţină imaginea de acoperire originală şi acest lucru este posibil deoarece cel care încorporează un watermark nu doreşte să ascundă o informaţie, ci doreşte doar să vadă dacă produsul a fost clonat sau nu. Acest lucru îl poate constata prin recuperarea mesajului şi compararea cu mesajul original. În această ipostază cele 2 mesaje trebuie să difere cât mai puţin. Această soluţie poate fi utilizată în protecţia drepturilor de autor.

9.2.2.8 ASAC$_{MS}$ – Experimente

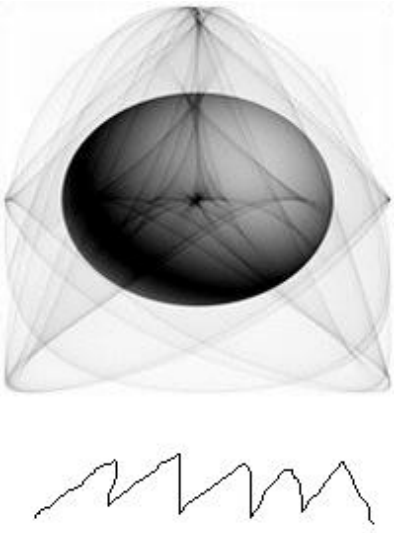
$\mathbf{ASAC_{MS}-E_1}$ – Rezultate experimentale obţinute în cazul în care la extragerea mesajului se utilizează numai imaginea steganografică sunt reprezentate în figurile 9.23, 9.24, 9.25, 9.26:

Dimensiune: 200x283x24biti = 165,9kb

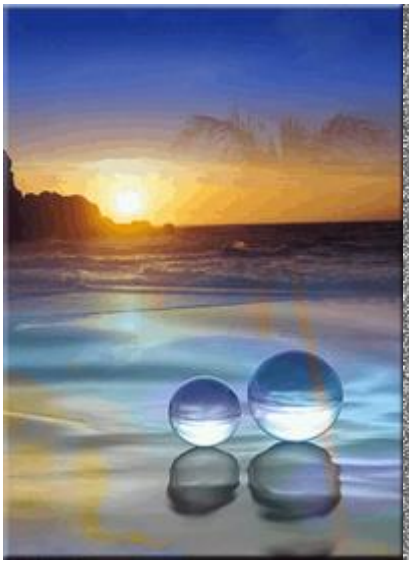
Dimensiune:200x283x8biti = 56,3kb



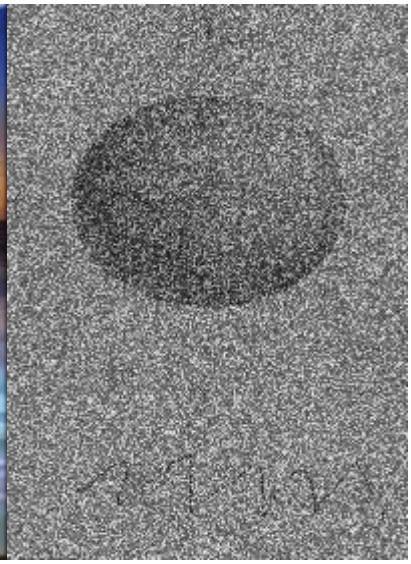
Imagine inițială



Mesajul secret



Imagine steganografică



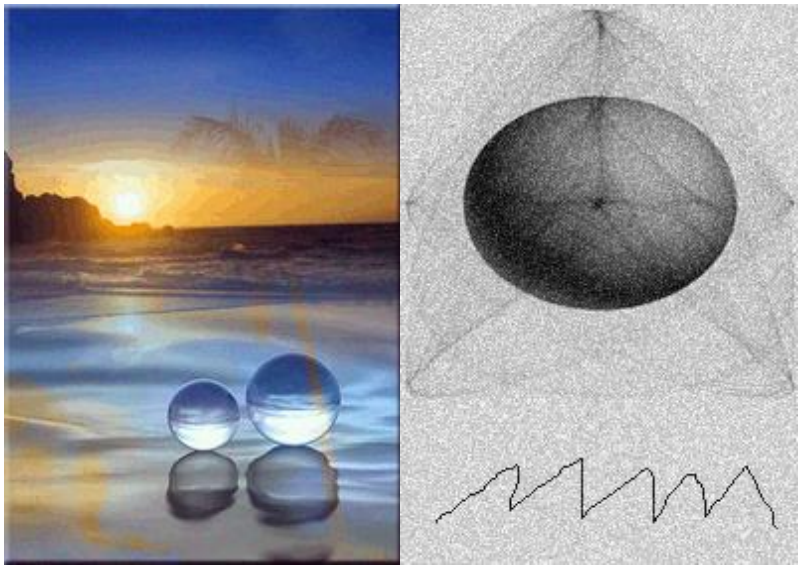
Imagine recuperată

Figura 9.23 Extragere mesaj $\mathbf{ASAC_{MS}} - E_1$ - Ascundere $\mathbf{ASAC_{MS}}$ - A_2

Eroarea relativă dintre C şi S : 0.27%
Eroarea relativă dintre mesajul ascuns şi mesajul recuperat: 35,21%
$coef = 0.2$

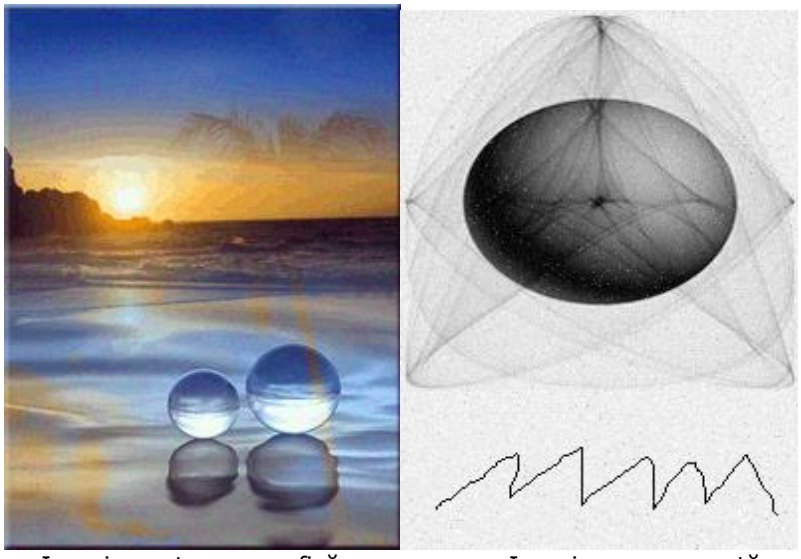
Imaginea steganografică Imaginea recuperata
Figura 9.24 Extragere mesaj $\mathbf{ASAC_{MS}} - E_1$ - Ascundere $\mathbf{ASAC_{MS}}$ - A_2

Eroarea relativă dintre C şi S : 0.7%
Eroarea relativă dintre mesajul ascuns şi mesajul recuperat: 22,03%
$coef = 0{,}5$



Imaginea steganografică Imaginea recuperată
Figura 9.25 Extragere mesaj $\mathbf{ASAC_{MS}} - E_1$ - Ascundere $\mathbf{ASAC_{MS}}$

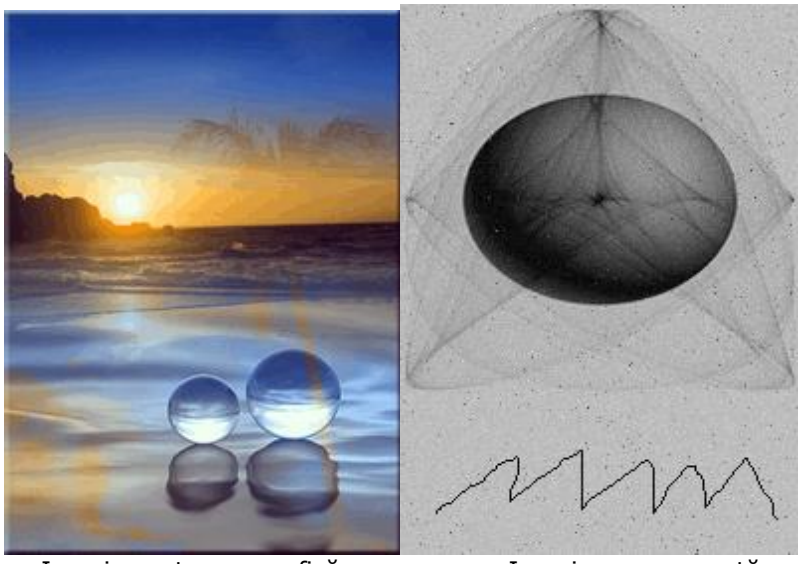
Eroarea relativă dintre QUOTE C C şi QUOTE S S : 0.98%
Eroarea relativă dintre mesajul ascuns şi mesajul recuperat: 12,88%
QUOTE $coef = 0{,}7$ $coef = 0{,}7$



Imaginea steganografică Imaginea recuperată

Figura 9.26 Extragere mesaj QUOTE $KLT_K - A$ $\mathrm{ASAC_{MS}} - E_1$ - Ascundere QUOTE $KLT_K - A_2$ $\mathrm{ASAC_{MS}}$ - A_2

Eroarea relativă dintre QUOTE C C şi QUOTE S S : 1,26%
Eroarea relativă dintre mesajul ascuns şi mesajul recuperat: 4,68%
$coef = 0{,}9$
QUOTE $KLT_K - E_1$ $\mathrm{ASAC_{MS}} - E_1$ – Rezultate experimentale obţinute în cazul în care la extragerea mesajului se utilizează numai imaginea steganografică sunt reprezentate în figurile 9.27, 9.28, 9.29, QUOTE ÷ 9.30



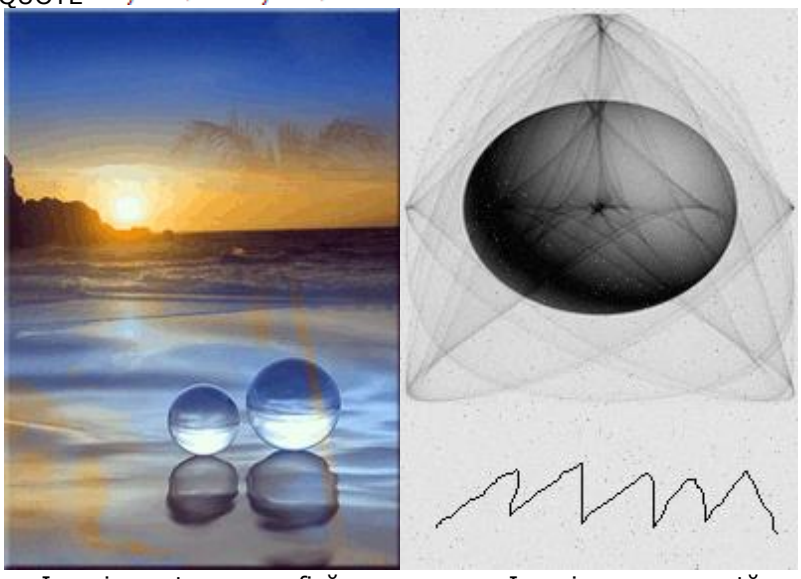
Imaginea steganografică Imaginea recuperată

Figura 9.27 Extragere mesaj QUOTE $KLT_K - A$ $\mathrm{ASAC_{MS}} - E_1$ - Ascundere QUOTE $KLT_K - A_1$ $\mathrm{ASAC_{MS}}$ - A_1

Eroarea relativă dintre QUOTE C C şi QUOTE S S : 0,89 %

Eroarea relativă dintre mesajul ascuns şi mesajul recuperat: 20,48%

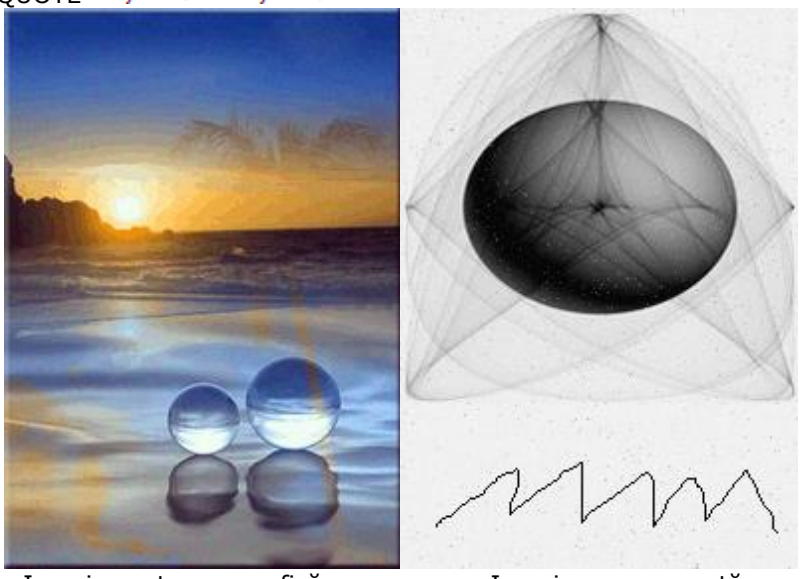
QUOTE $coef = 0{,}2$ $coef = 0{,}2$



Imaginea steganografică Imaginea recuperată

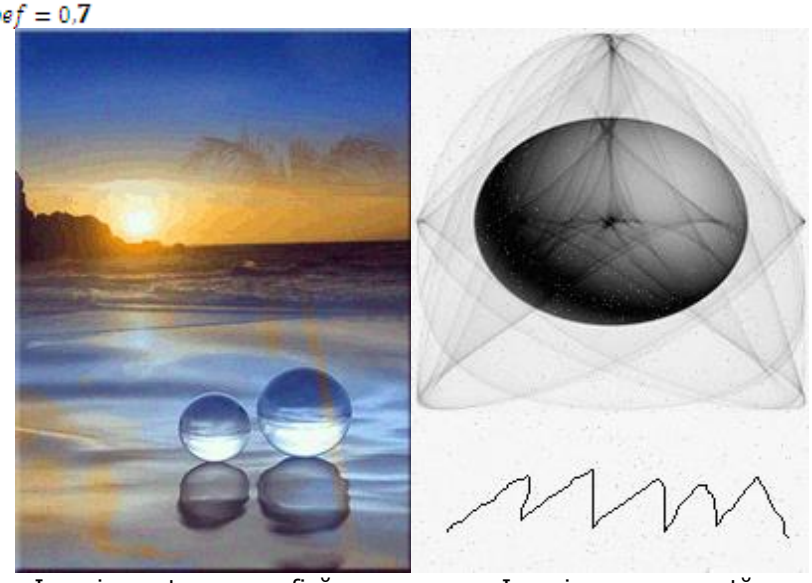
Figura 9.28 Extragere mesaj QUOTE $KLT_K - A$ $\mathrm{ASAC_{MS}} - E_1$ - Ascundere QUOTE $KLT_K - A_1$ $\mathrm{ASAC_{MS}}$ - A_1

Eroarea relativă dintre QUOTE C C şi QUOTE S S : 1,04 %
Eroarea relativă dintre mesajul ascuns şi mesajul recuperat: 8,5%
QUOTE $coef = 0{,}5$ $coef = 0{,}5$



Imaginea steganografică Imaginea recuperată
Figura 9.29 Extragere mesaj QUOTE $KLT_K - A$ $ASAC_{MS} - E_1$ - Ascundere QUOTE $KLT_K - A_1$ $ASAC_{MS}$ - A_1

Eroarea relativă dintre QUOTE C C şi QUOTE S S : 1,17 %
Eroarea relativă dintre mesajul ascuns şi mesajul recuperat: 4,34 %
$coef = 0{,}7$

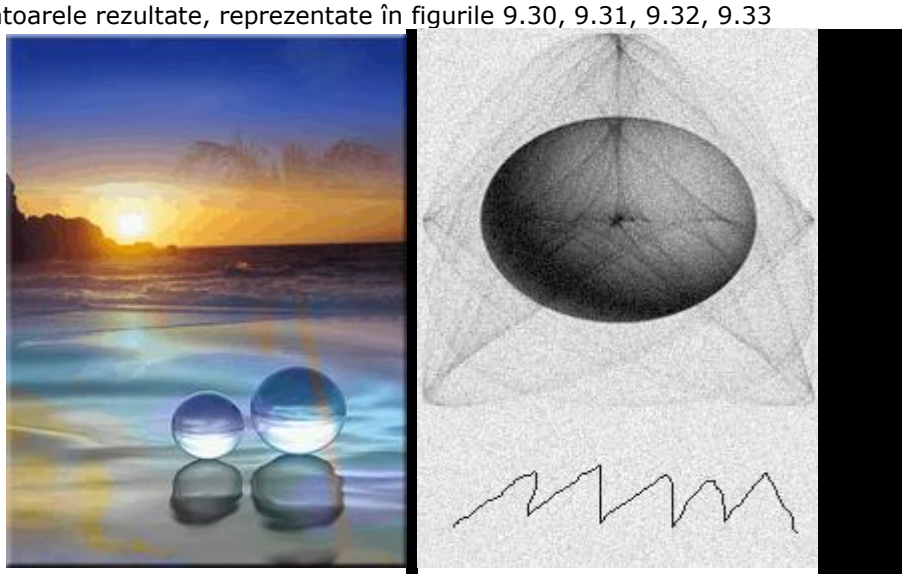


Imaginea steganografică Imaginea recuperată

Figura 9.30 Extragere mesaj QUOTE $KLT_K - \mathrm{A}\ \mathrm{ASAC_{MS}} - E_1$ - Ascundere QUOTE $KLT_K - A_1\ \mathrm{ASAC_{MS}}$ - A_1

Eroarea relativă dintre QUOTE $C\ C$ şi QUOTE $S\ S$: 1,32 %
Eroarea relativă dintre mesajul ascuns şi mesajul recuperat: 2,53 %
QUOTE $coef = 0{,}9\ \ coef = 0{,}9$

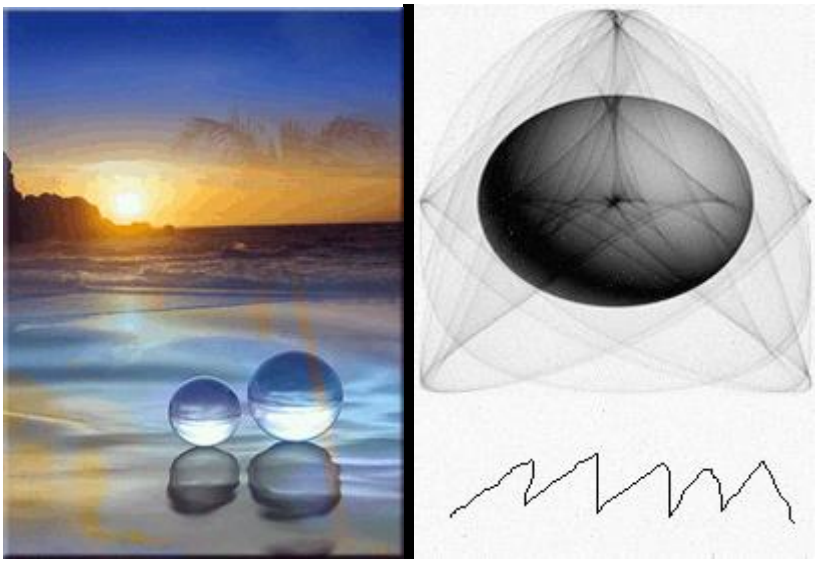
QUOTE $KLT_K - E_2\ \ ASAC_{MS} - E_2$ - Dacă la extragerea mesajului se utilizează atât imaginea steganografică cât şi imaginea originală se obţin următoarele rezultate, reprezentate în figurile 9.30, 9.31, 9.32, 9.33



Imaginea steganografică imaginea recuperate

Figura 9.31 QUOTE $KLT_K - E_2\ \mathrm{ASAC_{MS}} - E_2$ - Ascundere şi recuperare mesaj

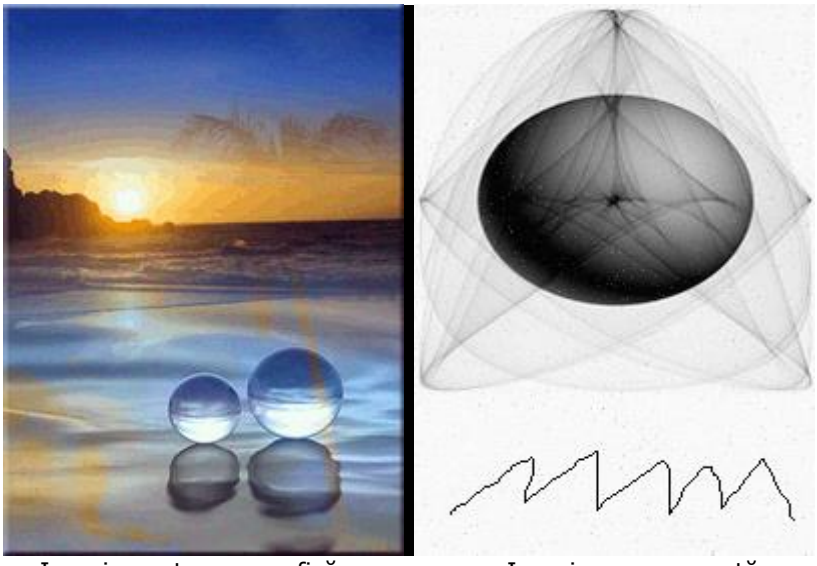
Eroarea relativă dintre QUOTE $C\ C$ şi QUOTE $S\ S$: 0,41 %
Eroarea relativă dintre mesajul ascuns şi mesajul recuperat: 3,13 %
QUOTE $coef = 0{,}2\ \ coef = 0{,}2$



Imaginea steganografică Imaginea recuperată

Figura 9.32 QUOTE $KLT_K - E_2$ $\mathrm{ASAC_{MS}} - E_2$ - Ascundere şi recuperare mesaj

Eroarea relativă dintre QUOTE C C şi QUOTE S S : 0,70 %
Eroarea relativă dintre mesajul ascuns şi mesajul recuperat: 1,85 %
QUOTE $coef = 0{,}5$ $coef = 0{,}5$

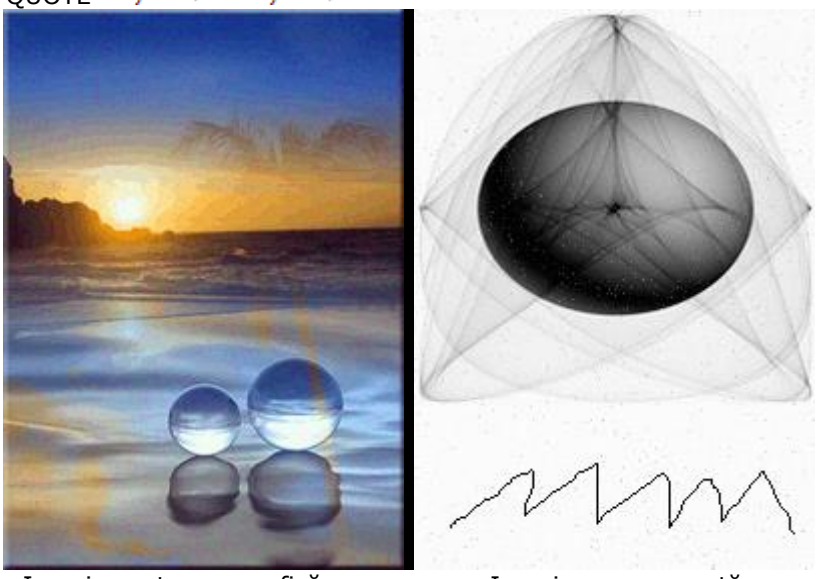


Imaginea steganografică Imaginea recuperată

Figura 9.33 QUOTE $KLT_K - E_2$ $\mathrm{ASAC_{MS}} - E_2$ - Ascundere şi recuperare mesaj

Eroarea relativă dintre QUOTE C C şi QUOTE S S : 0,98 %
Eroarea relativă dintre mesajul ascuns şi mesajul recuperat: 1,77 %

QUOTE $coef = 0{,}7$ $coef = 0{,}7$



Imaginea steganografică Imaginea recuperată

Figura 9.34 QUOTE $KLT_K - E_2$ $ASAC_{MS} - E_2$ - Ascundere şi recuperare mesaj

Eroarea relativă dintre QUOTE C C şi QUOTE S S : 1,26 %
Eroarea relativă dintre mesajul ascuns şi mesajul recuperat: 1,20 %
QUOTE $coef = 0{,}9$ $coef = 0{,}9$

9.2.2.9 ASAC$_{MS}$ - Concluzii

Algoritmul prezentat în acest subcapitol prin cele 4 variante discutate utilizează ca obiect de acoperire o imagine digitală color, iar mesajul secret este o imagine digitală alb-negru. În cadrul algoritmului are loc atât prelucrarea obiectului de acoperire, cât şi a mesajului secret care la rândul lui este încorporat prin repartizarea lui în toată imaginea de acoperire.

Distribuirea mesajului secret în cadrul algoritmul QUOTE KLT_K $ASAC_{MS}$ îi conferă acestuia un grad mare de siguranţă deoarece pentru ascunderea lui se utilizează un algoritm pseudoaleator (Mersenne-Twister), a cărui rată de repetiţie este de 2^{19937}-1. Spre exemplu, dacă se consideră că numărul de iteraţii pe secundă este 1 miliard ar fi necesari 40 de ani pentru a parcurge toate iteraţiile, iar la 1 milion de iteraţii pe secundă sunt necesari 40.000 de ani. Acest aspect permite o securizare deosebit de bună a mesajului, ceea ce implică un timp de descifrare imposibil de realizat. Mai mult introducerea unui coeficient de proporţionalitate măreşte gradul de incertitudine al unui atacator. Utilizarea algoritmului QUOTE $ASAC_{MS}$ $ASAC_{MS}$ generează un sistem steganografic superior dacă ascunderea datelor secrete se face în imagini eterogene, cu foarte puţine zone compacte de aceeaşi culoare.

Algoritmul steganografic mai prezintă câteva artificii care sunt greu de descifrat de un eventual atacator, cum ar fi scalarea cu valoarea medie a pixelilor, folosirea unor valori ale coeficienţilor utilizaţi în transformările făcute. Extragerea mesajului devine foarte dificilă în acest caz, deoarece coeficienţii utilizaţi sunt necunoscuţi atacatorului.

Caracteristicile algoritmului QUOTE KLT_K $ASAC_{MS}$ constau în faptul că pe lângă procesarea mesajului secret are loc şi o procesare a obiectului de acoperire care conduce la obţinerea unui obiect steganografic cu erori ce pot scădea până la 0,41%, iar eroarea dintre mesajul iniţial şi mesajul recuperat poate scădea până la 1,2% în funcţie de varianta aleasă atât la ascunderea mesajului secret, cât şi la extragerea acestuia. Cele patru variante diferite ale algoritmului QUOTE KLT_K $ASAC_{MS}$ permit o mare flexibilitate în utilizarea acestuia în funcţie de situaţia concretă ce trebuie rezolvată.

Mai mult, şi acest algoritm validează modelul propus în capitolul 6 în sensul că se utilizează atât procesarea obiectului de acoperire, cât şi a mesajului secret. Astfel, în situaţia în care se trimit seturi de imagini dintre care unele nu conţin informaţie ascunsă, atacatorul este obligat să le proceseze pe toate. În urma procesării el trebuie să sesizeze în care dintre imaginile procesate există date utile sau nu. Presupunând ca ia cea mai bună decizie va constata că mesajul recuperat este fără valoare, deoarece acesta este codificat. În cazul în care ar putea să-şi dea seama de metoda prin care mesajul a fost codificat şi dispune de o putere de calcul semnificativă, timpul de decriptare devine extrem de mare, ceea ce conduce la costuri foarte mari. În ceea ce priveşte cantitatea de informaţie ascunsă rezultatul experimentelor efectuate a condus la obţinerea unei valori încorporare de 33% din capacitatea obiectului de acoperire.

În concluzie, algoritmul conceput şi prezentat în acest subcapitol oferă o protecţie suplimentară din punct de vedere al încercării extragerii mesajului secret de către persoane neautorizate, ceea ce l-ar putea de asemenea recomanda a fi utilizat şi în telefonia mobilă deoarece timpul de execuţie este comparabil cu cel al celorlalţi algoritmi dezvoltaţi în acest capitol. Ca viitoare direcţie de cercetare îmi propun şi testarea acestui algoritm pe noua variantă a microprocesorului ISAAC în vederea obţinerii unor rezultate care să îndeplinească eventuale cerinţe legate de o comunicare confidenţială cu un grad mai ridicat de robusteţe în cazul unui atac.

9.3 ***Concluzii***

În cadrul acestui capitol s-a realizat o prezentare a patru algoritmi diferiţi ce utilizează domeniul vectorial de reprezentare a imaginilor digitale. Punctul de plecare a constat în transformarea imaginilor digitale din spaţiul RGB într-un spaţiu vectorial folosind diferite proceduri de transformare, cum ar fi descompunerea în valori singulare, transformata Karthunen-Loeve, după care a urmat practic aplicarea diferitelor metode de ascundere specifice celor 4 algoritmi. Ca şi obiect de acoperire s-a utilizat o imagine color digitală, iar ca mesaje secrete au fost utilizate imagini binare, alb-negru şi color.

Fiecare dintre cei patru algoritmi se caracterizează prin una sau mai multe proprietăţi specifice sistemelor steganografice. Astfel dacă se doreşte o robusteţe mare a mesajului secret se recomandă algoritmul bazat pe descompunerea în valori

singulare (QUOTE SVD SVD). În cazul în care se doreşte creşterea cantităţii de informaţie ce poate fi ascunsă se recomandă algoritmul ce se bazează pe ascunderea în biţii cei mai puţini semnificativi combinată cu o procedură de comprimare efectuată asupra mesajului original (QUOTE $ASAC$ $ASAC$). Pentru a obţine un sistem steganografic cu dificultăţi sporite în extragerea mesajului secret în eventualitatea în care un atacator ar dori acest lucru se recomandă algoritmul bazat pe codificarea acestuia (QUOTE $ASAC_{MS}$ $ASAC_{MS}$). În situaţia în care se doreşte inducerea în eroare a unor eventuali atacatori se recomandă algoritmul prin care mesajul secret este ascuns într-un semnal de zgomot generat artificial (QUOTE $ASAZ$ $ASAZ$) astfel încât aceştia să interpreteze zgomotele ca fiind produse de canalele de transmisie.

Pe de altă parte trebuie menţionat că o bună parte din algoritmii descrişi în acest capitol pot fi consideraţi că deţin şi alte proprietăţi. Spre exemplu algoritmul QUOTE $ASAZ$ $ASAZ$ prezintă o robusteţe mare în cazul unor atacuri, ca de altfel şi algoritmul QUOTE $ASAC_{MS}$ $ASAC_{MS}$. Mai mult, acesta din urmă prezintă calităţi din punct de vedere al recuperării mesajului secret. În ceea ce priveşte algoritmul QUOTE $ASAC$ $ASAC$ se poate spune că satisface în condiţii foarte bune recuperarea mesajului secret.

Despre toţi cei trei algoritmi ce folosesc parţial sau total transformata Karthunen-Loeve se poate remarca faptul că prezintă o imagine steganografică de o calitate foarte bună cu erori foarte mici raportate la obiectul de acoperire. Cele câteva caracteristici ale algoritmilor steganografici descrişi în acest capitol se regăsesc în tabelul 10.1. Este de remarcat că toţi cei trei algoritmi validează modelul propus de mine în capitolul 6 referitor la faptul că atât procesarea obiectului de acoperire, cât şi a mesajului secret conduce la îmbunătăţirea întregului sistem steganografic. Aceasta se poate constata atât prin obţinerea unei imagini steganografice de o calitate foarte bună, cât şi prin recuperarea mesajului aproape în totalitate.

Pentru toţi algoritmii am efectuat experimente pe diferite seturi de imagini digitale scoţând în evidenţă caracteristicile acestora, iar acolo unde a fost cazul am făcut comparaţii referitoare la timpul de execuţie al lor. Precizez că în lucrare sunt prezentate doar o mică parte din experimentele efectuate.

Referitor la algoritmul bazat pe descompunerea în valori singulare este de menţionat că a constituit obiectul unui articol [STA08b] şi a fost folosit ca termen de comparaţie pentru alţi algoritmi dezvoltaţi de mine.

În continuare s-a prezentat o sinteză a utilizării transformatei Karthunen-Loeve în domeniul steganografiei şi s-a dezvoltat un prim algoritm (QUOTE $ASAC$ $ASAC$) ce permite utilizarea transformatei menţionate pentru comprimarea mesajului secret şi ascunderea acestuia în biţii cei mai puţini semnificativi ai obiectului de acoperire. Pentru acest algoritm am dezvoltat trei variante, fiecare dintre acestea fiind testată şi verificată pe un număr de imagini digitale de mărimi diferite, atât pentru obiectul de acoperire, cât şi pentru mesajul secret. În vederea reducerii timpului de execuţie acelaşi algoritm a fost implementat pe un microprocesor ARM, o mică parte din rezultatele experimentale fiind prezentate în această lucrare.

Tot pe baza transformatei Karthunen-Loeve am dezvoltat un algoritm QUOTE $ASAZ$ $ASAZ$ ce urmăreşte obţinerea altor caracteristici steganografice. În acest sens imaginea de acoperire este transformată din domeniul spaţial RGB în domeniul vectorial, efectuându-se în prealabil prelucrări asupra acesteia. Pasul următor presupune generarea artificială a unui zgomot şi mixarea acestuia cu

mesajul secret în mod pseudoaleator, scopul urmărit fiind inducerea în eroare a unui eventual atacator. Semnalul astfel rezultat este încorporat în obiectul de acoperire. Pentru extragerea mesajului se aplică funcţiile inverse folosite la generarea obiectului steganografic.

În ceea ce priveşte ultimul algoritm creat QUOTE $ASAC_{MS}$ $ASAC_{MS}$ după transformarea obiectului de acoperire am prelucrat mesajul secret cu scopul ca acesta să fie distribuit pseudoaleator în obiectul de acoperire. Prin această soluţie pixelii vecini ai mesajului secret sunt încorporaţi în diferite zone, ceea ce reduce senzaţia vizuală percepută de ochiul uman. Folosirea unei astfel de soluţii permite atât îmbunătăţirea clarităţii obiectului steganografic, cât şi crearea unor obstacole suplimentare în cazul încercării extragerii mesajului secret de către un eventual atacator. În cadrul algoritmului au fost concepute două soluţii privind modul de ascundere a mesajului secret. Prima soluţie constă în faptul că acesta este încorporat în totalitate în obiectul de acoperire, iar a doua presupune mixarea în proporţii alese printr-un coeficient a câta parte din mesajul secret se poate ascunde în obiectul de acoperire pentru ca obiectul steganografic rezultat să fie obţinut cu o eroare cât mai mică. Şi pentru procesul de extragere s-au realizat două variante. Astfel că, o într-o primă variantă se presupune că receptorul este suficient să cunoască doar obiectul steganografic pentru extragerea mesajului secret, iar în a doua variantă acesta trebuie să aibă cunoştinţă atât despre obiectul de acoperire original, cât şi despre obiectul steganografic.

Pe baza algoritmilor dezvoltaţi în acest capitol se poate desprinde concluzia că un algoritm steganografic care să fie performant nu poate satisface în totalitate toate caracteristicile unui sistem steganografic. În acest sens, am urmărit ca prin algoritmii dezvoltaţi de mine să îndeplinesc o parte din caracteristicile sistemelor steganografice, în ideea de a obţine performanţe maxime în acea direcţie. Astfel, cu unii dintre algoritmii descrişi în acest capitol am reuşit să ascund o cantitate ce tinde spre un maxim de informaţie ce se poate încorpora, obţinând totodată un raport de recuperare a mesajului secret cu o eroare minimă, iar cu ceilalţi am urmărit ca mesajul ascuns să prezinte o robusteţe cu un grad ridicat în cazul unor atacuri. Menţionez că pentru reducerea timpilor de execu?ie urmează ca toţi algoritmii descrişi să fie implementaţi pe mai multe microprocesoare ce vor fi utilizate în telefonia mobilă, în scopul furnizării funcţiei steganografice privind transmiterea confidenţială a convorbirilor telefonice.

10 CONCLUZII FINALE ?I CONTRIBU?II PERSONALE. PERSPECTIVE

10.1 *Concluzii*

Lucrarea de faţă este dedicată cercetărilor din domeniul de mare actualitate al dezvoltării de algoritmi steganografici, abordându-se probleme atât teoretice cât şi aplicative de reală utilitate, direcţionate în principal pe optimizarea creşterii cantităţii de informaţie ascunsă, a recuperării în condiţii cât mai bune a mesajului încorporat, precum şi a îmbunătăţirii timpului de execuţie.

Obiectivul principal al lucrării îl constituie găsirea unui model steganografic care să asigure un grad ridicat de securitate şi dezvoltarea unor algoritmi steganografici în concordanţă cu modelul propus. În plus s-a dorit ca algoritmii dezvoltaţi să prezinte şi o utilitate practică în sensul modelărilor pe diferite platforme, cum ar fi un calculator personal, microprocesoare utilizate în prezent în telefonia mobilă, respectiv microprocesoare ce vor fi utilizate în viitor în telefonia mobilă. Utilitatea practică a rezultat din cerinţa unui producător de microprocesoare ca urmare a necesităţilor identificate la viitorii beneficiari a acestor echipamente.

Direcţiile de cercetare dezvoltate în teză au urmărit o succesiune de problematici specifice domeniului steganografiei.

Pe baza definirii terminologiei legate de steganografie şi ţinând cont de dezvoltarea tehnologică din ultimii ani s-a constatat o tendinţă tot mai crescută de utilizare a steganografiei în diferite scopuri, cum ar fi transmiterea de informaţii secrete, stocarea acestora, respectiv protecţia lor în ceea ce priveşte dreptul de autor.

În ultimul timp se observă o tendinţă tot mai accentuată de creştere a mobilităţii aplicaţiilor în domeniul tehnologiei informaţiei datorită depăşirii vânzărilor de echipamente mobile în comparaţie cu cele staţionare. În această categorie se încadrează şi telefonia mobilă, unde se remarcă de asemenea o evoluţie a performanţelor echipamentelor utilizate, mai cu seamă în ceea ce priveşte puterea de prelucrare a datelor în cadrul acestora.

Dacă numărul de specialişti în domeniul calculatoarelor la ora actuală este foarte mare, nu se poate spune acelaşi lucru şi despre numărul celor care furnizează aplicaţii în domeniul telefoniei mobile. Bazându-mă pe aceste constatări unii dintre algoritmii steganografici realizaţi au fost dezvoltaţi şi pe microprocesoare utilizate în telefonia mobilă.

Pentru a determina cel mai bun purtător în care să fie încorporată informaţie secretă s-a făcut o sinteză a celor mai adecvate medii steganografice utilizate ca şi suport de ascundere. Pe baza analizării proprietăţilor de bază ale steganografiei în ceea ce priveşte cantitatea de informaţie ce poate fi ascunsă, dificultatea de interceptare a informaţiei secrete de către un eventual atacator, respectiv robusteţea manifestată de către mesajul secret în cazul intervenţiei unor persoane neautorizate pe canalul de transmisie cu scopul deteriorării acestuia s-a constatat că imaginile digitale prezintă calităţile cele mai bune în acest sens. Ca urmare, în

această teză s-a decis utilizarea în continuare a imaginilor digitale ca şi obiecte de acoperire în vederea realizării unui proces steganografic.

Imaginile digitale exprimate sub formă binară, alb-negru şi color sunt reprezentate în trei domenii diferite în funcţie de modul de utilizare a acestora. În domeniul spaţial se pleacă de la modalitatea de achiziţie a imaginii care este reprezentată de aşa manieră încât aceasta să fie cât mai adaptată fiziologiei ochiului uman, existând la ora actuală o multitudine de exprimări a culorilor în acest sens. Domeniul frecvenţă prezintă avantajul unor prelucrări ale imaginilor în mod optim şi se bazează pe diferite transformări analizate şi în această lucrare, plecând de la transformata Fourier şi ajungându-se la transformata cosinus discretă. În ceea ce priveşte domeniul vectorial, pixelii sunt exprimaţi sub această formă fiind în principiu un domeniu considerat optim din punct de vedere statistic, în sensul că ar putea obţine o compactare cât mai bună a unei imagini fără pierdere semnificativă a calităţii acesteia. Şi acest domeniu se bazează pe o serie de transformări cum ar fi Karthunen-Loeve sau descompunerea în valori singulare.

Dintre cele trei domenii de reprezentare a imaginii, domeniul spaţial este cel care implică prelucrări cu un grad ridicat de paralelizare fiind foarte potrivit în dezvoltarea unor algoritmi steganografici ce permit ascunderea unor cantităţi suficient de mari de informaţie, în schimb calitatea obiectului steganografic poate fi degradată în cazul în care nu se adoptă soluţia potrivită pentru algoritmul implementat. În acest domeniu am dezvoltat mai mulţi algoritmi specifici.

Domeniul frecvenţă este un domeniu des utilizat în procesarea imaginilor referitor la recunoaşterea acestora, respectiv comprimarea lor fiind utilizat şi în steganografie datorită proprietăţilor transformărilor utilizate, în sensul ascunderii informaţiilor secrete în coeficienţii acestora. Este de remarcat faptul că datorită menţinerii unui număr relativ mic de coeficienţi şi cantitatea de informaţii ce poate fi ascunsă este relativ mică. Cu toate acestea şi în acest domeniu am implementat un algoritm bazat pe transformata cosinus discretă, scopul urmărit fiind analizarea proprietăţilor acestui domeniu şi compararea acestui algoritm cu cei dezvoltaţi în celelalte domenii.

Domeniul vectorial este un domeniu care a fost mai rar folosit în steganografie, în principal datorită vizibilităţii mesajului ascuns în obiectul de acoperire, fiind utilizat mai frecvent în watermarking, deoarece în această direcţie mesajul secret poate fi vizibil sau invizibil. Pentru acest domeniu am dezvoltat mai mulţi algoritmi care să pună în valoare fie robusteţea sistemului steganografic, fie cantitatea de informaţii maxime ce poate fi ascunsă, fie recuperarea în bune condiţii a mesajului secret şi chiar introducerea unor metode prin care extragerea acestuia în cazul unei eventuale depistări să devină foarte dificilă.

Pentru a îmbunătăţii timpul de execuţie al algoritmilor steganografici dezvoltaţi s-a propus executarea acestora pe două platforme ce conţin microprocesoare utilizate în telefonia mobilă actuală, respectiv în viitoarea generaţie de telefoane mobile. Pentru a avea acces la unul dintre microprocesoarele ce vor echipa telefoanele mobile s-a colaborat cu o companie ce proiectează microprocesoare din familia ISAAC. La cererea acesteia privind realizarea unei funcţii steganografice în vederea obţinerii confidenţialităţii comunicării pentru clienţii companiei s-au dezvoltat pentru testare şi validare mai mulţi astfel de algoritmi steganografici care să îndeplinească această cerinţă. Rezultatele experimentelor efectuate pe cele două microprocesoare confirmă faptul că aceşti algoritmi pot fi implementaţi, mai mult s-a constatat o îmbunătăţire semnificativă a performanţelor legate de timpul de execuţie. Este de menţionat faptul că performanţele algoritmilor

steganografici se păstrează şi în cazul rulării pe microprocesoare, fiind apreciate şi de firma producătoare.

În urma sistematizării şi sintezei privind modelele steganografice existente şi a analizării avantajelor şi dezavantajelor acestora am propus un model teoretic prin care sunt înlăturate o parte din dezavantajele constatate la modelele cele mai frecvent utilizate în prezent. Modelul propus constă în transmiterea către receptor a unui set de imagini digitale ca şi obiecte de acoperire. Modalitatea de obţinere a acestora nu este cunoscută, ceea ce conduce la creşterea incertitudinii unui eventual atacator. Setul de obiecte de acoperire se poate constitui dintr-un număr nedefinit de obiecte, asupra cărora se efectuează un proces de prelucrare cunoscut doar de emiţător şi receptor. În unele dintre aceste obiecte de acoperire se încorporează mesajul secret printr-un algoritm steganografic propus.

Receptorul cunoaşte atât obiectul de acoperire în care s-a încorporat mesajul, cât şi algoritmul de ascundere. Toate obiectele de acoperire, respectiv atât cele care conţin informaţie secretă, cât şi cele care nu conţin sunt trimise pe canalele de comunicare la receptor, iar acesta pe baza algoritmului steganografic cunoscut, precum şi a procedurii de procesare a obiectelor poate extrage mesajul secret din obiectul steganografic cunoscut. A doua variantă a modelului propus are ca bază varianta prezentată anterior cu singura observaţie că mesajul secret este procesat şi el înainte de a fi încorporat. Alegerea uneia dintre cele două variante se va face în funcţie de gradul dorit de protecţie a datelor.

Modelul prezentat în urma demonstraţiei matematice efectuate se dovedeşte a avea un grad mai ridicat de securizare decât cele existente în literatură datorită utilizării unei funcţii de procesare adecvată. Pe lângă confirmarea teoretică a modelului s-a verificat şi practic acest lucru prin faptul că eroarea dintre obiectul de acoperire şi obiectul steganografic scade în urma procesării, cunoscând faptul că obţinerea unei erori mici între cele două obiecte conduce la obţinerea unei diferinţe dintre distribuţiile de probabilitate corespunzătoare obiectelor, ce tinde şi ea spre o valoare mai mică.

Cu alte cuvinte se poate spune că, dacă diferenţa dintre cele două distribuţii este foarte mică cel ce doreşte să intercepteze mesajul steganografic nu poate face diferenţa dintre obiectul de acoperire şi cel steganografic, deci nu poate extrage mesajul secret. Mai mult, prin faptul că sunt trimise un set de obiecte din care nu poate fi depistat practic care anume obiect conţine informaţie secretă, un eventual atacator este obligat să prelucreze toate aceste obiecte în încercarea de a găsi mesajul ascuns printr-un algoritm polinomial. Este evident că timpul de extragere a întregului mesaj creşte cu cât numărul de necunoscute este mai mare, făcând foarte dificilă obţinerea acestuia într-un timp real.

Modelul propus a fost verificat şi testat pe un număr de obiecte de acoperire utilizate folosind ca mesaje secrete imagini digitale. Testarea s-a efectuat în trei modalităţi. Un prim set de teste s-a realizat doar prin prelucrarea obiectelor de acoperire, un al doilea test s-a efectuat doar prin prelucrarea mesajului şi un al treilea test s-a efectuat prin prelucrarea atât a obiectului de acoperire, cât şi a mesajului secret. Toate testele au confirmat faptul că eroarea dintre obiectul de acoperire şi obiectul steganografic s-a micşorat, iar recuperarea mesajului recuperat a crescut în calitate în urma prelucrării.

Prin stabilirea mecanismelor de îmbunătăţire a securităţii sistemelor steganografice, în urma demonstra?iilor efectuate s-a trecut la dezvoltarea unor algoritmi steganografici a căror concepere să includă şi astfel de concepte, legate de prelucrarea obiectelor de acoperire, respectiv a mesajului secret.

Algoritmii propuşi în domeniul spaţial de reprezentare a imaginilor au menirea de a satisface proprietăţile legate de cantitatea de informaţii ce poate fi ascunsă, a calităţii mesajului recuperat, cât şi rezolvarea unor aspecte legate de robusteţea sistemului steganografic. Un prim algoritm bazat pe ascunderea informaţiilor în biţii cei mai puţini semnificativi a urmărit procedee de creştere a capacităţii informaţiei ascunse cu obţinerea unui obiect steganografic care să satisfacă condiţiile teoretice demonstrate în modelul propus. Ca urmare, pentru toate cele trei variante ale algoritmului propus rezultatul obiectului steganografic prezintă diferenţe imperceptibile ochiului uman. Mai mult, recuperarea mesajului secret se realizează cu o eroare foarte bună comparativ cu mesajul original.

Prin al doilea algoritm dezvoltat în domeniul spaţial s-a urmărit atât creşterea gradului de securitate a sistemului, cât şi a robusteţii mesajului ascuns prin prelucrarea obiectului de acoperire cu ajutorul transformatei YUV. Informaţiile secrete au fost încorporate în biţii cei mai puţini semnificativi ai obiectului de acoperire astfel prelucrat.

Algoritmii menţionaţi mai sus au fost dezvoltaţi în continuare pentru a fi implementaţi pe două microprocesoare, unul utilizat în prezent cu precădere în telefonia mobilă, iar al doilea urmând a fi folosit în generaţia viitoare de telefonie.

Rezultatele testelor efectuate pe cele două microprocesoare au condus la îmbunătăţirea semnificativă a timpului de execuţie de până la 20 de ori şi au fost obţinute în condiţiile în care frecvenţele de lucru ale echipamentelor utilizate au fost compatibile. Îmbunătăţirea timpilor de execuţie s-a obţinut în special prin valorificarea superioară a arhitecturii microprocesoarelor utilizate pentru testare. Astfel se confirmă valabilitatea acestor algoritmi şi posibilitatea utilizării lor în generarea unor funcţii steganografice privind realizarea unor convorbiri confidenţiale în viitorul apropiat.

În vederea obţinerii unui optim între cantitatea de informaţii ce se poate ascunde, calitatea mesajului recuperat şi robusteţea acestuia cu menţinerea unui grad de securitate ridicat am implementat un algoritm bazat pe complexitatea planurilor de biţi ca studiu de caz în vederea comparării cu rezultatele obţinute prin algoritmii menţionaţi mai sus. În urma testelor efectuate s-a constatat posibilitatea implementării acestui algoritm pe microprocesoarele ce urmează a fi utilizate în telefonia mobilă cu condiţia reducerii cantităţii de memorie utilizată şi a micşorării timpului de execuţie sau în ideea utilizării unor microprocesoare mai performante, deoarece timpul de procesare al algoritmului în prezent este mare.

Algoritmul utilizat pentru realizarea unui proces steganografic în domeniul frecven?ei se bazează pe ascunderea informaţiei în coeficienţii transformatei cosinus discretă care implică încorporarea unei cantităţi relativ mici de informaţii. Acest tip de ascundere se pretează mai bine în watermarking. Luat ca şi termen de comparaţie se poate constata că mesajul recuperat se obţine cu o eroare mai mare, însă în schimb este robust în cazul unui atac intenţionat. Algoritmul a fost utilizat în vederea comparării acestuia din punct de vedere a performanţelor cu ceilalţi algoritmi dezvoltaţi în această lucrare.

Unul dintre domeniile care s-a dovedit potrivit pentru generarea de algoritmi steganografici îl constituie domeniul vectorial. Acest domeniu permite dezvoltarea unor algoritmi steganografici cu o flexibilitate relativ mare pentru obţinerea diferitelor proprietăţi ale sistemelor steganografice. Mai mult, se pot găsi diverse modalităţi de a îmbina proprietăţile domeniului vectorial cu cele ale altor domenii. Pe baza ideilor menţionate în lucrare s-a dezvoltat un set de algoritmi deosebit de performanţi din punct de vedere steganografic prin faptul că permit o cantitate maximă de informaţii ce poate fi ascunsă, cu obţinerea unei imagini

steganografice de o claritate foarte bună şi cu un grad de recuperare a mesajului secret cu erori mici la recuperare. Un astfel de algoritm dezvoltat în lucrare constă în comprimarea mesajului secret folosind transformata Karthunen-Loeve şi încorporarea vectorilor rezultaţi în urma comprimării în obiectul de acoperire în biţii cei mai puţini semnificativi, rezultând astfel unul dintre cei mai performanţi algoritmi dezvoltaţi în această lucrare.

Pentru creşterea gradului de securizare a sistemelor steganografice s-a dezvoltat un algoritm care are drept scop inducerea în eroare a unui eventual atacator, iar în acest sens informa?ia secretă este ascunsă în zgomote create artificial, deoarece există posibilitatea ca acestea să fie interpretate ca fiind generate pe canalul de transmisie şi pot fi ignorate practic de eventualii intruşi. Algoritmul se caracterizează printr-o robusteţe foarte bună a mesajului secret fiind dificil de deteriorat în cazul unor astfel de intenţii.

În cazul utilizării unui mesaj secret exprimat sub forma unei imagini alb-negru s-a dezvoltat un algoritm cu un grad ridicat de siguranţă privind încercările de recuperare neautorizată a informaţiei secrete. Algoritmul se bazează pe transformarea obiectului de acoperire folosind transformata Karthunen-Loeve într-un domeniu vectorial în vederea ascunderii unei informaţii secrete. Utilizând principiile enunţate în dezvoltarea modelului propus a fost concepută o soluţie de prelucrare a mesajului secret şi încorporarea acestuia în vectorii proprii corespunzători valorii proprii cu valoarea cea mai mică.

Este de remarcat faptul că procesul de încorporare a mesajului secret se efectuează după redistribuirea pixelilor acestuia pe baza unui algoritm pseudoaleator. În acest sens, doi pixeli vecini a căror probabilitate de a avea valori apropiate este foarte mare, vor fi distribuiţi în zone diferite ale obiectului de acoperire, ceea ce conduce la îmbunătăţirea semnificativă a obiectului steganografic. În urma acestor prelucrări urmează o transformare inversă din domeniul vectorial în domeniul spaţial obţinându-se obiectul steganografic propriu-zis. Pentru a asigura flexibilitate mărită a algoritmului, procesul de ascundere se efectuează în două variante, fiecare variantă depinzând de un coeficient ce poate fi ales aleator. Extragerea mesajului la recepţie de asemenea prezintă două variante, însă este de subliniat faptul că nu depind de modul în care a fost ascuns mesajul. Rezultă că acest algoritm poate prezenta o varietate mare de modalităţi de ascundere, ceea ce conferă un grad mare de incertitudine. În plus, recuperarea mesajului secret nu se poate realiza decât în cazul modalităţii de dispersie a acestuia. Multiplele incertitudini avansate prin acest algoritm permit să se facă afirmaţia că algoritmul prezintă un grad mare de siguranţă.

O comparaţie sintetică între toţi algoritmii dezvoltaţi şi utilizaţi în această lucrare se prezintă în tabelul 10.1 privind cantitatea de informaţie ascunsă raportată la mărimea obiectului de acoperire, respectiv calitatea obiectului steganografic exprimată faţă de obiectul de acoperire şi calitatea mesajului recuperat faţă de mesajul secret original.

Tabel 10.1 Comparaţie sintetică a algoritmilor steganografici

Nr.crt.	Nume algoritm	Cantitate informaţie ascunsă raportată la obiectul de acoperire	Calitate obiect steganografic	Calitate mesaj recuperat
1	$LSB - P_1$	12,5%	0,39%	0,39%
2	$LSB - P_2$	25%	1,17%	1,17%
3	$LSB - P_4$	100%	2,74%	2,74%
4	$YUV - P$	4%-10%	0,33%	0,33%
5	$BPCS$	31,42%	1,05%	1,7%
6	DCT	12,5%	2%	3%
7	SVD	6,25%	1,5%	3%
8	$ASAC$ pe 1 bit	29%	0,195%	0,8% - 1,67%
9	$ASAC$ pe 2 biţi	54%	0,5%	0,8% - 1,77%
10	$ASAC$ pe 4 biţi	101%	2,19%	0,8% - 1,77%
11	$ASAZ$	5%	0,8%	0,9%
12	$ASAC_{MS}$	33%	0,41% - 6,27%	1,2% - 35,21%

Concluzia care se poate desprinde în finalul acestei lucrări este faptul că pe baza principiilor enumerate la dezvoltarea unui model steganografic cu un grad ridicat de siguranţă prin care este implicată prelucrarea obiectului de acoperire şi a mesajului secret, a rezultat în obţinerea unui sistem steganografic superior din punct de vedere al siguranţei în funcţionare.

Pentru validarea practică a modelului teoretic propus au fost dezvoltaţi o serie de algoritmi în toate domeniile de reprezentare a imaginilor digitale. Folosind principiile desprinse din analiza modelului steganografic propus s-a constatat nu numai valabilitatea modelului, dar şi faptul că s-au obţinut algoritmi steganografici deosebiţi de performanţi. Mai mult, o parte dintre aceştia au fost adaptaţi pentru a fi implementaţi atât pe microprocesoare din clasa celor utilizate în prezent, respectiv în viitor în telefonia mobilă. Toate acestea au implicat o foarte bună valorificare a arhitecturilor microprocesoarelor utilizate în această lucrare, iar rezultatele experimentale au condus la obţinerea unor timpi de execuţie mult îmbunătăţiţi faţă de platformele clasice de calcul.

10.2 ***Contribuţii personale***

Pornind de la obiectivele şi scopul declarat ale acestei lucrări în continuare se prezintă principalele contribuţii originale:

- Elaborarea unei sinteze critice asupra stadiului actual al domeniului steganografiei.
- Elaborarea unui studiu şi a unei analize asupra problematicii de bază vizând mediile ce pot constitui obiecte de acoperire în steganografie, în vederea stabilirii celui mai potrivit dintre acestea în funcţie de capacitatea de încorporare a mesajelor secrete, respectiv detecţia şi robusteţea acestora.

- Elaborarea unei sinteze asupra principalelor caracteristici ale imaginilor digitale utilizate în această lucrare ca suport pentru ascunderea mesajelor secrete.
- Prezentarea sintetică pe baza caracteristicilor esenţiale ale principalelor domenii utilizate în steganografie de reprezentare ale imaginilor digitale.
- Analiza posibilităţilor de utilizare a unor microprocesoare caracteristice folosite în prezent, respectiv viitor în telefonia mobilă.
- Elaborarea unui studiu critic asupra modelelor steganografice existente.
- Propunerea unui nou model original steganografic pentru îmbunătăţirea siguranţei sistemelor steganografice.
- Demonstrarea teoretică din punct de vedere matematic a modelului steganografic propus privind îmbunătăţirea siguranţei acestuia.
- Dezvoltarea pe baza modelului propus a două variante originale de lucru în funcţie de obiectivele urmărite.
- Testarea şi validarea experimentală a celor două variante ale modelului steganografic propus.
- Dezvoltarea, testarea şi validarea adaptării algoritmilor steganografici bazaţi pe ascunderea datelor secrete în biţii cei mai puţini semnificativi ai obiectului de acoperire ?i implementarea originală pe două microprocesoare utilizate în telefonia mobilă în prezent, respectiv viitor.
- Dezvoltarea pe două microprocesoare a trei variante de lucru în ceea ce priveşte algoritmii steganografici bazaţi pe ascunderea datelor în cei mai puţini semnificativi biţi în funcţie de obiectivele urmărite.
- Analiza calitativă şi cantitativă a celor trei variante de lucru a algoritmilor steganografici bazaţi pe ascunderea datelor în cei mai puţini semnificativi biţi pentru trei platforme de lucru în vederea determinării timpului de execuţie cel mai mic.
- Conceperea, testarea şi validarea unui algoritm steganografic original bazat pe prelucrarea obiectului de acoperire în domeniul spaţial YUV şi ascunderea mesajului secret în biţii cei mai puţini semnificativi ai acestuia în vederea creşterii gradului de securitate şi a robusteţii mesajului secret.
- Adaptarea algoritmului steganografic bazat pe prelucrarea obiectului de acoperire în domeniul spaţial YUV ?i implementarea originală pe două microprocesoare utilizate în telefonia mobilă în prezent, respectiv viitor.
- Analiza calitativă şi cantitativă a algoritmului steganografic bazat pe prelucrarea obiectului de acoperire în domeniul spaţial YUV pentru trei platforme de lucru în vederea determinării timpului de execuţie cel mai mic.
- Implementarea, testarea şi validarea a câte unui algoritm steganografic pentru cele trei domenii de reprezentare ale imaginilor digitale prezentate în lucrare.
- Conceperea, testarea şi validarea unui algoritm original bazat pe prelucrarea mesajului secret prin comprimare şi ascunderea acestuia în biţii cei mai puţini semnificativi ai obiectului de acoperire.

- Adaptarea algoritmului steganografic bazat pe prelucrarea mesajului secret prin comprimare în trei variante de lucru pentru un microprocesor utilizat în prezent în telefonia mobilă.
- Analiza calitativă şi cantitativă a celor trei variante de lucru ale algoritmilor steganografici bazaţi pe prelucrarea mesajului secret prin comprimare, pe două platforme de lucru în vederea determinării timpului de execuţie cel mai mic.
- Conceperea, testarea şi validarea unui algoritm original bazat pe prelucrarea obiectului de acoperire şi a mesajului secret cu scopul ascunderii într-un zgomot artificial creat în vederea creşterii siguranţei sistemului steganografic.
- Conceperea, testarea şi validarea unui algoritm original bazat pe prelucrarea obiectului de acoperire şi ascunderea mesajului secret prin distribuirea aleatoare a acestuia în diferite zone ale obiectului de acoperire în vederea creşterii dificultăţii gradului de recuperare a informaţiilor încorporate de către persoane neautorizate.
- Dezvoltarea, testarea şi validarea a patru variante de lucru pentru algoritmul bazat pe distribuirea aleatoare a mesajului secret în vederea creşterii siguranţei sistemului steganografic.

10.3 ***Direcţii de cercetare generate de studiile efectuate***

Dintre principalele direcţii de cercetare ce pot continua rezultatele obţinute în cadrul acestei teze se pot enumera:

- Determinarea teoretică şi practică atât a funcţiei optime de prelucrare a obiectului de acoperire, cât şi a valorii acesteia.
- Determinarea teoretică şi practică a diferenţei optime dintre distribuţiile de probabilitate corespunzătoare obiectului steganografic, respectiv obiectului de acoperire. O diferenţă prea mică ar conduce la obţinerea unei distribuţii uniformă de probabilitate care nu ar mai permite încorporarea nici unei cantităţi de informaţie secretă. În cazul în care aceasta este prea mare există şansa ca mesajul secret să fie descoperit.
- În cazul algoritmului steganografic bazat pe prelucrarea obiectului de acoperire în domeniul spaţial YUV îmi propun să exploatez pentru ascunderea mesajului secret şi proprietăţile altor domenii de reprezentare ale imaginilor, cum ar fi utilizarea transformatei cosinus discrete specifică domeniului frecvenţă, respectiv transformata bazată pe descompunerea în valori singulare caracteristică domeniului vectorial.
- Optimizarea şi a celorlalţi algoritmi concepuţi în lucrarea de faţă în vederea adaptării acestora pentru implementarea pe microprocesoarele ce vor fi utilizate în telefonia mobilă, cu scopul de a obţine un grad mai ridicat de securitate.
- În continuare urmează să fie stabilit pe baza unor criterii clare, dar şi ţinând seama de costurile şi posibilităţile de integrare, respectiv şi de cerinţele pieţei din domeniu, care dintre algoritmii propuşi se încadrează cel mai bine spre a fi utilizat în continuare.

11 BIBLIOGRAFIE

[ABO08] Abolghasemi M., Aghainia H., Faez K., Mehrabi M.A. , "*Steganalysis of LSB Matching Based on Co-occurrence Matrix and Removing Most Significant Bit Planes*", Intelligent Information Hiding and Multimedia Signal Processing, 2008. IIHMSP '08 International Conference on, Harbin,15-17 Aug. 2008, pp 1527-1530, ISBN: 978-0-7695-3278-3

[AND05] Andre R.S.Marcal, Patricia R.Pereira, "*A Steganographic Method for Digital Images Robust to RS Steganalysis*"(book chapter), "Image analysis and recognition", 2005, pp. 1192-1199, ISBN 978-3-540-29069-8

[AGR09] Agrawal N., Gupta A., "*DCT Domain Message Embedding in Spread-Spectrum Steganography System*", HYPERLINK "/xpl/RecentCon.jsp?punumber=4976434"Data Compression Conference, 2009. DCC '09., 16-18 March 2009, pp. 433-433, Snowbird, UT, ISBN: 978-1-4244-3753-5

[BAB07] Babu V., Suresh S., Raja K. B. Uma, Maheshwar Rao K. Rashmi , K. A. Venugopal, K. R. Patnaik, " *Robust and high capacity image steganography using SVD* " , Information and Communication Technology in Electrical Sciences (ICTES 2007), 2007. ICTES. IET-UK International Conference on, Chennai, Tamilnadu, India, 20-22 Dec. 2007 , pp. 718-723, ISSN: 0537-9989

[BAO04] Bao P, Xiaohu Ma Nanyang, "*MP3-resistant music steganography based on dynamic range transform*", Technol. Univ., Singapore, Intelligent Signal Processing and Communication Systems, 2004. ISPACS 2004. Proceedings of 2004 International Symposium on, 2004, pp. 266 - 271, ISBN: 0-7803-8639-6

[BAR98] M. Barni, F. Bartolini, V. Cappellini and A. Piva, "*A DCT domain system for robust image watermarking"*, Signal Processing, vol. 66, no.3, pp. 257-372, 1998; XP004124957 ISSN: 0165-1684

[BAR00] Baruch Z. F., "*Sisteme de intrare ieşire ale calculatoarelor*", Editura Albastră, 2000, ISBN 973-9443-39-7

[BEE08] HYPERLINK "http://portal.acm.org/author_page.cfm?id=81350606032&coll=GUIDE&dl=GUIDE&trk=0&CFID=64680687&CFTOKEN=11715507" \t "_self"F. P. Beekhof, HYPERLINK

"http://portal.acm.org/author_page.cfm?id=81100552655&coll=GUIDE&dl=GUIDE&trk=0&CFID=64680687&CFTOKEN=11715507" \t "_self"S. Voloshynovskiy, HYPERLINK "http://portal.acm.org/author_page.cfm?id=81100612726&coll=GUIDE&dl=GUIDE&trk=0&CFID=64680687&CFTOKEN=11715507" \t "_self"O. Koval, HYPERLINK "http://portal.acm.org/author_page.cfm?id=81350605734&coll=GUIDE&dl=GUIDE&trk=0&CFID=64680687&CFTOKEN=11715507" \t "_self"R. Villan, HYPERLINK "http://portal.acm.org/author_page.cfm?id=81350590833&coll=GUIDE&dl=GUIDE&trk=0&CFID=64680687&CFTOKEN=11715507" \t "_self"E. Topak, *Document forensics based on steganographic anti-counterfeiting markings and mobile architectures,* Proceedings of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop,Adelaide, Australia, Art. No. 28, 2008, ISBN:978-963-9799-19-6

[BER05] Bertrand Anckaert, Bjorn De Sutter, Dominique Chanet, Koen De Bosschere, "*Steganography for Executables and Code Transformation Signatures*", Publisher, Springer Berlin / Heidelberg, Book Information Security and Cryptology – ICISC 2004, Vol. 3506/2005, Mai 24, 2005, ISBN 978-3-540-26226-8

[BOH04] Bohme Rainer, Westfeld Andreas, "*Breking Cauchy model-based JPEG steganography with first order statistics*", ESOROCS 2004, 13 Sept.France, vol. 3193, pp.125-140, ISBN: 3-540-22987-6

[BON07a] Boncelet C., Marvel L., "*Lossless Compression-Based Steganalysis of LSB Embedded Images"*, Information Sciences and Systems, 2007. CISS '07. 41st Annual Conference on, Baltimore, MD, 14-16 March 2007, pp. 923-923, ISBN: 1-4244-1037-1

[BON07b] Boncelet C., Marvel L., "*Steganalysis of Â±1 Embedding using Lossless Image Compression*", Image Processing, 2007. ICIP 2007. IEEE International Conference on, San Antonio, TX, Sept. 16 2007-Oct. 19 2007, Vol 2, pp. II - 149-II – 152, ISBN: 978-1-4244-1437-6

[BOR05] Borda Monica Elena, "*Teoria transmiterii informaţiei*", Editura DACIA, Cluj Napoca, 2005, ISBN: 973-35-0870-5

[BUD06] Budhia U., Kundur D., Zourntos T., "*Digital Video Steganalysis Exploiting Statistical Visibility in the Temporal Domain*", Information Forensics and Security, IEEE Transactionson on, 2006, Vol. 1, pp. 502-516

[BUR08] Wilhelm Burger, Mark J. Burger *„Digital Image Proocessing"*, ed.

Springer, 2008, pp. 5-36, 199-311, 367-373, ISBN: 978-1-84628-379-6

[CAH04] Cachin C.,"*An Information-Theoretic Model for Steganography*", Information and Computation, 2004, Vol.192, pp. 41-56, ISSN:0890-5401

[CAI07] Wei Cai B.E., " *FPGA Prototyping of a watermarking algorithm for MpPEG-4*", Thesis, University of North Texas, 2007

[CAN08] HYPERLINK "http://ieeexplore.ieee.org/search/searchresult.jsp?disp=cit&queryText=(candik%20%20m.%3cIN%3eau)&valnm=Candik%2C+M.&reqloc%20=others&history=yes"Candik M., HYPERLINK "http://ieeexplore.ieee.org/search/searchresult.jsp?disp=cit&queryText=(%20brechlerova%20%20d.%3cIN%3eau)&valnm=+Brechlerova%2C+D.&reqloc%20=others&history=yes"Brechlerova D., "*Digital watermarking in digital images",* HYPERLINK "http://ieeexplore.ieee.org/xpl/RecentCon.jsp?punumber=4747413"Security Technology, 2008. ICCST 2008. 42nd Annual IEEE International Carnahan Conference on**,** 13-16 Oct. 2008, pp. 43-46, ISBN: 978-1-4244-1816-9

[CHA04] Chandramouli Rajarathnam, Kharrazi Mehdi, Memon Nasir, "*Image steganography and steganalysis: Concepts and practice*", IWDW, Seoul, Coreea, vol 2939, pp. 35-49, 2004, ISBN: 3-540.21061-X

[CHA06a] Channgzoung XU, Xijian Ping, Tao Zhang, "*Steganography in Compressed Video Stream*", Proceedings of the First International Conference on Innovative Computing, Information and Control – Vol.1, pp. 269 – 272, 2006, ISBN:0-7695-2616-0

[CHA06b] Chang C-C., Chou H., Lin C-C., „*Colour image-hiding scheme using human visual system*", Imaging Science Journal, Oxford, UK, September 2006 , Vol54, Nr 3, pp. 152-163(12)

[CHA08] Chin-Chen Chanq, Zunq-Chen Chou, The Duc Kieu, "*An Information Hiding Scheme Using Sudoku*", ICICIC'08: Proceedings of the 2008 3rd nternational Conference on Inovative Computing Information and Control, Vol. 00, June 2008, IEEE Computer Society.

[CHE06] Po-Yueh Chen and Hung-Ju Lin, "*A DWT Based Approach for Image Steganography*", International Journal of Applied Science and Engineering, Taiwan,2006, vol 3 pp. 275-290, ISSN 1727-2394

[CHE08a] Chang-Chu Chen, Chin-Chen Chang, "*LSB-Based Steganography Using Reflected Gray Code*", IEICE-Transactions on Information and

Systems, Vol. E91-D, Issue4, April 2008, ISSN: 0916-8532

[CHE08b] Cheddad A.Condell, J.Curran, K.McKevitt, "*Biometric Inspired Digital Image Steganography*", Engineering of Computer Based Systems, 2008. ECBS 2008. 15th Annual IEEE International Conference and Workshop on the, Belfast, March 31 2008-April 4 2008, pp.159-168, ISBN: 0-7695-3141-5.

[CHI05a] Chin-Chen Chang, Chi-Lung Chiang, Ju-Yuan Hsiao ,"*A DCT-domain system for hiding fractal compressed images*", HYPERLINK "/xpl/RecentCon.jsp?punumber=9746"Advanced Information Networking and Applications, 2005. AINA 2005. 19th International Conference on, 28-30 March 2005 , pp. 83 - 86 vol.2, ISBN: 0-7695-2249-1

[CHI05b] Chi-Shiang Chan, Chin-Chen Chang, "*An Image Hiding Scheme Based on Multi-bit-reference Substitution Table Using Dynamic Programming Strategy*", Fundamenta Informaticae, 2005, Volume 65, pp. 291 - 305 , ISSN:0169-2968

[CHI08] Ching-Chiuan Lin, Nien-Lin Hsueh, "*A lossless data hiding scheme based on three-pixel block differences*", Elsevier Science Inc. New York, NY, USA,Vol. 41, pp. 1415-1425, 2008, ISSN:0031-3203

[CHI09] Chia-Chen Lin ,Pei Feng Shiu*, "DCT-based reversible data hiding scheme",* Conference On Ubiquitous Information Management And Communication Proceedings of the 3rd International Conference on Ubiquitous Information Management and Communication,Suwon, Korea, pp. 327-335 , 2009, ISBN:978-1-60558-405-8

[CHO06] Chang C-C.; Chou H.; Lin C-C., „*Colour image-hiding scheme using human visual system*", Imaging Science Journal, September 2006 , Vol54, Nr 3, pp. 152-163(12)

[CHO08] Yung-Chen Chou, Chin-Chen Chang, Kuan-Ming Li, "*A Large Payload Data Embedding Technique for Color Images* " , Fundamenta Informaticae, IOS Press, 2008, Vol 88, Number 1-2 / 2008, pp. 47-61, ISSN 0169-2968

[CHR06] Christian Kratzer, Jana Dittmann , Andreas Lang , Tobias Kühne "*WLAN steganography: a first practical review*", International Multimedia Conference, Proceeding of the 8th workshop on Multimedia and security , Geneva, Switzerland, 2006, pp. 17 – 22, ISBN:1-59593-493-6

[CHU01] Chun-Hsien Chou and Tung-Lin Wu, "*Embedding color watermarks in color images*", EURASIP Journal on Applied Signal Processing, vol. 1,

pp. 327-332, 2001, ISBN: 0-7803-7025-2

[CIU71] Ciucu G., Craiu V.,*"Introducere în teoria probabilităţilor şi statistică matematică",* Editura Didactică şi Pedagogică, Bucureşti, 1971

[COL03] Eric Cole,*"Hiding in Plain Sight:Steganography and the Art of Covert Communication*", Wily publishing, Inc,Indianapolis, Indiana, ISBN:0-471-44449-9

[CRU06] William A. Irizarry-Cruz, FPGA Implementation of a video watermarking algorithm, Thesis, University of Puerto Rico Mayaguez campus, 2006

[DAF03] Dafas P., Stathaki, T., *" Digital image watermarking using block-based Karhunen-Loeve transform*", Image and Signal Processing and Analysis, 2003, ISPA 2003, Proceedings of the 3rd International Symposium, 18-20 Sept. 2003, pp. 1072 – 1075, Vol.2, ISBN: 953-184-061-X

[DEE03] Deepa Kundur, *"Practical internet steganography: data hiding in IP*", in IP, Proceedings of the Texas Workshop on Security of Information Systems, April 2 nd , 2003

[DUT05] Sorin Duta, Mihai Mitrea, Françoise Prêteux, *"Informed watermarking for low rate video*", Proceedings of the 9th WSEAS International Conference on Communications, Athens, Greece, Article No. 69, 2005, ISBN:960-8457-29-7

[EFF03] Michelle Effros, Hanying Feng, Kenneth Zeger, "*Suboptimality of the Karhunen-Loeve Transform for Transform Coding*", Proceedings of Data Compression Conference(DCC '03), 2003

[EIS00] Eisenring M., Platzner M.,*"Synthesis of interfaces and communication in reconfigurableembedded systems*", Computers and Digital Techniques, IEE Proceedings, May 2000, Vol 147, Issue: 3, pp 159-165, ISSN: 1350-2387

[ELT07] Elhadedy M.E., Madian A.H., Saleh H.I., Ashour M.A. Aboelsaud, "*Hardware implementation of the encoder modified mid-band exchange coefficient technique (MMBEC) based on FPGA*" , Microelectronics, 2007. ICM 2007. Internatonal Conference on, Cairo, 29-31 Dec. 2007, pp. 43-46, ISBN: 978-1-4244-1846-6

[ERF09] Yousof Erfani, Shadi Siahpoush, "*Robust audio watermarking using improved TS echo hiding*", Digital Signal Processing, Vol.19, Issue 5, pp. 809-814, Sept 2009, Orlando, Florida, SUA, ISSN: 1051-2004

[FAR04] Hala Farouk, Magdi Saeb, "*Design and implementation of a secret key steganographic micro architecture employing FPGA*", Design, Automation and Test in Europe Conference and Exhibition, 2004.

Proceedings, 16-20 Feb. 2004, Vol.3, pp. 212-217, ISSN:1530-1591, ISBN: 0-7695-2085-5

[FAR05] Hala Farouk, Magdy Saeb, "*An improved FPGA implementation of the modified hybrid hiding encryption algorithm (MHHEA) for data communication security*", Proceeding of the Design, Automation and Test in Europe, March 2005, pp. 76-81, Vol. 3, ISSN: pp.1530-1591, 2005, ISBN: 0-7695-2288-2

[FEG02] George R. Fegan, "*Issue in SBRA: the Simulation of Correlated Random Variables Using the Karhunen-Loeve Transform(KLT)*", Euro SiBRAM, Prague, 24-26 June 2002, Session 2.

[FEN02] Feng H., Effros M. , "*On the rate-distortion performance and computational efficiency of the Karhunen-Loeve transform for lossy data compression*", Image Processing, IEEE Transactions on , Feb. 2002 , Vol 11 , Issue: 2 , pp. 113 - 122 ,ISSN: 1057-7149

[FER08] Ferreira R., Ribeiro B., Silva C., Qingzhong Liu Sung A.H., "*Building resilient classifiers for LSB matching steganography*" ,Neural Networks, 2008. IJCNN 2008. (IEEE World Congress on Computational Intelligence). IEEE International Joint Conference on, Hong Kong, 1-8 June 2008, pp. 1562-1567, ISBN: 978-1-4244-1820-6

[FRA04] Elke Franz, Antje Schneidewind, *Adaptive steganography based on dithering*, IMC Proceedings of the 2004 workshop on Multimedia and security, Magdeburg, Germany, pp.56-62, ISBN: 1-58113-854-7

[FRI08] Fritsch L., "*Low bitrate video coding using Karhunen- Loeve transform*"**,** Radioelektronika 2008 18th International Conference , 24-25 April 2008, pp.1 – 4,Prague, ISBN: 978-1-4244-2087-2

[FRU05] Clemens Fruhwirth,"*New Methods in Hard Disk Encryption",* Institute for Computer Languages, Vienna University of Technology, Cap.3, Jul 18, 2005

[FUR03] Furuta T., Noda H., Niimi M., Kawaguchi E., "*Bit-plane decomposition steganography using wavelet compressed video*", Information, Communications and Signal Processing, 2003 and the Fourth Pacific Rim Conference on Multimedia, Proceedings of the 2003 Joint Conference of the Fourth International Conference, 15-18 Dec. 2003, pp. 970 – 974, vol.2, ISBN: 0-7803-8185-8

[GAS06] Michael Gastpar, Pier Luigi Dragotti, Martin Vetterli, "*The Distributed Karthunen- Loeve Transform*", IEEE Transactions on Information Theory, Vol.52, NO.12, December 2006, pag.512, ISBN: 0018-9448

[GOM08] Gomez-Hernandez E., Feregrino-Uribe C., Cumplido R., "*FPGA Hardware Architecture of the Steganographic ConText Technique*", Electronics, Communications and Computers, CONIELECOMP 2008,

18th International Conference on, Puebla, 3-5 March 2008, pp. 123-128, ISBN: 978-0-7695-3120-5

[GOR03] Vladimir Gorodetsky, Vladimir Samoilov, "*Simulation-Based Exploration of SVD-Based Technique for Hidden Communication by Image Steganography Channel"*, Lecture Notes in Computer Science, Springer Berlin / Heidelberg , 2003, Vol 2776/2003, pp. 349-359, ISBN 978-3-540-40797-3

[GUI99] Gui Vasile, Lacrama Dan, Pescaru Dan, "*Prelucrarea imaginilor"*, Ed. Politehnica, 1999, Timisoara

[GUL06] Gul G., Dirik A.E., Avcibas I., „Steganalysis of Perturbed Quantization",Signal Processing and Communications Applications, 2006 IEEE 14th, Antalya, 17-19 April 2006, pp. 1-4, ISBN: 1-4244-0238-7.

[GUL07a] Gökhan Gül, Ahmet Emir Dirik, and ˙Ismail Avcıbas¸, Member, IEEE, "*Steganalytic Features for JPEG Compression-Based Perturbed Quantization*", IEEE SIGNAL PROCESSING LETTERS, MARCH 2007,VOL. 14, NO. 3, Digital Object Identifier 10.1109/LSP.2006.884010

[GUL08a] Gul G., Kurugollu F., "*Detection of watermarking methods using Steganalysis*", Acoustics, Speech and Signal Processing, 2008. ICASSP 2008. IEEE International Conference on, Las Vegas, NV, March 31 2008-April 4 2008, pp. 1725-1728, ISBN: 978-1-4244-1483-3

[GUL08b] Gul G., "*Spatial domain universal steganalysis based on singular value decomposition*", Signal Processing, Communication and Applications Conference, 2008. SIU 2008. IEEE 16th, Aydin, 20-22 April 2008, pp. 1-4, ISBN: 978-1-4244-1998-2.

[HEI92] Heilmeier G.H., "*Global' begins at home*", HYPERLINK "http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=35"Communications Magazine, IEEE,Vol.30, HYPERLINK "http://ieeexplore.ieee.org/xpl/tocresult.jsp?isnumber=4218&isYear=1992"Issue:10,pp.50-56,1992,ISSN:0163-6804

[HER 06] G. Gomez- Herrero, I. Jekova, V Krasteva, I Christov, A. Gotchev, K. Egiazarian, "*Relative Estimation of the Karhunen-Loeve Transform Basis Functions for Detection of Ventricular Ectopic Beats*", Computers in Cardiology, 2006, Vol 33, pp. 569-572, ISSN 0276-6547

[HOG06] S.G.Hoggar, "*Mathematics of Digital Images*", Cambridge University Press, 2006, ISBN-13 9780521780292

[HON04] Hong Heather Yu, Peng Yin, Xiaolong Yu, "*Joint content*

authentication and error control for wireless multimedia communications", Consumer Communications and Networking Conference, CCNC 2004, First IEEE, 5-8 Jan. 2004, pp. 412- 417, ISBN: 0-7803-8145-9

[HUL08] Lingna Hu ,Lingge Jiang ,Chen He, "*A novel steganalysis of LSB matching based on kernel FDA in grayscale images*", Neural Networks and Signal Processing, 2008 International Conference on, Nanjing, 7-11 June 2008, pp. 556-559, ISBN: 978-1-4244-2310-1

[HYU06] Hyun Woo Cho, Ahn Woo Lee, Hua Jun Chi, Seung Won Song, Gyeong Su Gwon, Ju Sung Park, "*An ARM7 processor with the Modified Multiplier and The Flip-Flop Based Pipelines*", The 1st International Forum on Strategic Technology, pp.68-71, oct.2006, Ulsan

[JAE08] Jae-Gil Yu, Eun-Joon Yoon, Sang-Ho Shin, Kee-Young Yoo, "*A New Image Steganography Based on 2k Correction and Edge-Detection*", Information Technology: New Generations, 2008. ITNG 2008. Fifth International Conference on, Las Vegas, NV, 7-9 April 2008, pp .563-568, ISBN: 0-7695-3099-0

[JAI89] Anil K. JAIN, "*Fundamentals of Digital Image Processing*", Prentice Hall, Englewood Cliffs, California, NJo7632, 1989

[JOH01] Johnson N.F., Duric Z., Jajodia S., "*Information Hiding: Steganography and Watermarking – Attacks and Countermeasures*", Kluwer Academic Publishers, 2001, ISBN 0-7923-7204-2

[JUN02] Wu Zhi-Jun, Niu Xin-Xin, Yang Yi-Xian, "*Design of speech information hiding telephone*", TENCON '02. Proceedings. 2002 IEEE Region 10 Conference on Computers, Communications, Control and Power Engineering, 28-31 Oct. 2002, Volume: 1, pp. 113- 116 vol.1, ISBN: 0-7803-7490-8

[JUN03] Wu Zhi-Jun, Niu Xin-Xin, Yang Yi-Xian, "*Design of speech information hiding telephone*", TENCON '02, Proceedings 2002 IEEE Region 10 Conference on Computers, Communications, Control and Power Engineering, 28-31 Oct. 2002, Vol. 1, pp. 113- 116, ISBN: 0-7803-7490-8

[JUN08] Ki-Hyun Jung, Kyeoung-Ju Ha, Kee-Young Yoo, " *Image Data Hiding Method Based on Multi-Pixel Differencing and LSB Substitution Methods*" , Convergence and Hybrid Information Technology, 2008. ICHIT '08. International Conference on , Daejeon, 28-30 Aug. 2008, pp. 355-358, ISBN: 978-0-7695-3328-5

[KAM95] Kamata S, Eason R.O., Kawaguchi E., "*Depth-First Coding for multi-valued pictures using bit-plane decomposition*", IEEE Trans. on Comm., vol. 43, no. 5, pp. 1961-1969, 1995

[KAT00] Stefan Katzenbeisser, Fabien A. P. Petitcolas, "*Information hiding techniques for steganography and digital watermarking*", 2000, ISBN 1-58053-035-4

[KAW02] Kawaguchi E., Eason R., "*Large Capacity Steganography*," U.S. Patent no. 6,473,516, Oct. 29, 2002

[KAW86] Kawaguchi E., Taniguchi R., "*Complexity of binary pictures and image thresholding – An Application of DF-Expression to the thresholding problem*", Proceedings of 8th ICPR, vol.2, pp. 1221-1225, 1986

[KAW89] Kawaguchi E., Taniguchi, R., "*The DF-Expression as an image thresholding strategy*", IEEE Trans. on SMC, vol. 19, no. 5, pp. 1321-1328, 1989

[KAW98] Kawaguchi E., Eason R. "*The Principle and Applications of BPCS-Steganography*", SPIE International Symposium on Voice, Video and Data Communications: Multimedia Systems and Aplications, pp. 464-473, Boston, MA, Noiembrie 2-4, 1998

[KEJ04] Arun Kejariwal, Sumit Gupta, Alexandru Nicolau, Nikil Dutt, Rajesh Gupta, "*Proxy-based task partitioning of watermarking algorithms for reducing energy consumption in mobile devices*", Annual ACM IEEE Design Automation Conference Proceedings of the 41st annual conference on Design automation, San Diego, CA, USA, 2004, pp. 556 - 561, ISBN:1-58113-828-8

[KEJ05] Kejariwal A., Gupta S., Nicolaut A., Dutt N., Gupta R., *"Energy analysis of multimedia watermarking on mobile handheld devices"*, Embedded Systems for Real-Time Multimedia, 2005 3rd Workshop on, 22-23 Sept. 2005, pp. 33- 38, ISBN: 0-7803-9347-3

[KER05] Kermani Z.Z., Jamzad M., "*A robust steganography algorithm based on texture similarity using Gabor filter*" , Signal Processing and Information Technology, 2005. Proceedings of the Fifth IEEE International Symposium on, Athens, 21-21 Dec. 2005, pp. 578-582, ISBN: 0-7803-9313-9

[KER08] Andrew D. Ker, "*Locating steganographic payload via ws residuals*" , International Multimedia Conference Proceedings of the 10th ACM workshop on Multimedia and security ,Oxford, United Kingdom, 2008,Pp 27-32 , ISBN:978-1-60558-058-6

[KES04] HYPERLINK "mailto:gary.kessler@champlain.edu"Gary C. Kessler, "*An Overview of Steganography for the Computer Forensics Examiner*", HYPERLINK "http://www.fbi.gov/hq/lab/fsc/backissu/july2004/research/2004_03_research01.htm"Forensic Science Communications, July 2004, *Computer &* Digital Forensics Program, Champlain College, Burlington, Vermont, *USA, 2004.*

[KHA06] Mehdi Kharrazi, Husrev T Sencar, Nasir Memon, "*Cover Selection for Steganographic Embedding*", ICIP 2006, IEEE International Conference on 8-11 Oct, 2006, pp. 117-120, ISBN: 1-4244-0481

[KHO09] Khosvirad S.R., Eghlidos T., Ghaemmaghami S., "*Higher-order statistical steganalysis of random LSB steganography*", HYPERLINK "/xpl/RecentCon.jsp?punumber=5010318"Computer Systems and Applications, 2009. AICCSA 2009 IEEE/ACS International Conference on 10-13 May 2009 , pp. 629 – 632, ISBN: 978-1-4244-3807-5

[KIM07] Younhee Kim, Zoran Duric, Dana Richards, *„Modified Matrix Encoding Technique for Minimal Distortion Steganography*", Lecture Notes in Computer Science, Berlin/Heidelberg, 2007, Vol 4437/2007, pp.314-327, ISBN 978-3-540-74123-7

[KRA07] Philipp K. Krause,"Texture Compression", pdf, 2007

[KOC95] Koch E, J. Zhao, "*Embedding Robust Labels into Images for Copyright Protection*", inProceedings of the International Conference on Intellectual Property Rights for information, Knowledge and New Techniques, Munchen, Wien, 1995, pp. 242-251

[KOK07] Koksheik Wong, Xiaojun Qi, Kiyoshi Tanaka, "*A DCT-based Mod4 steganographic method*", Signal Processing, pp.1251-1263, 2007, ISSN:0165-1684

[KUR92] C. Kurak , J. McHugh, *A Coutionary Note on Image* Dowmgranding In Computer Security Applications Conference, San Antonio, TX, USA, pp.153-159, Dec.1992

[LAC99] John Lach, William H. Mangione-Smith, Miodrag Potkonjak, "*Robust FPGA Intellectual Property Protection through multiple small watermarks*", *DAC 99: Proceedings of the 36 th ACM/ IEEE Conference on Design Automation, New Orleans, LA,* , June 1999, USA, pp. 831-836 ISBN: 1-58113-092-9

[LIU08] Chengjun Liu, "*Learning the Uncorrelated, Independent, and Discriminating Color Spaces for Face Recognition*" , Information Forensics and Security, IEEE Transactions on, June 2008, Vol 3, Issue: 2, pp. 213-222, ISSN: 1556-6013.

[LIX08] Xiaolong Li, Tieyong Zeng ,Bin Yang , "*Improvement of the embedding efficiency of LSB matching by sum and difference covering set*" , Multimedia and Expo, 2008 IEEE International Conference on, Hannover, June 23 2008-April 26 2008, pp 209-212,

ISBN: 978-1-4244-2570-9

[LON05] Ernesto Gomez Londono, Luis Castillo Lopez, Thais de Souza Kazmierczak, "*Using the Karhunen-Loeve Transform to Suppress Ground Roll in Seismic Data*", Earth sciences research journal, Dec 2005, vol9, p 139-147

[MAK98] Makoto Matsumo, Takuji Nishimura, **„** *Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator*", ACM Transactions on Modeling and Computer Simulation TOMACS ,1998, Vol 8, pp. 3-30, ISSN:1049-3301

[MAT94] Matsui K, Tanaka K, "*Video-Steganography: How Secretly Embed a Signature in a Picture",* IMA Intellectual Property Project Proceedings, vol1, no1, 1994, pp.187-205

[MAT06] Matsuoka H., NTT DoCoMo, "*Spread Spectrum Audio Steganography Using Sub-band Phase Shifting*", Intelligent Information Hiding and Multimedia Signal Processing, 2006. IIH MSP '06. International Conference on , USA, pp. 3 - 6, ISBN: 0-7695-2745-0

[MAZ06] W. Mazurczyki, Z. Kotulski, "*New security and control protocol for VoIP based on steganography and digital watermarking*", Annales UMCS, Informatica, AI 4 (2006), ISNN 1732-1360

[MAZ08] Wojciech Mazurczyk, Krzysztof Szczypiorski, "*Steganography of VoIO Streams*", Lecture Notes In Computer Science, Vol.5332 Proceedings of the OTM 2008 Confederated International Conferences, 2008, Monterrey, Mexico, pp. 1001-1018, ISBN:978-3-540-88872-7

[MIE06] Mielikainen J., *„LSB matching revisited*", Signal Processing Letters, May 2006, Vol13, Issue: 5, pp 285- 287, ISSN: 1070-9908

[MEH08] Mehrabi M.A., Aghaeinia H., Abolghasemi M., "*Steganalysis of LSB-Matching steganography by removing most significant bit planes*", Telecommunications, 2008. IST 2008. International Symposium on, Tehran, 27-28 Aug. 2008, pp 731-734, ISBN: 978-1-4244-2750-5

[MOH05] Saraju P. Mohanty, Nagarajan Ranganathan, Ravi K. Namballa, "*VLSI Architecture for watermarking in a secure still digital camera (* QUOTE S^2 S^2 *DC) design* ", IEEE Transactions on very large scale integration (VLSI) systems, Vol 13, Issue 7, July 2005, ISSN: 1063-8210

[MOH07] Mohanty S.P., Kougianos E., Ranganathan N. ,"*VLSI architecture and chip for combined invisible robust and fragile watermarking*", Computers & Digital Techniques, IET, Sept. 2007, Vol 1, Issue: 5, pp. 600-611, ISSN: 1751-8601

[MOH08] B. Chandra Mohan, S. Ssrinivaskumar, B.N. Chatterji, "*A robust Digital Image Eatermarking Scheme using Singular Value*

Decomposition (SVD), Dither Quantization and Edge Detection", ICGST_GVIP Journal, Issue 1, June 2008, pp.17-23 ISSN: 1687-398X

[MOS01] Ira S. Moskowitz, Garth E Longdon, LiWu Chang, " *A new paradigm hidden in steganography*", New Security Paradigms Workshop, Proceedings of the 2000 workshop on New security paradigms, Ballycotton, Ireland, pp. 41-50, 2001, ISBN: 1-58113-260-3

[MOU03] HYPERLINK "http://ieeexplore.ieee.org/search/searchresult.jsp?disp=cit&queryText=(moulin%20%20p.%3cIN%3eau)&valnm=Moulin%2C+P.&reqloc%20=others&history=yes"Moulin P. HYPERLINK "http://ieeexplore.ieee.org/search/searchresult.jsp?disp=cit&queryText=(%20ivanovic%20%20a.%3cIN%3eau)&valnm=+Ivanovic%2C+A.&reqloc%20=others&history=yes"Ivanovic A. , "*The zero-rate spread-spectrum watermarking game"*, HYPERLINK "http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=78"Signal Processing IEEE Transactions on, Apr 2003, Vol. 51, HYPERLINK "http://ieeexplore.ieee.org/xpl/tocresult.jsp?isnumber=26657&isYear=2003"Issue: 4, pp. 1098- 1117, ISSN: 1053-587X

[NAV08] Navas K.A., Ajay M.C., Lekshmi M. Archana, T.S. Sasikumar, "*DWT-DCT-SVD based watermarking*", Communication Systems Software and Middleware and Workshops, 2008. COMSWARE 2008. 3rd International Conference on, Bangalore, 6-10 Jan. 2008, pp. 271-274, ISBN: 978-1-4244-1796-4

[NED04] Nedeljko Cvejic, Tapio Seppanen, *„Increasing robustness of LSB audio steganography using a novel embedding method*", Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. International Conference on, 2004, Vol. 2, pp. 533 – 537, ISBN: 0-7695-2108-8

[NOD02a] HYPERLINK "http://ieeexplore.ieee.org/search/searchresult.jsp?disp=cit&queryText=%28noda%20%20h.%3Cin%3Eau%29&valnm=Noda%2C+H.&history=yes"Noda H., HYPERLINK "http://ieeexplore.ieee.org/search/searchresult.jsp?disp=cit&queryText=%28%20spaulding%20%20j.%3Cin%3Eau%29&valnm=Spaulding%2C+J.&history=yes"Spaulding J., HYPERLINK "http://ieeexplore.ieee.org/search/searchresult.jsp?disp=cit&queryText=%28%20shirazi%20%20m.n.%3Cin%3Eau%29&valnm=Shirazi%2C+M.N.&history=yes"Shirazi M.N., HYPERLINK

"http://ieeexplore.ieee.org/search/searchresult.jsp?disp=cit&queryText=%28%20kawaguchi%20%20e.%3Cin%3Eau%29&valnm=Kawaguchi%2C+E.&history=yes"Kawaguchi E., "*Application of bit-plane decomposition steganography to JPEG2000 encoded images*", HYPERLINK "http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=97"Signal Processing Letters, IEEE, Dec. 2002, pp. 410 – 413, ISSN: 1070-9908

[NOD02b] Noda H., Spaulding J., Shirazi M.N., Niimi M., Kawaguchi E.,"*Application of bit-plane decomposition steganography to wavelet encoded images*" Image Processing 2002, Proceedings 2002 International Conference, 22-25 Sept. 2002 , pp. II-909 - II-912 vol.2, ISBN: 0-7803-7622-6

[NOD04] Noda H., Furuta T., Niimi M., Kawaguchi E., "*Application of BPCS steganography to wavelet compressed video*", Image Processing, 2004, ICIP '04. 2004 International Conference, 24-27 Oct. 2004, pp. 2147 – 2150, Vol. 4, ISBN: 0-7803-8554-3

[NII02a] Niimi M., Noda H., Kawaguchi E., Eason R.O, " *Luminance quasi-preserving color quantization for digital steganography to palette-based images*", Pattern Recognition, 2002, Proceedings 16th International Conference, 11-15 Aug. 2002, pp. 251 – 254, vol.1, ISBN: 0-7695-1695-X

[NII02b] Niimi M, Noda H., Kawaguchi E, Eason R.O., "*High capacity and secure digital steganography to palette-based images* ", Image Processing 2002, Proceedings 2002 International Conference, 22-25 Sept 2002, pp. 917-920, vol 2, ISBN: 0-7803-7622-6

[NII04] Niimi M., Ei T., Noda H., Kawaguchi E., Segee, B, "*An attack to BPCS-steganography using complexity histogram and countermeasure*", Image Processing, 2004. ICIP '04. 2004 International Conference on, 24-27 Oct. 2004,Vol2, pp. 733- 736 Vol.2, ISBN: 0-7803-8554-3

[OGI96] Ogihara T., Nakamura D.,Yokoya N., "*Data embedding into pictorial images*", Pattern Recognition, 1996., Proceedings of the 13th International Conference on, 25-29Aug1996, Vol.2, pp. 675-679, Austria, ISBN: 0-8186-7282-X

[OWE02] Mark Owens, "*Disscusion of Covert Channels and Steganography*", Information Security, SANS Institute, 2002

[PET05] Mihai Petrescu, Mihai Mitrea, Françoise Prêteux, "*Spread spectrum watermarking for low rate video*", Proceedings of the 9th WSEAS International Conference on Communications, Athens, Greece,

Article No. 66, 2005, ISBN:960-8457-29-7

[PET07] Emilia Petrişor," *Probabilităţi şi statistică. Aplicaţii în economie şi inginerie*", Editura "Politehnica" Timişoara, 2007, ISBN 947-625-210-8

[PIV00] Piva A., Bartolini F., Boccardi L., Cappellini V., De Rosa A., Barni M., "*Watermarking through color image bands decorrelation*", HYPERLINK "http://ieeexplore.ieee.org/xpl/RecentCon.jsp?punumber=6974" Multimedia and Expo, 2000, ICME 2000, IEEE International Conference on**,** 30 July-2 Aug. 2000, pp. 1283 - 1286 vol.3, New York,ISBN: 0-7803-6536-4

[PIY04] Piyu Tsai, Yu-Chen Hu, and Chin-Chen Chang, "*A color image watermarking scheme based on color quantization*," Signal Processing, vol. 84, pp. 95-106, 2004, ISSN:0165-1684

[POO07] Pooyan, Mohammad Delforouzi, Ahmad," LSB-based "*Audio SteganographyMethod Based on Lifting Wavelet Transform*", Signal Processing and Information Technology, 2007 IEEE International Symposium on, Egypt , pp. 600 – 603, ISBN: 978-1-4244-1835-0

[POR08] L. Y. Por ,W. K. Lai ,Z. Alireza, B. Delina, " *StegCure: an amalgamation of different steganographic methods in GIF image*" , Recent Advances In Computer Engineering Proceedings of the 12th WSEAS international conference on Computers , Heraklion, Greece, 2008, pp. 420-425, ISBN ~ ISSN:1790-5109 , 978-960-6766-85-5

[PRA72] William K. Pratt, "*Generalized Wiener Filtering Computation Techniques*", IEEE Transactions on Computers, July 1972, Vol C-21, No. 7

[RAF07] Rafael C Gonzales, Richard Eugene Woods, "*Digital Image Processing*", 2007, Publicată de Prentice Hall, 2007, ISBN 013168728X, 9780131687288

[RAJ05] Raja K.B., Chowdary C.R., Venugopal K.R., Patnaik, "*A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images* ", Intelligent Sensing and Information Processing, 2005. ICISIP 2005. Third International Conference on, 14-17 Dec. 2005, pp. 170- 176, ISBN: 0-7803-9588-3

[RON06] Rongrong Ji, Hongxun Yao, Shaohui Liu, Liang Wang, "*Genetic Algorithm Based Optimal Block Mapping Method for LSB Substitution*" , iih-msp, International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'06), 2006, pp.215-218

[RUF04] Rufeng Chu, Xinqqanq Xiaohui Ba,"*A DCT-based image*

steganographic method resisting statistical attacks", HYPERLINK "/xpl/RecentCon.jsp?punumber=9248"Acoustics, Speech and Signal Processing, 2004. Proceedings (ICASSP '04) IEEE International Conference on, 17-21 May 2004, pp. V - 953-6 vol.5, ISBN: 0-7803-8484-9

[SAL08] Saleh R.H.I.,*"Efficient Mid-band Exchange Coefficient Watermarking System"*, Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. 3rd International Conference on, Damascus, 7-11 April 2008, pp. 1-5, ISBN: 978-1-4244-1751-3

[SAJ08] Hedieh Sajedi Jamzad, "*Cover Selection Steganography Method Based on Similarity of Image Blocks*", Computer and Information Technology Workshops, 2008. CIT Workshops 2008. IEEE 8th International Conference on, Sydney, QLD, 8-11 July 2008, pp 379-384, ISBN: 978-0-7695-3242-4

[SAR07] Sarkar A., Manjunath B.S., "*Estimating Steganographic Capacity for Odd-Even Based Embedding and its Use in Individual Compensation*" ,Image Processing, 2007. ICIP 2007. IEEE International Conference on, San Antonio, TX, Sept. 16 2007-Oct. 19 2007,Vol1, pp. I - 409-I – 412, ISBN: 978-1-4244-1437-6

[SCH01] Gerhard Schmid, Final REPORT on the existence of a global system for interception of private and commercial communications (ECHELON interception system), (2001/2098) (INI), EUROPEAN PARLIAMENT 1999-2004, A5-0264/2001, PAR1, 11 July 2001, RR/445698EN.doc

[SHA01] Linda G. Shapiro, George C. Stockman *„Computer Vision*" ed Prentice Hall, 2001, pp.35-40, 254-277. ISBN:0-13-030796-3

[SHA05] Mohammad Shirali Shahreza, "*An improved method for steganography on mobile phone*", Proceedings of the 9th WSEAS International Conference on Systems table of contents, Athens, Greece, 2005, Article No. 28 , ISBN:960-8457-29-7.

[SHA06a] Shahreza S., "*Stealth steganography in SMS*", Wireless and Optical Communications Networks, 2006 IFIP International Conference on, 2006, ISBN: 1-4244-0340-5

[SHA06b] Mohammad Shirali-Shahreza, "*Steganography in wireless application protocol*", International Association Of Science And Technology For Development Proceedings of the 24th IASTED international conference on Internet and multimedia systems and applications, Innsbruck, Austria, 2006, pp: 91 - 95 , ISBN:0-88986-564-7

[SHA06c] Shirali-Shahreza M., *"Java Applets Copy Protection by Steganography*", Intelligent Information Hiding and Multimedia

Signal Processing, 2006. IIHMSP'06, International Conference on, 2006, pp. 388-391, Pasadena, CA, USA, ISBN: 0-7695-2745-0

[SHI06d] Shirali-Shahreza M., "*A new method for Real Time Steganography*", Signal Processing, 2006 8th International Conference on, 2006,Volume: 4, Beijing, ISBN: 0-7803-9737

[SHA07a] Shirali-Shahreza, S. Manzuri-Shalmani, M.T.,"*Adaptive Wavelet Domain Audio Steganography with High Capacity and Low Error Rate*", Information and Emerging Technologies, 2007. ICIET 2007. International Conference on, Karachi, 6-7 July 2007, pp.1-5, ISBN: 978-1-4244-1247-1

[SHA07b] Shirali-Shahreza, M., Shirali-Shahreza, M.H, "*Text Steganography in SMS*", Convergence Information Technology, 2007. International Conference on, 21-23 Nov. 2007, ISBN: 0-7695-3038-9

[SHA08a] Shirali-Shahreza M., "*A simple method for detecting the possible changes of hidden information of watermarked image in an MMS message*", Biometrics and Security Technologies, ISBAST 2008, International Symposium on, Islamabad, 23-24 April 2008, pp. 1-4, ISBN: 978-1-4244-2427-6

[SHA08b] M. Hassan Shirali-Shahreza, Mohammad Shirali-Shahreza, "*Steganography in SMS by Sudoku puzzle*",AICCSA, Proceedings of the 2008 IEEE/ACS International Conference on Computer Systems and Applications, pp.844-847, 2008, ISBN:978-1-4244-1967-8

[SHI93] Lan Leu-Shing, Reed Irving S., "*Fast approximate Karhunen-Loeve Transform with applications to digital image coding*", Visual Communications and Image Processing '93, Proc. SPIE , 1993,Vol 2094, pp 444-455

[SIM84] Gustavus J. Simmons, „*The prisoners' problem and the subliminal channel*", Advances in Cryptology: Proceedings of Crypto 83 (David Chaum, ed.), Plenum Press, 1984, pp. 51-67

[SLO04] Andrew N. Sloss, Dominic Symes, Chris Wright John Rayfield, "*ARM system developer's guide*", Elsevier, 2004

[SRI04] Srinivasan Y., Nutter B., Mitra S., Phillips B., Ferris, D,"*Secure transmission of medical records using high capacity steganography*", Computer-Based Medical Systems, 2004. CBMS 2004. Proceedings. 17th IEEE Symposium on, 24-25 June 2004, pp. 122- 127, ISBN: 0-7695-2104-5.

[STA99] D. Stanomir, L. Tincu, "Acustică aplicată", Vol.1, "*Structuri şi sisteme mecano-acustice*", Casa de Editură Tincu şi Stanomir, Bucureşti, 1999

[STA07a] Stanescu D., Stratulat M., Ciubotaru B,. Chiciudean D, Cioarga R.,

Borca D, "*Digital Watermarking using Karhunen-Loeve transform*", 4th International Symposium on Applied Computational Intelligence and Informatics, 2007. SACI '07, 18 Mai 2007, pp. 187-190, Timisoara, Romania, ISBN:1-4244-1234X

[STA07b] Stanescu D., Stratulat M., Ciubotaru B., Chiciudean D., Cioarga, R., Micea, M.,"*Embedding Data in Video Stream using Steganography*", 4th International Symposium on Applied Computational Intelligence and Informatics, 2007. SACI '07. 18 Mai 2007, pp. 241-244, Timisoara, Romania, ISBN: 1-4244-1234-X

[STA07c] Stanescu D., Stratulat M., Groza V., Ghergulescu I., Borca D., "*Steganography in YUV color space*", Robotic and Sensors Environments, 2007. ROSE 2007. International Workshop on, 12-13 Oct. 2007, pp. 131-137 Ottawa, Canada, ISBN: 978-1-4244-1527-6

[STA08a] Stanescu D, Groza V, Stratulat M., Borca D., Ghergulescu I., "*Robust Watermarking with High Bit Rate*", Third International Conference on Internet and Web Applications and Services, 2008, ICIW2008, 8-13 iune 2008, Athena, Greece, pp. 257-260, 2008, ISBN: 978-0-7695-3163-2

[STA08b] Stanescu D., Borca D., Groza V., Stratulat M., *"A Hybrid Watermarking Technique Using Singular Value Decomposition"*HYPERLINK "http://ieeexplore.ieee.org/xpl/RecentCon.jsp?punumber=4662485", 2008. HAVE 2008. IEEE International Workshop on Haptic Audio visual Environments and their applications**,** 18-19 Oct. 2008, Ottawa, pp.166-170, ISBN:978-1-4244-2668-3

[STA09] D. Stănescu, V Stângaciu, I. Gergulescu, M. Stratulat*, "Steganography on embedded devices",* SACI, 2009 "Politehnica" University of Timişoara, România, pp.313-317, ISBN: 978-1-4244-4478-6

[STR03] G. Strang*," Introduction to Linear Algebra"*, Wellesley-Cambridge Press, 2003, (biblioteca UPT).

[SUK06] Suk-Ling Li, Kai-Chi Leung, L.M. Cheng, Chi-Kwong Chan, "*Data Hiding in Images by Adaptive LSB Substitution Based on the Pixel-Value Differencing*" , First International Conference on Innovative Computing, Information and Control , icicic, 2006, Vol. 3, pp.58-61

[SUN07] Hung-Min Sun, King-Hang Wang, Chih-Cheng Liang, Yih-Sien Kao, *"A LSB substitution compatible steganography*" ,TENCON 2007 - 2007 IEEE Region 10 Conference, Taipei, Oct. 30 2007-Nov. 2 2007, pp.1-3, ISBN: 978-1-4244-1272-3

[SUZ08] Genta Suzuki, Nobuyasu Yamaguchi, Shigeyoshi Nakamura, Hirotaka Chiba, "*Mobile interaction using steganographic image on mobile*

display", Mobile HCI September 2008, Amsterdam the Netherlands, pp. 505-510, ISBN 978-1-59593-952-4/08/09

[TAC04] Tachibana T., Fujiyoshi M., Kiya H., "*An image-quality guaranteed watermarking scheme with spreading spectrum of watermark*", Communications and Information Technology, 2004. ISCIT 2004. IEEE International Symposium on, 26-29 Oct. 2004,Volume: 1, pp. 330- 334 vol.1, ISBN:0-7803-8593-4

[TAN08] He Junhui Tang, Shaohua Wu Tingting, "*On the Security of Steganographic Techniques*", Image and Signal Processing, 2008. CISP '08. Congress on, Sanya, China, 27-30 May 2008, Vol 5, pp: 716-719, ISBN: 978-0-7695-3119-9

[TOR06] Torres-Maya S., Nakano-Miyatake M., Perez-Meana H, "*An Image Steganography Systems Based on BPCS and IWT*", Electronics, Communications and Computers, 2006, CONIELECOMP 2006. 16th International Conference ,27-01 Feb. 2006, pp: 51 – 51,ISBN: 0-7695-2505-9

[TRE05] Trevor Martin., *The Insider's Guide To The Philips ARM7-Based Microcontrollers, An Engineer's Introduction to the LPC2100 Series*, 2005, Hitex Ltd, ISBN:0-95499881

[UNS 84] Michael Unser, "*On the Approximation of the Discrete Karhunen-Loeve Transform for Stationary Processes*", Signal Processing Laboratory, Swiss Federal Institute of Technology, 16 Ch. De Bellerive, Switzerland, Elsevier Science Publishers, 19 July 1984, Vol 7, pp 231-249, ISSN 0165-1684

[WAR97] Waldemar P., Ramstad T.A., "*Hybrid KLT-SVD image compression*", HYPERLINK "http://ieeexplore.ieee.org/xpl/RecentCon.jsp?punumber=4635"Acoustics, Speech and Signal Processing, ICASSP-97, 1997 IEEE International Conference, 21-24 April 1997, pp. 2713 – 2716, vol.4, 04/21/1997 - 04/24/1997, Munich, ISBN: 0-8186-7919-0

[WAT08] Paul Watters , Frances Martin,H. Steffen Stripf , "*Visual detection of LSB-encoded natural image steganography*" ,ACM Transactions on Applied Perception (TAP), 2008 ,Vol 5 , Issue 1, Article No. 5, ISSN:1544-3558

[WUZ96] Zi-Long Wu , "*Reversible Data Hiding Based on KLT Feature Points*", Thesis Search, 1996

[XIA08c] Xiaoyi Yu, Babaguchi, N.," *Breaking the YASS algorithm via pixel and DCT coefficients analysis*", Pattern Recognition, 2008. ICPR 2008. 19th International Conference on, Tampa, FL, 8-11 Dec. 2008, pp 1-4,ISBN: 978-1-4244-2174-9

[XIA08a] Xiaoyi Yu Babaguchi, N. ,"*Run length based steganalysis for LSB matching steganography*" HYPERLINK "/xpl/RecentCon.jsp?punumber=4599583"Multimedia and Expo, 2008 IEEE International Conference, June 23 2008-April 26 2008 ,pp. 353 - 356, Hannover, ISBN: 978-1-4244-2570-9

[XIA08b] Xiaolong Li Tieyong Zeng Bin Yang ," *Improvement of the embedding efficiency of LSB matching by sum and difference covering set*", HYPERLINK "/xpl/RecentCon.jsp?punumber=4599583"Multimedia and Expo, 2008 IEEE International Conference on, June 23 2008-April 26 2008 , pp. 209 - 212 , Hannover ISBN: 978-1-4244-2570-9

[XUB07] Xu Bo; Wang Jia-zhen; Peng De-yun, "*Practical Protocol Steganography*: *Hiding Data in IP Header*", Modelling & Simulation, 2007, AMS apos; 07. First Asia International Conference on, 27-30 March 2007, pp. 584 – 588, D.O.0.1109/AMS.2007.80

[YAH08] Ching-Yu Yang , Wu-Chih Hu ,Jen-Yuan Lai, *"DCT-Based Watermarking By Quotient-Embedding Algorithm*", Innovative Computing Information and Control, 2008. ICICIC '08. 3rd International Conference on, Dalian, Liaoning, 18-20 June 2008,pp 20-20, ISBN: 978-0-7695-3161-8

[YAN01] Dai Yang, Hongmei Ai, Chris Kyriakakis, C.C. Jay Kuo, "*Adaptive Karhunen-Loeve Transform for Enhanced Multichannel Audio Coding* ", Integrated Media Systems Center, 2001.

[YAN08] Cheng-Hsing Yang ,Chi-Yao Weng ,Shiuh-Jeng Wang ,Hung-Min Sun, "*Adaptive Data Hiding in Edge Areas of Images With Spatial LSB Domain Systems*" , Information Forensics and Security, IEEE Transactions on, Sept. 2008, Vol 3, Issue: 3, pp 488-497,ISSN: 1556-6013

[YAV07] Erkan Yavuz , Ziya Telatar ,"*Improved SVD-DWT based digital image watermarking against watermark ambiguity*", Symposium on Applied Computing Proceedings of the 2007 ACM symposium on Applied computing Seoul, Korea , Multimedia and visualization track table of contents, 2007, pp. 1051 – 1055, ISBN:1-59593-480-4.

[YUA07] Yuan-Hui Yu, Chin-Chen Chang, Iuon-Chang Lin, "*A new steganographic method for color and grayscale image hiding*", Elsevier Science Inc. New York, NY, USA, Vol. 107, pp. 183-194, 2007, ISSN:1077-3142

[YUC06] Yu-Chen Hu, "*Multiple Images Embedding Scheme Based on Moment Preserving Block Truncation Coding*" ,Fundamenta Informaticae, IOS Press, 2006, Vol 73, Number 3/2006,Pp 373-387, ISSN 0169-2968

[YUC08] Yu-Cheng Fan, "*Testing Based Watermarking Techniques for intellectual-Property Identification in SOC design*", Instrumentation and Measurement, IEEE Transactions on, March 2008, Vol.57, pp. 467-479, Germany, ISSN: 0018-9456

[YUN99] Yun Q. Shi, Huifang Sun, "*Image and video compression for multimedia engineering*", 1999, ISBN: 0-8493-3491-8

[YUX08] Xiaoyi Yu , Babaguchi, N. , "*Run length based steganalysis for LSB matching steganography*", Multimedia and Expo, 2008 IEEE International Conference on, Hannover, June 23 2008-April 26 2008, pp 353-356, ISBN: 978-1-4244-2570-9

[ZHA07a] Hong-Juan Zhang , Hong-Jun Tang, "*A Novel Image Steganography Algorithm Against Statistical Analysis*" , Machine Learning and Cybernetics, 2007 International Conference on, Hong Kong, 19-22 Aug. 2007, Vol 7, pp 3884-3888, ISBN: 978-1-4244-0973-0

[ZHA07b] Weiming Zhang ,Xinpeng Zhang ,Shuozhong Wang, " *A Double Layered "Plus-Minus One" Data Embedding Scheme*" ,Signal Processing Letters, IEEE, Nov. 2007, Vol14, Issue: 11, pp 848-851, ISSN: 1070-9908

[ZHA06] Zhang H., Zang X., Liu J., "*A Secure BPCS Steganography against Statistical Analysis*", Signal Processing, 2006 8th International Conference on, Beijing, 16-20 2006, Vol 2, ISBN: 0-7803-9736-3

[ZOL98] J. Zöllner, H. Federrath, H. Klimant, A. Pfitzmann, R. Piotraschke, A. Westfeld, G. Wicke, G. Wolf, "*Modeling the Security of Steganographic Systems*", 2nd Workshop on Information Hiding: April 1998, Portland, LNCS 1525, Springer-Verlag, pp. 345-355, ISSN: 1556-6013

[ZOU08] El Zouka H.A., "*FPGA Based Implementation of Robust Watermarking System*", Information Technology: New Generations, 2008. ITNG 2008. Fifth International Conference on, Las Vegas, NV, 7-9 April 2008, pp. 1274-1278, ISBN: 0-7695-3099-0

[QUI00] Philip Quick, David Capson, *"Analysis of Determining Camera Position Via Karhunen-Loeve Transform",* Proceedings of the 4th IEEE Southwest Symposium on Image Analysis and Interpretation, pp.88, 2000, ISBN:0-7695-0595-3.

[1] HYPERLINK "http://www.itu.int/ITU-D/ict/statistics/ict/graphs/mobile.jpg"http://www.itu.int/ITU-D/ict/statistics/ict/graphs/mobile.jpg

[2] HYPERLINK**Error! Hyperlink reference not valid.**

[3] HYPERLINK "http://senseable.mit.edu/realtimerome"http://senseable.mit.edu/realtimerome

[4] ARM ARM7TDMI-S (Rev 4), Technical Reference Manual

[5] http://www.olimex.com

[6] Phillips Semiconductors, *„LPC2119/2129/2194/2292/2294 User Manual”*, 03 May 2004

[7] Movidia Labs – internal documentation and architecture July 2008

A1. LISTA LUCRĂRILOR PUBLICATE ÎN DOMENIUL TEZEI

A. Volumele unor manifestări ştiinţifice internaţionale cotate ISI

1. Stanescu D., Stratulat M., Ciubotaru B,. Chiciudean, D, Cioarga, R., Borca, D, "*Digital Watermarking using Karhunen-Loeve transform*", 4th International Symposium on Applied Computational Intelligence and Informatics, 2007. SACI '07, 18 Mai 2007, pp. 187-190, Timisoara, Romania, ISBN:1-4244-1234X, [ISI Proceedings]

2. Stanescu D., Stratulat M., Ciubotaru B., Chiciudean D., Cioarga R., Micea M., "*Embedding Data in Video Stream using Steganography*", 4th International Symposium on Applied Computational Intelligence and Informatics, 2007. SACI '07. 18 Mai 2007, pp. 241-244, Timisoara, Romania, ISBN: 1-4244-1234-X, [ISI Proceedings]

3. Stanescu D., Borca D., Groza V., Stratulat M., "*A Hybrid Watermarking Technique Using Singular Value Decomposition*"HYPERLINK "http://ieeexplore.ieee.org/xpl/RecentCon.jsp?punumber=4662485", 2008. HAVE 2008. IEEE International Workshop on Haptic Audio visual Environments and their applications**,** 18-19 Oct. 2008, Ottawa, pp.166-170, ISBN: 978-1-4244-2668-3, [ISI Proceedings]

B. Volumele unor manifestări ştiinţifice internaţionale indexate în baze de date internaţionale (BDI)

1. Stanescu D., Stratulat M., Groza V., Ghergulescu I., Borca D., "*Steganography in YUV color space*", Robotic and Sensors Environments, 2007. ROSE 2007. International Workshop on, 12-13 Oct. 2007, pp. 131-137 Ottawa, Canada, ISBN: 978-1-4244-1527-6, [IEEExplorer]

2. Stanescu D., Groza V., Stratulat M., Borca D., Ghergulescu I., "*Robust Watermarking with High Bit Rate*", Third International Conference on Internet and Web Applications and Services, 2008, ICIW2008, 8-13 iune 2008, Athena, Greece, pp. 257-260, 2008, ISBN: 978-0-7695-3163-2, [IEEExplorer]

3. D. Stănescu, V Stângaciu, I. Gergulescu, M. Stratulat,

"Steganography on embedded devices", SACI, 2009 "Politehnica" University of Timişoara, România, pp.313-317, ISBN: 978-1-4244-4478-6, [IEEExplorer]

A2. LISTA LUCRĂRILOR PUBLICATE (EXCEPTÂND CELE DIN DOMENIUL TEZEI)

Cărţi

1. Mircea Stratulat, Horatiu Moldovan, Adrian Pop, Daniela Stanescu, "Circuite integrate. Familia TTL – principii si aplicatii", Ed. Politehnica, 2001, 322 pagini, ISBN 973-8247-41-1

2. Mircea Stratulat, Daniela Stanescu, "Circuite si semnale numerice", Ed. Politehica, 2008,290 pagini, ISBN 978-973-625-557-9

Volumele unor manifestări ştiinţifice din străinătate

1. Andrei Novak, Mircea Stratulat, Daniela Stanescu, Dan Chiciudean, Bogdan Ciubotaru, Razvan Cioarga "Research and Development Platform for Multimedia Streaming of MP3 Audio Content", Journal of Applied Sciences at Budapest Tech, Hungary, Volume 3, 2006, ISSN: 1785-8860

2. M. Popa, D. Stanescu, "A node for serial communications in microcontroller networks", The 6th International Scientific Conference, Electronic Computers and Informatics ECI, 2004, Kosice-Herlany, Slovakia, Sept 22-24, ISBN 80-8073-950-0

Volumele unor manifestări ştiinţifice internaţionale organizate în România (cu referenţi ştiinţifici) şi redactate integral într-o limbă de circulaţie internaţională

1. Dan Chiciudean, Bogdan Ciubotaru-Petrescu, Daniela Stanescu, Razvan Cioarga "Event Reporting and System Diagnosis for Autonomous Monitoring and Control Equipments", Proceedings of the 7th international conference on technical informatics – CONTI'2006, vol. 2, pp. 311-316.

2. Nicolae Mircea Dehelean, Liana-Maria Dehelean, Daniela Stanescu, "A minimal System Structure for Human Trait-Detection", Proceedings of the 7th international conference on technical informatics – CONTI'2006, vol. 2, pp.101-107

3. Razvan-Dorel Cioarga, Mihai V. Micea, Bogdan Ciubotaru, Dan Chiuciudean, Daniela Stanescu, "CORE-TX: Collective Robotic Environment - the Timisoara Experiment", Proceedings of the 3rd Romanian-Hungarian Joint Symposium on Applied Computational Intelligence – SACI'2006, pp. 495-506, ISBN: 963-7154-46-9.

4. Bogdan Ciubotaru-Petrescu, Dan Chiciudean, Razvan Cioarga, Daniela Stanescu "Wireless Solutions for Telemetry in Civil Equipment and Infrastructure Monitoring", Proceedings of the 3rd Romanian-Hungarian Joint Symposium on Applied Computational Intelligence – SACI'2006, pp. 386-395, ISBN: 963-7154-46-9.

5. Andrei Novak, Mircea Stratulat, Daniela Stanescu, Dan Chiciudean, Bogdan Ciubotaru, Razvan Cioarga "Multimedia Streaming of MP3 Audio Content Based on FM Stereo Radio Transmitter", Proceedings of the 3rd Romanian-Hungarian Joint Symposium on Applied Computational Intelligence – SACI'2006, pp. 386-395, ISBN: 963-7154-46-9.

6. M. Popa, R. Igret, C. Lupu, D. Stanescu, "WebPic – An Embedded Internet Solution", Proceedings of the 6th international conference on technical informatics – CONTI'2004, pp. 9-12, ISBN: 1224-600X

7. M. Stratulat, I. Mihu, I. M. Mihu, Daniela Stanescu,D. Mastei, " Digital Signal Processing for ECG Signal", International Conf. on Computers Communications, ICCC2004, pp. 394 – 400, 973-613-542-X

A3. CITARI

1. Hanafy A.A.; Salama G.I.; Mohasseb Y.Z, "A secure covert communication model based on video steganography", Military Communications Conference, 2008. MILCOM 2008. IEEE , vol., no., pp.1-6, 16-19 Nov. 2008

2. Thanuja Tiptur Chandrashekhar, Uttara Kumari Mannava, "Invertible Data Hiding in Color Images Using Multiple Peaks Histogram," Signal Processing Systems, International Conference on, pp. 52-55, 2009 International Conference on Signal Processing Systems, 2009.