CONTRIBUŢII LA MARCAREA TRANSPARENTĂ A IMAGINILOR ÎN DOMENIUL TRANSFORMATEI WAVELET

Teză destinată obţinerii
titlului ştiinţific de doctor inginer
la
Universitatea Tehnică din Cluj-Napoca
în cotutelă cu Universitatea "Politehnica" din
Timişoara
în domeniul INGINERIE ELECTRONICĂ ŞI TELECOMUNICAŢII
de către

ing. Corina Alda NAFORNIŢĂ

Conducători ştiinţifici: Prof.dr.ing. Monica Borda (UTCN)
Prof.dr.ing. Alexandru Isar (UPT)
Referenţi ştiinţifici: Prof.dr.ing. Paul Cristea, M.C. al Academiei Române
Prof.dr.ing. Valeriu Munteanu
Prof.dr.ing. Radu Vasiu
Prof.dr.ing. Aurel Vlaicu

)2.2008

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

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

Doresc să-mi exprim recunoştinţa şi să aduc mulţumirile mele celor doi conducători ştiinţifici, prof. Monica Borda şi prof. Alexandru Isar. D-na prof. Monica Borda a fost şi va rămâne un model pentru mine, la fel ca şi dl. prof. Alexandru Isar. Domniile lor m-au susţinut în mod constant în momentele grele, inerente drumului parcurs până la finalizarea tezei şi mi-au sugerat, cu generozitate, căi şi idei.

Ţin să mulţumesc d-nei prof. Deepa Kundur, de la Universitatea Texas A&M, USA, o autoritate în domeniul de watermarking. Domnia sa a avut bunăvoinţa de a fi primul critic al lucrărilor mele din domeniu. Îi mulţumesc pentru tactul cu care m-a corectat şi îndrumat, precum şi pentru sprijinul moral acordat de-a lungul mai multor ani.

Trebuie să mulţumesc, de asemenea, echipei Barni, Bartolini şi Piva, şi în mod special d-lui Alessandro Piva (Universitatea din Firenze, Italia), care mi-a transmis programele utilizate de ei, necesare pentru a realiza comparaţiile prezente în lucrările mele. Se pare că îmbunătăţirile aduse de mine unor metode elaborate de dânşii, i-au determinat să mă susţină în continuare.

Mulţumesc referenţilor tezei, care au analizat lucrarea şi au făcut comentarii şi aprecieri, şi anume: d-nul prof. Paul Cristea, M.C. al Academiei Române, d-nul prof. Valeriu Munteanu, d-nul prof. Aurel Vlaicu şi d-nul prof. Radu Vasiu. Ţin să menţionez ca d-nul prof. Aurel Vlaicu şi d-nul prof. Radu Vasiu m-au ajutat foarte mult şi pe durata derulării grantului CNCSIS tip TD, cod 47 nr. 33385/29.06.04, prin care s-au finanţat, parţial, cercetările mele. Fără ajutorul domniilor lor mi-ar fi fost mult mai greu să-mi finalizez teza.

Mulţumesc colegilor de catedră pentru atmosfera favorabilă lucrului, pentru încurajările şi sprijinul lor constant.

Am beneficiat de sprijinul direct al domnilor rectori, prof. Nicolae Robu şi prof. Radu Munteanu, pe care îi asigur de recunoştinţa mea.

Nu în ultimul rând, mulţumesc întregii mele familii, pentru încurajările şi sprijinul necondiţionat oferite pe întregul parcurs al elaborării tezei.

Timişoara, Februarie 2008 Corina Naforniţă

Naforniţă, Corina Alda

Contribuţii la marcarea transparentă a imaginilor în domeniul transformatei wavelet

Teze de doctorat ale UPT, Seria 7, Nr. 8, Editura Politehnica, 2008, 240 pagini, 39 figuri, 27 tabele.

ISSN:1842-7014

ISBN: 978-973-625-777-2

Cuvinte cheie:
protecţia drepturilor de autor, imagini, marcare transparentă, transformare wavelet discretă, mascare perceptuală

Rezumat:
Lucrarea de faţă analizează construcţia sistemelor de protecţie a drepturilor de autor de imagini prin marcare transparentă (watermarking) în domeniul transformatei wavelet.
Se face o clasificare şi apreciere critică a metodelor de marcare transparentă şi a atacurilor.
Sunt propuse metode originale informate de marcare transparentă în domeniul transformatei wavelet discrete, cu o arhitectură de detector care asigură o detecţie optimă.
Sunt dezvoltate tehnici de mascare perceptuală în domeniul wavelet pentru marcare transparentă neinformată.

CUPRINS

1. INTRODUCERE

În ultimul deceniu, am asistat la o explozie în folosirea şi distribuirea datelor multimedia digitale. Conectarea la Internet a calculatoarelor personale a facilitat şi accelerat distribuirea aplicaţiilor şi datelor multimedia. Astfel, s-au dezvoltat rapid aplicaţiile de comerţ electronic şi de servicii on-line. Echipamentele audio şi video analogice sunt înlocuite progresiv cu echipamente digitale. Rezultatul a fost apariţia unor dispozitive de înregistrare de masă, de capacităţi mari şi foarte mari, pentru datele multimedia, care au pătruns masiv pe piaţă.

Astfel, o dată cu dezvoltarea pe scară largă a comunicaţiilor prin intermediul Internet-ului, a apărut nevoia de protejare a informaţiei digitale împotriva copierii şi manipulării ilegale. Dezvoltarea rapidă a tehnologiei digitale face necesară dezvoltarea metodelor pentru protejarea produselor multimedia împotriva pirateriei. Atacurile pirat includ accesul ilegal al datelor pe Internet, modificări ale conţinutului făcute cu rea-voinţă, retransmisia copiilor neautorizate. Impactul acestui gen de atacuri ar putea fi foarte mare atât pe plan financiar, pierderi financiare cauzate de accesarea şi folosirea neautorizată a datelor, cât şi în planul securităţii.

Când este vorba de semnale analogice, problema se rezolvă de la sine, deoarece copiile sunt de o calitate mai redusă decât originalele (casete audio şi video). În schimb, informaţia digitală poate fi copiată perfect şi distincţia între original şi copii este dificil, dacă nu imposibil de făcut. În plus, nu există nici un mecanism pentru a depista copierea ilegală sau modificarea conţinutului.

Datele digitale sau numerice au multe avantaje faţă de cele analogice, dar producătorii de servicii au reţineri când oferă servicii sub formă digitală, din cauza uşurinţei cu care se pot realiza duplicate care se pot distribui neautorizat. Din această cauză, se impun măsuri pentru protejarea proprietăţii intelectuale şi a drepturilor de autor pentru materialele memorate digital [LSL00]. Absenţa unor sisteme de protecţie adecvate a dus la întârzierea introducerii DVD-urilor (Digital Video Disc); unele companii media au refuzat iniţial să producă şi să comercializeze materiale pe DVD-uri, înainte de a se rezolva aceste probleme de protejare a informaţiei [LSL00]. Astfel, în octombrie 1998 în SUA a fost adoptată o lege de protecţie intelectuală, *„Digital Millennium Copyright Act"* [DMCA98], iar în Uniunea Europeană în mai 2001, respectiv aprilie 2004, au fost adoptate directive pentru protejarea copyright-ului şi a drepturilor de proprietate intelectuală, inclusiv pentru produse multimedia digitale, cum ar fi CD-uri şi DVD-uri [Dir01, Dir04].

Pentru a asigura protecţia la copiere şi protecţia drepturilor de autor pentru date digitale audio sau video, au fost dezvoltate două categorii de tehnici complementare şi anume: *criptarea* şi *marcarea transparentă* (*watermarking*).

Tehnicile de *criptare* pot fi folosite pentru protejarea datelor digitale în timpul transmiterii între emiţător şi receptor [CMB02]. Dar după recepţia şi decriptarea de la receptor, când se obţine varianta originală a datelor, acestea nu mai sunt protejate. Folosind tehnica complementară criptării, de *marcare transparentă*, datelor li se adaugă un semnal secret imperceptibil, marcaj sau watermark. Acest marcaj se introduce direct în datele originale, într-un mod care-l face să rămână permanent prezent.

Asigurarea unui canal sigur de informaţie se referă la restricţionarea accesului, criptarea şi/sau autentificarea informaţiei. Aceasta este o problemă

rezolvată, pentru care există protocoale de securizare. Ea este însă o problemă diferită de cea a protejării dreptului de autor.

În cele ce urmează, se explică trei noţiuni importante: cheia criptografică, autentificarea şi protecţia dreptului de autor.

1.1 Cheia criptografică publică sau secretă

"There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files. This book is about the latter."
Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C

Datele transmise prin comunicaţiile în reţele pot fi protejate împotriva utilizatorilor neautorizaţi prin aplicarea tehnicilor bazate pe criptare.

Criptografia este *ştiinţa secretizării datelor*. Ea stă la baza multor servicii şi mecanisme de securitate folosite în reţele şi mai ales în Internet, utilizând metode matematice pentru transformarea datelor, în intenţia de a ascunde conţinutul lor sau de a le proteja împotriva modificării. Deşi are o istorie îndelungată, criptografia s-a dezvoltat în ultimii ani mai ales datorită dezvoltării reţelelor de calculatoare.

Datele originale sunt criptate de proprietar folosind o cheie privată. Utilizatorii pot decripta datele primite folosind un algoritm implementat hard sau soft. Condiţia necesară pentru o decriptare cu succes este ca utilizatorul să deţină cheia privată a furnizorului, sau o cheie asociată publică sau parţial publică. Un deziderat este implementarea rapidă a algoritmului de criptare-decriptare. În plus creşterea volumului de date datorată criptării ar trebui să fie în limite rezonabile. De asemenea, lungimea cheii ar trebui să fie suficientă pentru a preveni decriptarea neautorizată prin proceduri iterative de tip *trial and error*.

Datele care pot fi citite şi înţelese fără măsuri speciale se numesc *text clar*. Metoda prin care datele clare sunt mascate, ca să ascundă esenţa, se numeşte *criptare*, rezultând *textul cifrat*. Procesul invers de transformare a datelor cifrate în date clare se numeşte *decriptare* [PGP99, Isa02].

Criptarea convenţională, numită şi criptare cu cheie secretă sau cheie simetrică, foloseşte o cheie atât pentru criptare cât şi pentru decriptare. Cheia este cunoscută doar de către destinatarul mesajului. Pentru toţi ceilalţi utilizatori ai reţelei cheia este secretă. In anul 1975 a fost adoptat primul standard de criptare a datelor propus de IBM, numit DES (Data Encryption Standard). Acesta descrie un algoritm de criptare simetrică.

Witfield Diffie şi Martin Hellman, cercetători la universitatea Stanford au pus, în anul 1976, [DH76], bazele *criptografiei asimetrice cu chei publice*. Se utilizează două chei, una secretă (cunoscută doar de destinatarul mesajului) şi una publică care poate fi cunoscută de orice utilizator al reţelei. Pe baza cheii publice se poate face identificarea sursei de unde soseşte un anumit mesaj. Folosind acest algoritm se poate face şi autentificarea mesajului, adica destinatarul poate să verifice şi dacă expeditorul este cel declarat în cadrul mesajului şi dacă mesajul a fost cumva falsificat de către un alt utilizator. Funcţionarea acestei metode de criptare este descrisă în continuare.

Bob şi Alice au câte o copie a softului, distribuit liber, de criptare cu cheie publică. Fiecare foloseşte copia proprie pentru a crea o pereche de chei. Un mesaj criptat cu una dintre cheile din această pereche de chei poate fi decriptat doar cu cealaltă cheie din aceeaşi pereche. Cea de-a doua cheie nu poate fi generată matematic folosind doar prima cheie.

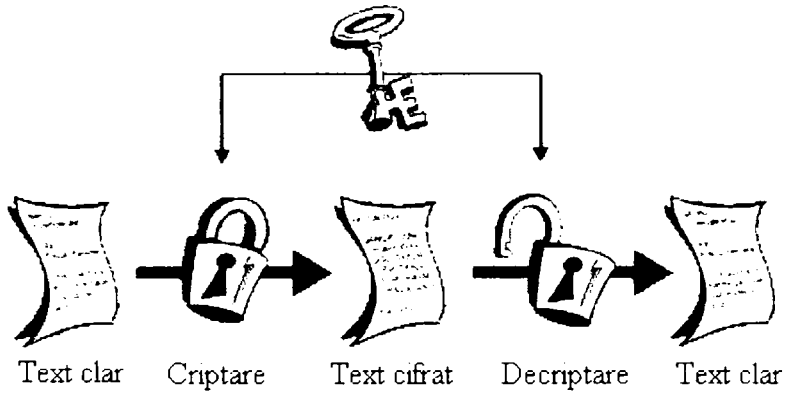


Fig. 1.1: Criptarea cu cheie privată (simetrică).

Bob face cunoscută una dintre cheile din perechea sa, aceasta devenind cheia sa publică. Alice face acelaşi lucru. Fiecare păstrează secretă cealaltă cheie din pereche, care devine cheia sa privată. Dacă Bob vrea să cripteze un mesaj, pe care să-l poată citi doar Alice, atunci el foloseşte cheia publică a lui Alice, care este disponibilă tuturor; acest mesaj va putea fi decodat doar cu ajutorul cheii secrete a lui Alice. Procesul invers, trimiterea unui mesaj criptat de la Alice la Bob este asemănător. De fapt, Bob şi Alice pot acum schimba între ei fişiere criptate, fără a avea vreun canal sigur pentru transmiterea cheilor, acesta fiind un avantaj major asupra comunicaţiilor bazate pe criptarea simetrică.

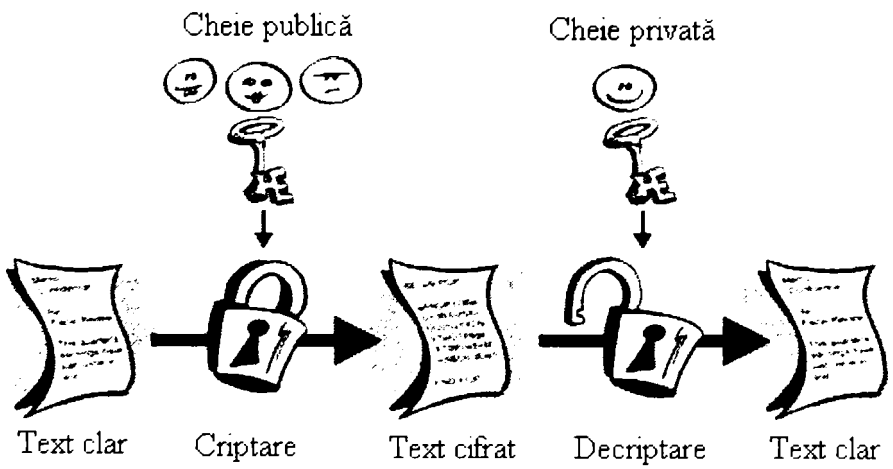


Fig. 1.2: Criptarea cu cheie publică (asimetrică).

1.2 Autentificarea

Autentificarea (în limba greacă, αυθεντικός înseamnă real sau original, iar în limba latină *authentes* înseamnă autor) este stabilirea sau confirmarea că ceva, sau cineva este autentic, adică este ceea ce pretinde. Autentificarea unui obiect

înseamnă confirmarea originii sale, în timp ce autentificarea unei persoane presupune de obicei verificarea identităţii sale.

În securitatea calculatoarelor şi reţelelor de calculatoare, autentificarea este încercarea de a verifica identitatea utilizatorului într-o comunicaţie, cum ar fi o cerere de login. Utilizatorul ce se doreşte a fi autentificat, poate fi o persoană ce foloseşte un calculator sau un program. Autentificarea exprimă ideea că unele resurse au fost puse la dispoziţie pentru a garanta că entităţile sunt ceea ce susţin că sunt, sau că informaţia nu a fost manipulată de părţi neautorizate, acesta fiind unele dintre obiectivele securităţii. Exemple de astfel de obiective includ controlul accesului, autentificarea entităţilor, autentificarea mesajelor, integritatea datelor, nerepudierea şi autentificarea cheilor.

Până la mijlocul anilor '70 se credea că *autentificarea* şi *confidenţialitatea* sunt conectate intrinsec. Odată cu descoperirea funcţiilor *hash* şi a semnăturilor digitale, s-a observat că autentificarea şi confidenţialitatea sunt obiective separate şi independente ale securităţii informaţiei. Separarea lor nu este doar folositoare, ci şi esenţială. De exemplu dacă Alice, aflată într-o ţară, comunică cu Bob, aflat în altă ţară, statele gazdă s-ar putea să permită sau nu confidenţialitatea canalului; una dintre ţări, sau ambele, ar putea dori să monitorizeze toate comunicaţiile. Însă Alice şi Bob vor să fie siguri de identitatea celuilalt, de integritatea şi originea informaţiilor pe care le trimit şi pe care le primesc.

Scenariul anterior relevă câteva aspecte independente ale autentificării. Dacă Alice şi Bob vor asigurări despre identitatea celuilalt sunt două posibilităţi:

- Alice şi Bob comunică *în timp real*, adică fără întârzieri apreciabile de timp. Alice şi Bob vor dori să-şi verifice identitatea în timp real. Acest lucru se poate realiza dacă Alice îl provoacă pe Bob să răspundă la o întrebare la care numai el ştie răspunsul corect. Acelaşi lucru îl poate face şi Bob pentru a o identifica pe Alice. Aceasta este o autentificare a entităţilor sau, mai simplu, o *identificare.*
- Alice şi Bob *nu comunică în timp real*, adică schimbă mesaje *cu o anumită întârziere,* adică mesajele sunt rutate prin numeroase reţele, stocate şi apoi redirijate după o perioadă. În acest caz nu este indicată o întrebare şi aşteptarea unui răspuns şi, în plus, comunicarea s-ar putea să se desfaşoare într-o singură direcţie. Sunt necesare alte tehnici pentru autentificarea originii mesajului. Aceasta este o nouă formă de autentificare numită *autentificarea originii datelor*.

Autentificarea expeditorului este operaţia de verificare a identităţii dintre expeditor şi persoana care, pe baza mesajului, pare să fie expeditorul. Să presupunem că Bob trimite tuturor utilizatorilor reţelei un mesaj, după ce l-a criptat cu cheia sa secretă. Oricare dintre utilizatori poate folosi cheia publică a lui Bob pentru a decripta acest mesaj, adeverind că acesta este un mesaj care ar putea veni numai de la Bob.

Autentificarea mesajului, reprezintă operaţia de validare a faptului că mesajul recepţionat este o copie neatinsă a mesajului trimis. Şi această operaţie poate fi realizată folosind criptarea cu cheie publică. Să presupunem că înainte de a expedia un mesaj, Bob efectuează o operaţie criptografică asupra acestuia, de exemplu îl transformă cu ajutorul unei funcţii „hash", ale cărei valori sunt dificil de calculat cu metode numerice. Cel mai simplu exemplu de astfel de funcţie este cea care asociază o sumă de control textului clar. Este foarte dificil să se modifice textul clar fără a modifica valoarea obţinută prin aplicarea funcţiei amintită mai sus.

Unul din avantajele criptării cu cheie publică este că oferă o metodă pentru implementarea semnăturilor digitale. De aceea Guvernul S.U.A a decis elaborarea unui standard de semnătură digitală, bazat pe utilizarea cheilor publice şi secrete, standardul DSS (*Digital Signature Standard*) publicat în 1991.

Semnătura digitală oferă posibilitatea de verificare a autenticităţii informaţiei şi a integrităţii ei. O semnătură digitală este un mesaj codat care se potriveşte cu conţinutul unui document digital autentic. În loc să criptăm informaţia folosind cheia publică a altei persoane, o criptăm cu cheia privată personală. Dacă informaţia poate fi decriptată cu cheia publică personală, atunci informaţia provine de la tine.

Metoda cea mai simplă de înserare a semnăturii digitale este arătată în figura de mai jos:

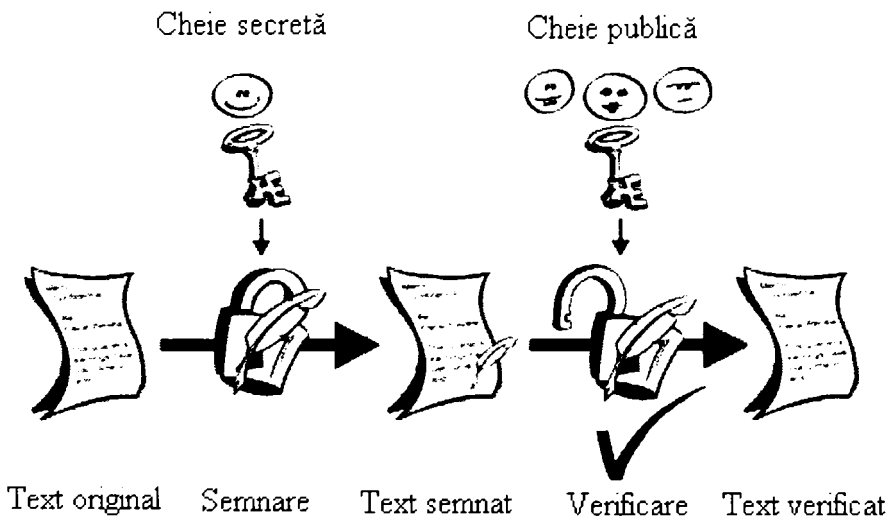


Fig. 1.3: Inserarea unei semnături digitale.

Acest standard se bazează pe un algoritm de semnătură digitală, DSA (Digital Signature Algorithm) folositor în aplicaţiile în care este mai potrivită utilizarea unei semnături digitale în locul unei semnături scrise. DSA asigură posibilitatea de a genera şi de a verifica semnături digitale. Generarea semnăturilor se bazează pe utilizarea unei chei secrete. Verificarea semnăturii se bazează pe folosirea unei chei publice care corespunde cheii secrete. Fiecare utilizator posedă o pereche de chei, formată din cheia sa publică şi cheia sa secretă. Cheile publice pot fi cunoscute de către orice utilizator al reţelei. Oricine poate verifica semnătura unui utilizator folosind cheia sa publică.

Generarea semnăturii unui utilizator poate fi realizată numai de către acesta, deoarece în procesul de generare se foloseşte cheia sa secretă. În procesul de generare a semnăturii se utilizează o funcţie hash, pentru a obţine o variantă condensată (rezumat al mesajului) a datelor care trebuie transmise (figura 1.4, 1.5).

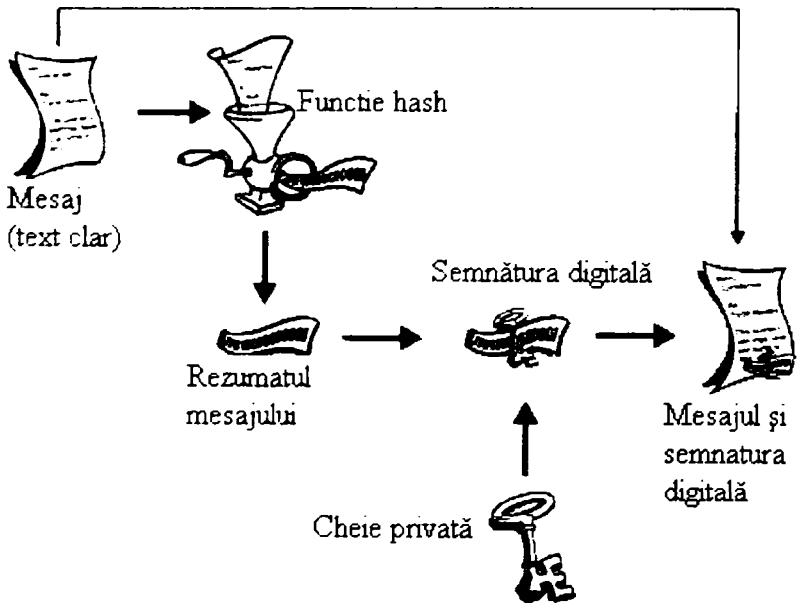


Fig. 1.4: Semnarea folosind o cheie privată

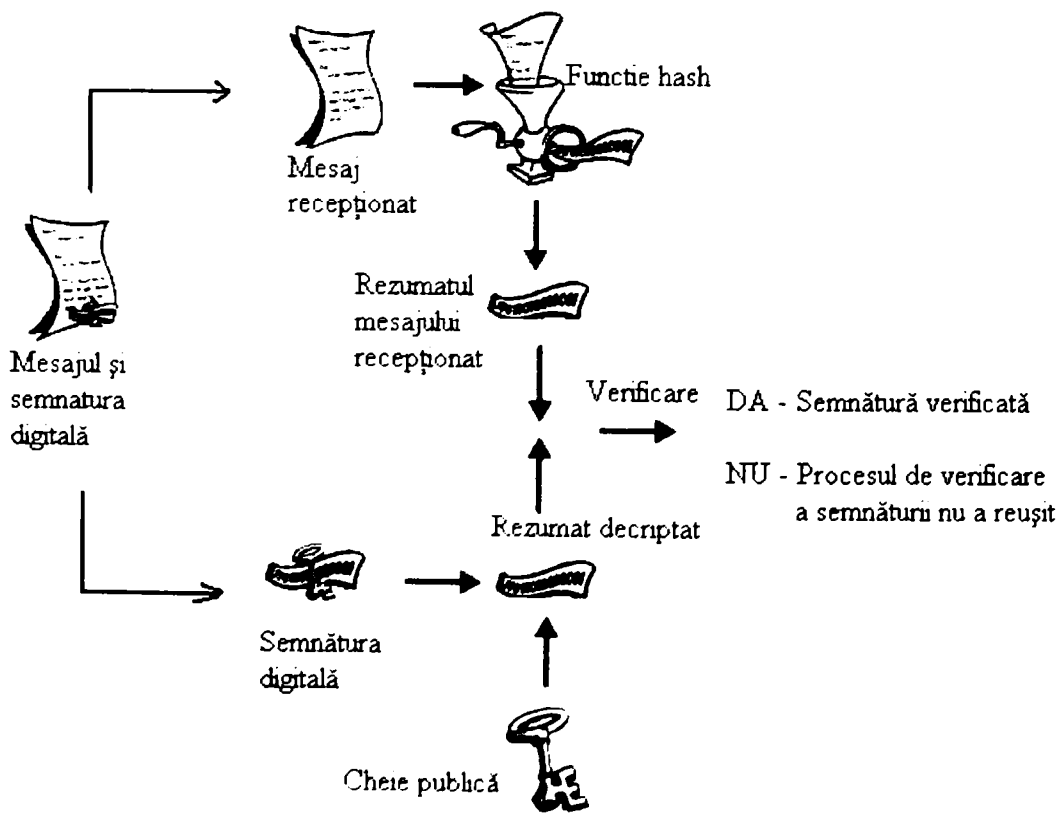


Fig. 1.5: Verificarea cu cheie publică.

Funcţiile *hash* sunt funcţii de compresie, contracţie sau de rezumat al mesajului, fiind nişte amprente digitale; ele au la intrare un şir de date de lungime variabilă *n*, numit *preimagine* şi la ieşire generează un şir de lungime fixă *m* (uzual 128 sau 160 biţi) numit *valoarea funcţiei hash*. Acestui rezumat i se aplică algoritmul DSA pentru a se genera *semnătura digitală*. Semnătura digitală împreună cu mesajul semnat sunt transmise celui care trebuie să o verifice, cu ajutorul cheii publice a expeditorului. În procesul de verificare trebuie folosită aceeaşi funcţie hash. Proceduri similare trebuie folosite şi pentru generarea şi verificarea semnăturilor digitale pentru date stocate (nu transmise). O semnătură digitală are acelaşi scop ca şi o semnătură scrisă de mână. Diferenţa este că cea scrisă de mână este uşor de falsificat, pe când cea digitală este aproape imposibil de fasificat.

În cazul datelor multimedia, manipularea conţinutului poate fi făcută în diferite scopuri, legale sau ilegale, prin compresie, filtrare, modificare cu rea intenţie. Produsul modificat nu este autentic. De aceea, utilizatorii ar trebui să poată verifica originalitatea conţinutului unui produs digital. Verificarea conţinutului poate fi făcută adăugând semnături digitale în datele transmise. Procedurile de verificare a autenticităţii se bazează pe algoritmi publici şi pe chei publice. Orice modificare nesemnificativă adusă produsului sau semnăturii ar trebui să ducă la neautentificare. Lungimea semnăturii este proporţională cu cantitatea de date „semnate", astfel că semnăturile sigure şi eficiente nu sunt fezabile pentru produse multimedia (care de obicei au o cantitate mare de date).

1.3 Concepte de bază ale marcării transparente

"A distinguishing mark or device impressed in the substance of a sheet of paper during manufacture, usually barely noticeable except when the sheet is held against strong light" - Oxford English Dictionary

Manipularea datelor în format digital şi transmiterea lor spre utilizatori poate fi făcută prin serviciile web. Utilizatorul poate avea acces la un produs interesant, fie direct de pe pagina *web* a proprietarului de drept, fie printr-o bibliotecă digitală, fie printr-un intermediar. Un produs digital poate să fie prezentat în forma sa originală sau ca parte dintr-o aplicaţie multimedia mai mare. Considerăm un sistem elementar de distribuţie a produselor digitale prezentat în Figura 1.6.

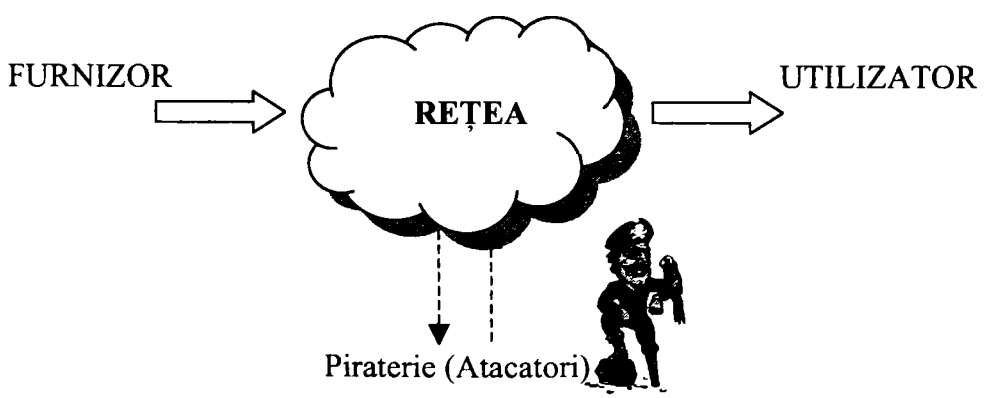


Fig. 1.6: Sistem elementar de distribuţie a produselor digitale. Sunt posibile atacurile pentru violarea dreptului de autor sau modificări făcute cu rea intenţie.

Utilizatorul primeşte un produs digital de la un editor care are drept de autor, şi care poate fi şi autorul original. Accesul şi transmiterea produsului au loc într-un mediu de comunicaţii. Atacatorii pot aduce daune proprietarului de *copyright*, prin reproducerea şi retransmiterea ilegală a produselor digitale. Mai mult, ei pot face modificări asupra produselor, furnizând utilizatorilor produse neautentice (false). De aceea, editorul şi utilizatorul au nevoie de protecţie:

- proprietarul dreptului de autor necesită o metodă de protejare eficientă în tot domeniul accesibil de adrese,
- utilizatorii cer produse autentice atunci când le achiziţionează legal.

Utilizatorii nu aduc daune altora pentru că nu retransmit sau expun produse pe pagini *web* publice, dar atacatorii sunt editori neautorizaţi.

Considerăm pirateria în primul rând ca activitatea de copiere ilegală şi/sau revânzarea produselor multimedia digitale. Uşurinţa cu care se pot face copii identice face pirateria o problemă majoră în securitatea informaţională. Se prezintă trei situaţii considerate în aplicaţiile obişnuite de securitate şi deficienţele tehnicilor de securitate în protejarea produselor multimedia [Kun99].

În prima situaţie (Figura 1.7), Alice vinde un produs multimedia lui Peter. Deşi informaţia poate fi protejată în timpul transmisiei către Peter, folosind algoritmi stabiliţi de criptare, produsul va fi neprotejat o dată ce este decriptat de Peter. Nu există nici un mecanism care să îl împiedice pe Peter să facă copii ilegale ale produsului cumpărat de la Alice. De aceea, este nevoie de un nivel de securitate suplimentar pentru protejarea proprietăţii intelectuale.

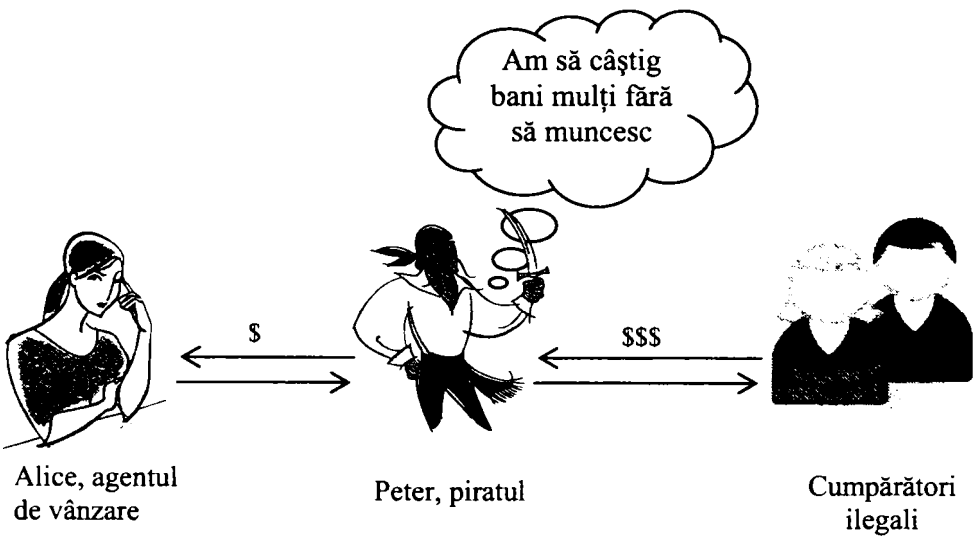


Fig. 1.7: Limitările tehnicilor obişnuite de securizare în piraterie.
Alice îi vinde lui Peter un produs multimedia. Deşi informaţia poate fi protejată în timpul transmisiei către Peter, prin proceduri obişnuite de securizare, aceasta va fi neprotejată atunci când este decriptată de Peter.

Abordările obişnuite de autentificare nu sunt nici ele potrivite pentru protejarea conţinutului produsului multimedia împotriva falsificării. Falsificarea (*tampering*) se referă la orice fel de modificare sau contrafacere a unui semnal dat. În Figura 1.8, prezentăm o astfel de situaţie posibilă. Alice îi trimite informaţii lui

Bob. Înainte de a ajunge la acesta, semnalul poate suferi distorsiuni întâmplătoare, cum ar fi eronarea aleatoare a biţilor, sau pierderi de pachete. Aceste distorsiuni întâmplătoare nu afectează integritatea semnalului.

În plus, este posibil ca Tom, care are acces la date, să modifice cu rea-credinţă semnalul pentru a ascunde informaţii false. Procedurile obişnuite de autentificare trec datele care trebuie să fie autentificate printr-o funcţie *hash one-way* pentru a produce o secvenţă de biţi, semnătura digitală. Semnalul şi semnătura digitală sunt transmise către Bob. La recepţie, Bob trece semnalul primit prin aceeaşi funcţie *hash one-way*, şi poate compara secvenţa obţinută de biţi cu semnătura digitală primită. Dacă cele două secvenţe se potrivesc, atunci semnalul este considerat autentic sau credibil, altfel se consideră că a avut loc o falsificare.

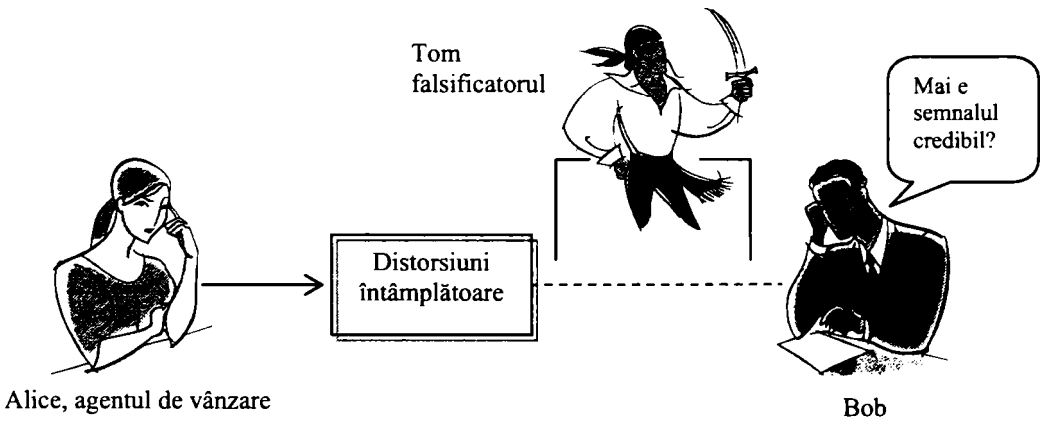


Fig. 1.8: Limitările securizării obişnuite în problema falsificării. Bob nu poate să facă diferenţa între distorsiuni întâmplătoare, care nu afectează integritatea semnalului, şi distorsiunile făcute cu rea voinţă de către Tom, pentru a-l induce în eroare pe Bob.

Deşi procedura de autentificare specificată este eficientă pentru unele tipuri de date, ea nu este eficientă pentru semnalele multimedia, deoarece nu se poate face deosebirea între cele două tipuri de distorsiuni, datorate marcării respectiv transmisiei. În ambele situaţii, semnalul este modificat. Când distorsiunile au caracter aleator, semnalul mai este încă perceptual credibil. De multe ori deciziile cu privire la integritatea conţinutului se impun pe baza aprecierii gradului de distorsiuni al semnalului recepţionat.

Figura 1.9 prezintă procesul de fraudă care se referă la orice fel de înşelătorie sau impostură. Fred trimite informaţii lui Bob, dar Fred ar vrea să pară că expeditorul a fost Alice. Pentru a preveni acest tip de atacuri, pot fi trimise mesaje criptate care să conţină informaţia separată de autentificare a expeditorului real. Cu toate acestea, semnalele multimedia suferă deseori schimbări în timpul tranzitului. Aceste schimbări pot elimina întâmplător informaţia de autentificare, în aşa fel încât Bob nu va putea identifica cu uşurinţă proprietarul de drept al produsului multimedia.

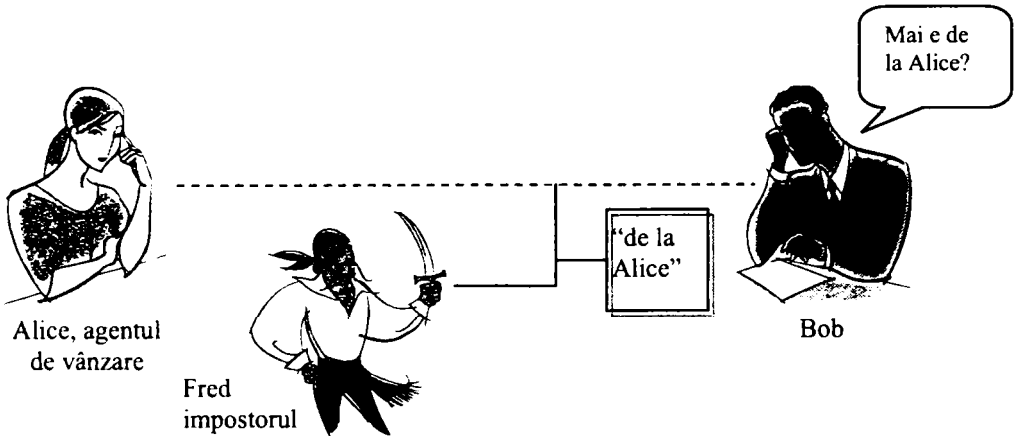


Fig. 1.9: Limitările securizării obişnuite în problema fraudei. Deoarece informaţia de autentificare este deseori transmisă ca informaţie adiţională semnalului, ea poate fi eliminată în timpul conversiei în alt format sau în timpul compresiei. Ca urmare, Bob va fi incapabil să afle dacă semnalul primit este sau nu de la Alice.

Pentru a trata neajunsurile metodelor de securizare tradiţionale discutate mai sus, a fost propusă metoda de înglobare a unei informaţii invizibile în produse multimedia, numită *digital watermarking* (marcare transparentă). Denumirea de watermark provine de la cuvintele din limba engleză water-apă şi mark-marcaj şi desemnează un marcaj transparent, invizibil, asemănător transparenţei apei. Termenul de watermarking este utilizat la modul general, pentru înserarea de biţi de informaţie, unul sau câţiva biţi, dar pentru cazurile în care se înserează mai mulţi biţi se mai foloseşte şi termenul de *data embedding*.

Marcarea este mai potrivită pentru semnale multimedia, cum ar fi imagini, audio şi video, deoarece conţinutul lor este protejat, în opoziţie cu formatul digital, care poate suferi conversii. În acest fel, informaţia de autentificare este înglobată în semnalul multimedia, chiar şi după conversii ale formatului sau alte prelucrări.

Marcajele sunt generate în mod privat şi apoi ar trebui să fie detectate folosind chei private sau publice în funcţie de întrebuinţarea lor. Marcajul conţine, în general, informaţii despre originea şi/sau destinaţia informaţiei gazdă. Deşi nu este folosit direct în protecţia proprietăţii intelectuale, el ajută la identificarea sursei şi destinatarului, fiind util în cazul disputelor privind dreptul de autor sau distribuitor al informaţiei.

Teoretic, marcajul trebuie să protejeze informaţia permanent, deci trebuie să aibă calitatea de a fi robust, astfel încât să nu poată fi înlăturat din informaţia gazdă, fără degradarea esenţială a calităţii acesteia. Acest marcaj este asemănător unei semnături, cu observaţia că trebuie să fie transparent.

Procedeul de marcare transparentă pentru a putea realiza protejarea informaţiei, constă din două operaţii: introducerea marcajului în datele gazdă, înainte de transmisie sau stocare, precum şi extragerea marcajului din datele recepţionate şi compararea marcajului adăugat la emisie cu cel extras la recepţie, pentru autentificare, în caz de dispută. În Figura 1.10, se prezintă schematic un sistem de protejare a datelor în format digital. Acestea sunt reprezentate prin simbolul D; se mai notează cu D' datele criptate, cu S semnătura, iar W reprezintă marcajul.

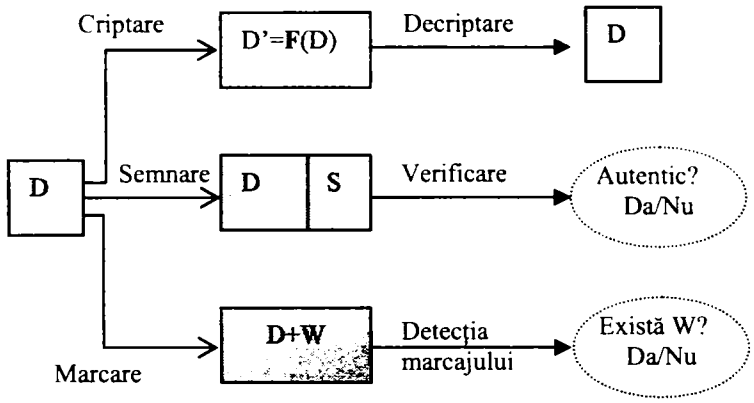


Fig.1.10: Reprezentare schematică a criptării datelor, verificarea autenticităţii şi marcarea datelor.

A. Marcare pentru protejarea dreptului de autor. Marcajul (numit şi etichetă pentru *copyright* sau ştampilă invizibilă în acest caz) conţine informaţie specifică proprietarului legal (de exemplu un *logo*) sau este un semnal aleator unic pentru respectivul proprietar. Protejarea se face în felul următor:

- Fiecare proprietar de *copyright* deţine un număr unic (sau un set de numere) care constituie cheia privată a marcajului K_{pr}.
- Folosind cheia privată şi un algoritm public sau privat, proprietarul dreptului de autor modifică datele digitale care sunt astfel marcate (este exclusă adăugarea de informaţii cum ar fi un antet sau altele).
- Folosind un algoritm de detecţie, proprietarul de *copyright* poate verifica sau decoda modificările făcute de el însuşi şi poate folosi această informaţie ca un indicator al proprietăţii legale asupra respectivului produs.

B. Marcare pentru autentificare. Aşa cum s-a spus în introducere, problema verificării autenticităţii produselor digitale se rezolvă cu ajutorul semnăturilor digitale. Autenticitatea este legată de un produs original de referinţă şi de obicei are de-a face cu originalitatea conţinutului, numele autorului, data la care produsul a fost creat, proprietarul dreptului de autor, etc. Marcajele se referă în principal la partea de autenticitate asociată cu originalitatea conţinutului (termenii de integritate a datelor, verificarea conţinutului sau dovada modificării datelor sunt de asemenea folosiţi). Se schiţează următoarea schemă de bază:

- Autorul original deţine o cheie privată unică K_{pr}.
- Cu ajutorul unui algoritm ce foloseşte cheia privată, datele sunt modificate cu scopul de a îngloba informaţia de autenticitate. Algoritmul ar trebui să furnizeze şi o cheie publică K_{pub}.

Receptorul poate să verifice autenticitatea produsului. El poate să-şi folosească cheia publică K_{pub} şi un algoritm public care furnizează un răspuns binar ce indică autenticitatea sau nu.

1.4 Aplicaţii posibile ale marcării transparente

Marcarea transparentă prezintă interes şi pentru aplicaţii care nu ţin de securizarea informaţională [CMB02, LSL00, Bar03a, Bar03b].

1. *Monitorizarea transmisiilor TV*: dacă o firmă care îşi face publicitate, doreşte să afle câte din reclamele plătite au fost efectiv transmise, poate să monitorizeze transmisiile TV cu ajutorul observatorilor umani. Desigur, acest lucru se poate dovedi extrem de costisitor şi în plus nefiabil. Există de asemenea sisteme de monitorizare, care nu apelează la observatori umani. Acestea se împart în două categorii: pasive şi active. Sistemele de monitorizare *pasive*, încearcă să recunoască direct conţinutul difuzat, la fel ca şi observatorii umani. Aceste sisteme sunt calculatoare care compară semnalul difuzat cu semnalele pe care le au în baza de date (şi anume, semnalele care reprezintă spoturile publicitare). Aceste sisteme se pot dovedi nepractice, din cauza mărimii bazelor de date. În practică, aceste sisteme nu sunt folosite pentru a verifica dacă, de exemplu, o reclamă a fost difuzată. Ele sunt folosite mai ales pentru a obţine date despre competitori.

Pentru a obţine acurateţea cerută de procesul de verificare, ar trebui folosite sisteme de monitorizare *active*, care se bazează pe informaţii asociate difuzate o dată cu conţinutul propriu-zis al reclamelor. Marcarea poate fi o soluţie pentru monitorizarea activă a transmisiilor TV. Prin înserarea marcajelor în reclamele comerciale, un sistem automat de monitorizare poate verifica dacă aceste reclame au fost difuzate conform contractului. Prin monitorizare pot fi protejate şi alte produse TV valoroase, ca de exemplu cele mai recente ştiri. Sistemele de monitorizare a difuzării pot verifica toate canalele de difuzare şi să taxeze staţiile TV conform constatărilor.

2. *Identificarea proprietarului*: acest lucru se poate face printr-o inscripţionare vizibilă a autorului. Acest tip de „marcare" a proprietăţii poate însă fi uşor eliminat din semnalul multimedia respectiv. Cel mai bun exemplu în acest sens este decuparea unei porţiuni dintr-o imagine, care să nu conţină „marca" autorului. Deoarece marcajele pot fi imperceptibile şi inseparabile de semnalul original, pot reprezenta o soluţie ideală pentru identificarea autorului.

3. *Dovada proprietăţii*: ar fi de dorit ca marcajele să servească nu numai pentru a „marca" proprietatea, dar chiar să o dovedească. Dacă Alice creează o imagine şi o marchează cu marca „© 2008 Alice", atunci Bob poate fura imaginea respectivă, şi folosind un program de procesare a imaginilor, poate înlocui marca cu „© 2008 Bob". Dacă Alice nu a înregistrat imaginea la o autoritate centrală, ea va trebui să demonstreze că imaginea îi aparţine. Dacă atacatorul nu dispune de un detector al marcajului, eliminarea acestuia poate fi greu de făcut. Pe de altă parte, chiar dacă marcajul nu poate fi eliminat, folosind propriul sistem de marcare, Bob poate să arate că marcajul lui ar exista în originalul lui Alice [CMYY98]. Astfel, o terţă parte nu ar putea să îşi dea seama cui aparţine imaginea.

Această problemă ar putea fi rezolvată dacă, în loc de a demonstra proprietatea prin marcare, s-ar demonstra că o imagine derivă din alta.

4. *Înregistrarea operaţiilor efectuate* (transaction tracking) sau *amprentarea* (fingerprinting): pentru a urmări sursa copiilor ilegale, proprietarul poate folosi această tehnică, prin care se înserează marcaje diferite, în copiile livrate la clienţi diferiţi. Acest număr serial este de fapt asociat cu identitatea clientului şi pot fi identificaţi acei clienţi care încalcă convenţia de licenţă, permiţând copierea datelor de către o terţă parte. Marcajul înregistrează una sau mai multe operaţii care au fost făcute asupra copiei unui produs multimedia. De exemplu, marcajul

poate „memora" o identitate a cumpărătorului (se presupune că fiecare cumpărător are o copie diferită a originalului, marcajele nefiind aceleaşi).

5. *Autentificarea conţinutului*: acest lucru poate fi realizat prin înglobarea *semnăturii digitale* în semnalul multimedia. Această semnătură mai este cunoscută şi sub numele de marcă de autentificare. Dacă un semnal ce conţine o astfel de marcă este modificat, se poate afla cum a fost distorsionat. Pentru verificarea autenticităţii datelor pot fi folosite marcaje fragile, care indică faptul că datele au fost sau nu alterate şi localizarea alterarii în caz că există.

6. *Controlul copierii* (copy control): prevenirea apariţiei copiilor ilegale poate fi făcută prin criptare. Există trei posibilităţi prin care un adversar poate obţine acces neautorizat la produse multimedia: dacă decriptează datele fără a avea o cheie; dacă obţine o cheie prin *reverse-engineering*; sau cel mai simplu dacă obţine o cheie în mod legal, făcând copii ilegale ale datelor decriptate. Marcajele însă pot rămâne în conţinut şi după decriptare. Cu toate acestea, protejarea DVD-urilor împotriva copierii nu a fost făcută încă cu succes, deoarece nu orice DVD-player conţine un detector al marcajului. Informaţia conţinută în watermark poate controla direct dispozitivele de înregistrare, deoarece watermark-ul reprezintă un bit de interdicţie a copierii; astfel, detectorul din dispozitiv stabileşte automat dacă datele pot fi memorate sau nu.

Tehnicile de marcare sunt folosite şi în alte scopuri [LSL00, AM05]:

7. *Indexarea* video-mail-urilor, a filmelor şi a ştirilor, în care pot fi introduse marcaje şi comentarii care pot fi folosite de motoarele de căutare.

8. *Siguranţa medicală*: înserarea în imaginile medicale a numelui şi datelor personale ale pacientului.

9. *Ascunderea datelor* (data hiding): watermarking-ul poate fi folosit la transmiterea unor mesaje private secrete, deoarece unele guverne restricţionează accesul la serviciile de criptare; astfel unele persoane pot să-şi ascundă mesajele în alte date.

10. *Corectarea erorilor din transmisii video (tehnici ECDH):* în comunicaţiile video, algoritmii de detecţie/corectare a erorii cu *data hiding* se axează pe recuperarea datelor pierdute în transmisii sau înlăturarea/ascunderea erorilor într-o manieră eficientă. La recepţia semnalului video, informaţia înserată este folosită ca referinţă pentru a recupera mai bine pierderile.

1.5 Etapele marcării

După cum am văzut, principial marcarea transparentă constă din două prelucrări de bază desfăşurate la emisie, respectiv la recepţie:

-introducerea marcajului, cu respectarea cerinţelor de *transparenţă perceptuală* şi *robusteţe*, în datele gazdă ce urmează a fi marcate;

-extragerea marcajului din semnalele marcate recepţionate (posibil modificate) şi compararea acestuia cu valoarea introdusă la emisie, în caz de dispută.

Pentru a îndeplini cerinţa de robusteţe, marcajul introdus la emisie va depinde de una sau mai multe chei criptografice sigure (secrete sau publice), chei necesare şi în procesul de detecţie de la recepţie.

Prima întrebare care se pune în legătură cu un sistem de marcare transparentă sau unul steganografic este *ce marcaj alegem,* adică ce formă va lua mesajul ce va fi integrat. Cea mai simplă metodă ar fi de a integra un text într-o imagine, permiţând imaginii să fie purtătorul direct al unor informaţii ca autor, titlu,

dată, ş.a.m.d. Dezavantajul acestei abordări este însă că textul ASCII se poate considera într-un fel ca fiind o compresie LZW, în care fiecare literă este reprezentată de un anumit şablon de biţi. Prin compresia marcajului înainte de integrare, robusteţea are de suferit. Având în vedere natura codului ASCII, o eroare de un singur bit, în urma unui atac, poate schimba înţelesul acelui caracter, şi prin urmare şi a mesajului. Ar fi simplu chiar şi pentru o simplă compresie JPEG ca să reducă textul de copyright la o colecţie aleatoare de caractere. De aceea informaţia se poate integra, în loc de caractere, într-o formă deja foarte redundantă, ca o imagine. Este de menţionat faptul că în ciuda numărului mai mare de erori apărute la recuperarea marcajului, marcajul este încă de recunoscut.

Fig. 1.11: Marcaj original, respectiv marcaj extras, cu 25% zgomot gaussian aditiv

În literatura de specialitate se pot întâlni diferite *definiţii pentru marcaj* [VP99, CMB02, SK01]. Marcajele pentru imagini sunt tratate ca:

i) manipulări ale biţilor celor mai puţin semnificativi, LSB, sau ai pixelilor;
ii) rezultate ale aplicării unor coduri ascunse de marcare;
iii) texturi invizibile;
iv) rezultatele aplicării unor constrângeri secrete unor transformate ale imaginilor, etc.

Putem defini marcajul ca un semnal numeric W, care este suprapus pe produsele digitale printr-un proces de înglobare. Se poate descrie W ca un semnal cu componente binare sau, mai general, ternare [VP99]:

$$\boldsymbol{W} = \left\{ w(\vec{k}) ; \middle| w(\vec{k}) \in \{-1, 0, 1\}, \vec{k} \in \hat{W}^{'} \right\} \qquad (1.1)$$

unde $\hat{W}^{d}$ este spaţiul de date digital (matrice) al marcajului de dimensiune d=1, 2, 3 pentru audio, imagini fixe, respectiv video. Vectorul $\vec{k}$ indică poziţiile elementelor matricii (coordonatele în spaţiul $\hat{W}^{'}$).

1.5.1 Generarea marcajului. Fie **W** setul de semnale de marcare posibile. În conformitate cu teorema de existenţă a unei chei asociate, considerăm spaţiul finit de chei **K** [VP99]. Dacă **I** este informaţia marcajului (*payload*), **X** este setul de imagini digitale fixe, atunci o metodă de generare a marcajului *W* ar trebui să fie definită de următoarea funcţie:

$$G : \mathbf{I} \times \mathbf{X} \times \mathbf{K} \rightarrow \mathbf{W}, \quad W = G(I, X_0, K) \qquad (1.2)$$

unde $K \in \mathbf{K}$ este cheia de marcare şi $X \in \mathbf{X}$ este semnalul în care este înglobat marcajul. Pentru un anumit produs X şi un semnal de marcare W, extragerea cheii ar trebui să fie imposibilă.

1.5.2. Înglobarea marcajului. Considerând semnalul de marcare $W = \{w(\vec{k})\}$, produs de $\mathcal{G}$, procesul de înglobare a marcajului este definit ca o suprapunere a lui W peste produsul original $X_0 = \{x(\vec{k})\}$. Notăm procedura de înglobare prin $\mathcal{E}$ şi o definim după cum urmează:

$$\mathcal{E} : \mathbf{X} \times \mathbf{W} \times \mathbf{R} \to \mathbf{X}, \quad X_w = \varepsilon(X_0, W; l) \tag{1.3}$$

Parametrul l, care este o valoare reală, este asociat energiei de înglobare a marcajului sau, echivalent, vizibilităţii marcajului. În practică, în locul unui singur parametru l, este nevoie şi de o mască de înglobare L pentru a atinge o înglobare satisfăcătoare. L este formată luând în considerare caracteristicile sistemelor vizual sau auditiv uman.

Figura 1.12 ilustrează procesul general de marcare descris de ecuaţia (1.3). Un marcaj, care de multe ori este alcătuit dintr-o secvenţă de biţi, este înserat într-un semnal gazdă cu ajutorul unei chei [CMB02]. Procedeul de înglobare impune schimbări mici în semnal, determinate de cheie şi de marcaj, pentru a genera semnalul marcat.

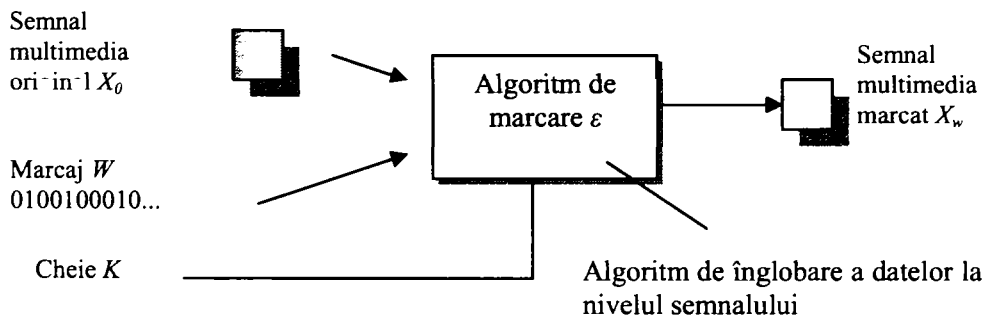


Fig. 1.12: Procesul de înglobare a marcajului. Marcajul este înglobat cu ajutorul unei chei, făcând schimbări imperceptibile în semnalul multimedia original.

Transparenţa perceptuală se realizează în concordanţă cu un anumit criteriu de perceptibilitate care poate fi implicit sau explicit. Astfel, eşantioanele individuale ale semnalului gazdă, folosite pentru înserarea informaţiei de marcaj, vor putea fi modificate numai între anumite limite situate sub pragurile de sensibilitate ale simţurilor umane (auz, văz). În cazul prelucrării imaginilor se obţine o mască perceptuală care ne va spune cât de mult pot fi alteraţi anumiţi pixeli, şi care sunt aceştia, fără a afecta calitatea imaginii.

Un exemplu de mască perceptuală îl putem vedea în Figura 1.13 [PH99].

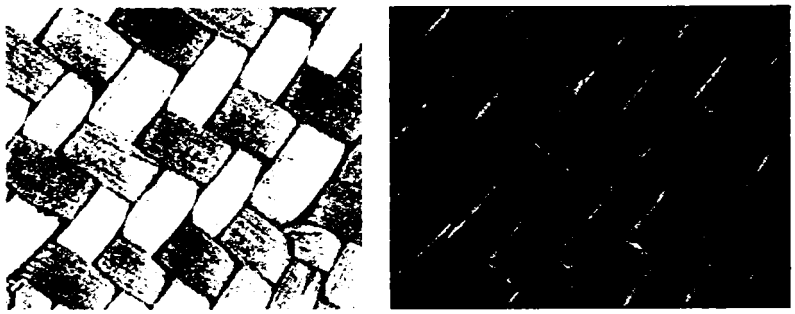


Fig. 1.13: a) imagine originală a unei ţesături; b) masca perceptuală a ţesăturii.

Inserţia transparentă a marcajului în semnalul digital gazdă este posibilă numai datorită faptului că destinatarul final este omul. Simţurile sale sunt detectoare imperfecte caracterizate de praguri de sensibilitate (intensitate sonoră, respectiv nivel de contrast) minime precum şi de fenomenul de *mascare*. Mascarea se referă la faptul că o componentă, dintr-un semnal dat, audio sau video, poate deveni imperceptibilă în prezenţa unui alt semnal, numit semnal de mascare. Majoritatea tehnicilor de codare ale semnalelor audio şi video folosesc caracteristicile sistemului auditiv uman, HAS (Human Audio System) şi ale sistemului vizual uman HVS (Human Visual System), direct sau indirect. Pentru ca semnalul de marcaj să fie robust (în ciuda amplitudinii mici a acestuia cerută de condiţia de transparenţă), el este împrăştiat pe mai multe eşantioane în conformitate cu cerinţele de granularitate, ceea ce conduce la detecţia lui şi din date marcate afectate de distorsiuni. Tehnica de împrăştiere este similară cu cea de întreţesere şi este folosită pentru a preveni distrugerea semnificativă, sau chiar înlăturarea marcajului în urma unor atacuri de *cropping*. Modul în care împrăştierea este efectuată depinde de cheia secretă, unică pentru fiecare marcaj în parte.

1.5.3 Căutarea pe *Web*. Copii ilegale ale produselor digitale sunt căutate pe paginile *web* accesibile şi suspecte. De aceea, marcarea transparentă ar trebui combinată şi cu o procedură automată de căutare pe *web*, notată cu *S*, care furnizează procedurii de detecţie a marcajului produsele găsite pe un anumit domeniu.

$$X = S\left(\text{domeniu de retea}\right), \quad X \in \mathbf{X} \tag{1.4}$$

1.5.4. Detecţia marcajului. Detectorul are la intrare un produs multimedia marcat sau nu şi posibil distorsionat, precum şi marcajul original. Răspunsul detectorului poate fi estimatul marcajului înglobat în semnalul multimedia $\hat{W}$, sau o valoare numerică care evidenţiază prezenţa sau absenţa marcajului [CMYY98]. În al doilea caz, algoritmul de detecţie este notat cu D şi definit după cum urmează [VP99]:

$$\mathcal{D}: \mathbf{X} \times \mathbf{K} \times \mathbf{W} \rightarrow \{0,1\}$$

$$\mathcal{D}\left(X, K, W\right) = \begin{cases} 1, & \text{daca } W \text{ exista in } X \\ 0, & \text{altfel} \end{cases} \tag{1.5}$$

Detecţia marcajului ar trebui să fie făcută fără a recurge la produsele originale. Folosirea originalelor poate genera un volum mare de calcul. Se generează mai întâi marcajul folosind G, bazat pe produsul *X*, care urmează a fi verificat şi pe cheia *K*. Procesul de detecţie şi extragere al marcajului este ilustrat în Figura 1.14.

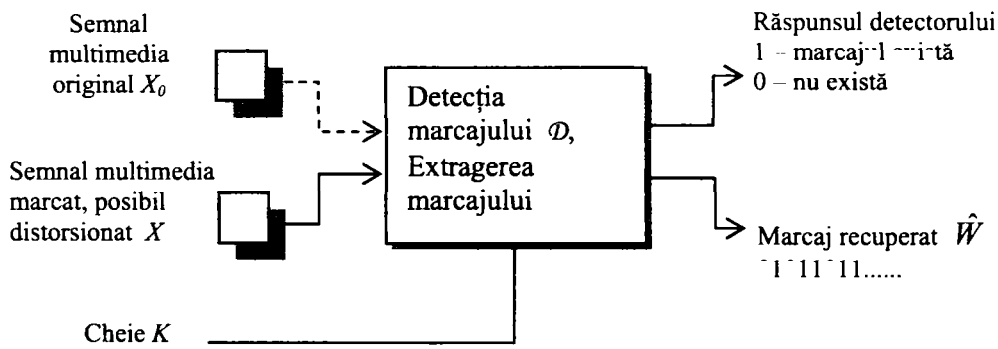


Fig. 1.14: Detecţia marcajului, fără, sau cu semnalul multimedia original.

Detectorul informat este cel care recurge la semnalul multimedia original pentru a verifica existenţa marcajului într-un semnal multimedia primit, care poate fi o versiune distorsionată a semnalului multimedia marcat [CMB02]. Dacă el nu are nevoie de semnalul original, detectorul este neinformat (*blind*). Cele două sisteme se numesc sistem de marcare *privat*, respectiv *public*.

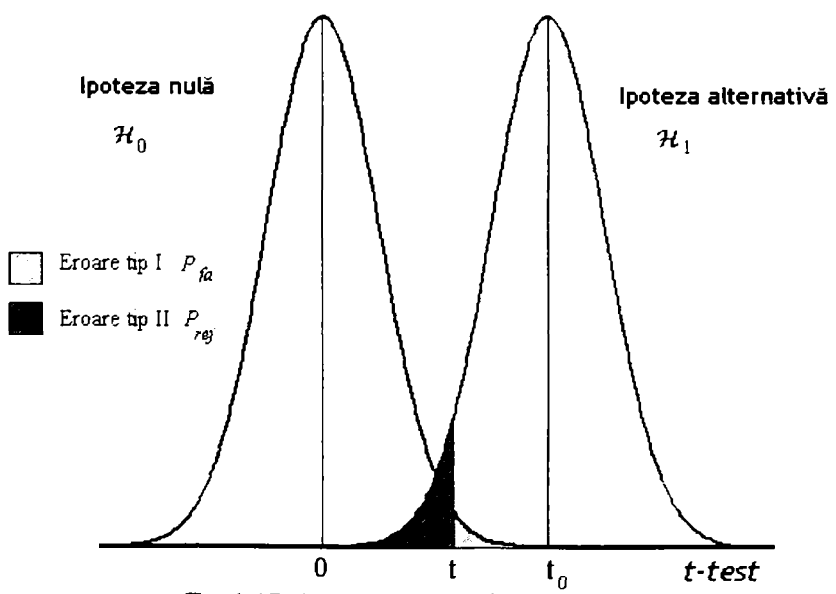


Fig. 1.15: Detecţia marcajului prin statistica t-test.
Ipotezele nulă şi alternativă reprezintă probabilităţile de inexistenţă sau de existenţă a marcajului. Erorile de tip I şi II sunt diferite de zero pentru orice valoare a lui t, derivată din t-test [Kay93].

În practică, realizarea lui $\mathcal{D}$ implică următoarele erori:

- tipul I de eroare: marcajul este detectat, deşi nu există (*fals pozitiv*).
- tipul II de eroare: marcajul nu este detectat, deşi există (*fals negativ*).

Erorile enunţate mai sus apar cu probabilităţile de alarmă falsă, P_{fa}, respectiv de rejecţie, P_{rej}. Ideea este de a minimiza P_{fa}. Pentru a avea un detector optimal, trebuie minimizată cealaltă eroare P_{rej}, sau echivalent de a maximiza 1- P_{rej}. Dar aceasta este chiar probabilitatea detecţiei, P_D, şi este criteriul Neyman-Pearson de testare a ipotezelor, adică în acest caz de detecţie a semnalelor. Dacă:

$$P_D = 1 - P_{rej} \tag{1.6}$$

este probabilitatea detecţiei corecte, atunci intenţia este de a maximiza P_D, pentru un prag P_{fa} impus [Kay93]. Testarea ipotezelor poate fi folosită pentru estimarea statistică a certitudinii şi a manipulării erorii. În general, când probabilitatea unui fals pozitiv devine nesemnificativă ($P_{fa} \to 0$), probabilitatea de a rejecta un marcaj creşte ($P_{rej} \to 1$) şi invers. Această situaţie este ilustrată în Figura 1.15 unde este considerată statistica t-test.

1.5.5 Căutarea în baze de date. Furnizorii şi creatorii îşi memorează produsele într-o bibliotecă personală notată cu $\mathcal{L}$. Dându-se un produs *X*, furnizorul ar trebui să fie capabil să găsească o metodă de potrivire/căutare $\hat{m}$ cu scopul de a verifica dacă *X* este sau nu inclus în biblioteca sa $\mathcal{L}$.

$$\hat{m}(X, \mathcal{L}) = \begin{cases} 1, \text{ dacă } X \in \mathcal{L} \\ 0, \text{ în rest} \end{cases} \tag{1.7}$$

O procedură de *matching* (identificare) este bazată, în general, pe algoritmi foarte complecşi. De aceea, nu este nici convenabil şi nici fezabil să se aplice procedura $\hat{m}$ tuturor produselor de pe domeniile web din sfera de interes. Procedura $\hat{m}$ este folosită pentru a confirma proprietatea asupra unui produs, atunci când detecţia marcajului se face cu un nivel de certitudine mic, dar nu neglijabil.

1.6 Proprietăţile principale ale metodei de marcare

Aşa cum am văzut, marcajele sunt structuri invizibile înglobate în *semnalul gazdă* pentru a „marca" proprietatea [KH98]. Din cadrul marcajelor fac parte codurile de *copyright* sau de autentificare, sau „legendele", care sunt absolut necesare pentru interpretarea semnalului. Aceste marcaje, existente în semnalul multimedia, trec neobservate de obicei şi pot fi depistate doar cu un detector adecvat. Cele mai răspândite tipuri de semnale care se marchează sunt imaginile statice, semnalele audio şi semnalele video numerice. În cele ce urmează, ne vom referi mai ales la *imagini statice*, aceleaşi principii putându-se aplica şi celorlalte tipuri de date.

1.6.1 Condiţii generale impuse marcării.

Fiecare aplicaţie de marcare transparentă îşi are cerinţele ei specifice. De aceea, nu există un set anume de cerinţe care să satisfacă toate tehnicile de marcare transparentă. Totuşi, pentru majoritatea aplicaţiilor menţionate mai sus, pot fi date nişte cerinţe generale [VP99, CKLS97, NP98, LSL00]:

- *Transparenţa perceptuală (imperceptibilitatea)*: în majoritatea aplicaţiilor, algoritmul de marcare transparentă trebuie să plaseze marcajul transparent în aşa fel încât acesta să nu afecteze calitatea datelor gazdă. Un marcaj transparent este într-adevăr imperceptibil, dacă observatorii umani nu pot distinge datele originale de datele marcate transparent. Totuşi, chiar şi cea mai nesemnificativă modificare în datele gazdă poate deveni vizibilă atunci când datele originale sunt comparate direct cu datele marcate transparent. În mod normal, utilizatorii nu au acces la datele originale şi nu pot efectua această comparaţie. De aceea poate fi suficient ca modificările din imaginea marcată transparent să treacă neobservate, atâta timp cât datele nu sunt comparate cu cele originale.
- *Încărcătura marcajului transparent*: cantitatea de informaţie care poate fi stocată într-un marcaj transparent depinde de aplicaţie. În scopul protejării la copiere, încărcătura de un singur bit este de obicei suficientă. Pentru protejarea drepturilor proprietăţii intelectuale, pare rezonabil să presupunem că se doreşte plasarea unei cantităţi de informaţie similară cu cea folosită pentru ISBN, International Standard Book Numbering, (10 cifre) sau ISRC, International Standard Recording Code (12 caractere alfanumerice). La toate astea, trebuie adăugat şi anul copyrightului, modificările permise asupra materialului, şi clasificarea acestor modificări. Aceasta înseamnă că aproximativ 60 de biţi de informaţie ar trebui să fie plasaţi în datele gazdă, imaginea, materialul video, sau fragmentul audio.
- *Granularitatea marcajului transparent* este un alt concept important cu privire la încărcătura marcajului transparent pentru date audio-video digitale. Fărâmiţarea marcajului transparent reprezintă cantitatea de informaţie necesară pentru plasarea unei unităţi de informaţie de marcaj. Folosind exemplul de mai sus, o unitate de informaţie de marcaj constă din 60 sau 70 de biţi. Aceştia ar putea fi plasaţi într-un singur cadru video, sau împrăştiaţi, de exemplu, asupra a 100 de cadre video.
- *Robusteţea*: un marcaj transparent fragil care trebuie să demonstreze autenticitatea datelor gazdă, nu trebuie să fie robust împotriva tehnicilor de procesare sau alterărilor intenţionate asupra datelor gazdă, deoarece eşecul detecţiei marcajului transparent demonstrează că datele gazdă au fost modificate şi nu mai sunt autentice. Totuşi, dacă un marcaj transparent este folosit pentru altă aplicaţie, este de dorit ca marcajul transparent să rămână întotdeauna în datele gazdă, chiar şi atunci când calitatea datelor gazdă a fost degradată, intenţionat sau neintenţionat. Exemple pentru degradări neintenţionate sunt aplicaţiile care implică transmisia sau stocarea de date, unde sunt folosite tehnici de compresie cu pierderi de date, pentru a reduce rata de bit şi a creşte eficienţa. Alte tehnici de prelucrare care degradează calitatea datelor în mod neintenţionat, includ filtrarea, re-eşantionarea, conversia analog-digitală şi digital-analogică. Pe de altă parte, marcajul transparent poate fi subiectul unor procesări cu intenţia de a-l elimina. Când există multe copii al

aceluiaşi conţinut, cu marcaje transparente diferite, ca în cazul amprentării, este posibilă eliminarea marcajului transparent datorită coliziunii dintre mai multe copii diferite. În general, nu ar trebui să existe nici o cale prin care marcajul transparent să fie eliminat sau modificat, fără degradarea suficientă a calităţii perceptuale a datelor gazdă.

- *Securitatea* tehnicilor de marcare transparentă poate fi interpretată în acelaşi mod ca şi securitatea tehnicilor de criptare. O tehnică de marcare transparentă este sigură, dacă cunoaşterea exactă a algoritmului de plasare şi extragere a marcajului transparent nu ajută o persoană neautorizată în detectarea prezenţei marcajului şi eliminarea ei.
- *Marcare publică şi marcare privată (oblivious/blind versus nonoblivious/non-blind)*: în unele aplicaţii, ca protecţia copyright şi monitorizarea datelor, algoritmii de extragere a datelor pot folosi imaginea originală nemarcată pentru a găsi marcajul transparent. Acest procedeu este numit marcare transparentă privată (nonoblivious watermarking). În majoritatea aplicaţiilor, cum ar fi protecţia la copiere şi indexarea, algoritmii de extragere a marcajului transparent nu au acces la imaginea originală, nemarcată. Acest lucru îngreunează extragerea marcajului transparent. Algoritmii de marcare transparentă de acest fel sunt publici (oblivious).
- *Universalitatea*: acelaşi algoritm de marcare transparentă ar trebui să fie aplicabil pentru toate cele trei tipuri de date considerate. Acest lucru serveşte în marcarea produselor multimedia. De asemenea, această caracteristică este favorabilă pentru implementarea de algoritmi de marcare a imaginilor şi semnalelor video pe suport hardware comun.
- *Neambiguitatea*: recuperarea marcajului ar trebui să identifice fără îndoială proprietarul. De asemenea, acurateţea identificării proprietarului ar trebui să se degradeze progresiv cu creşterea forţei atacurilor.

Alte proprietăţi pe care marcajele ar trebui să le aibă sunt [VP99]:

- *Complexitatea*: semnalele de marcare ar trebui să fie foarte complexe. Acest lucru este necesar pentru a se putea produce un set suficient de marcaje sesizabile. Un set foarte mare de marcaje previne refacerea unui marcaj anumit, prin proceduri iterative de tip *trial and error*. În majoritatea cazurilor, complexitatea unei marcaj este direct legată de mărimea produsului în care trebuie să fie înglobată.
- *Cheia asociată*: marcajele ar trebui să fie asociate cu un număr de identificare numit cheia marcajului. Cheia este folosită pentru a forma, detecta şi înlătura marca. Prin urmare, cheia ar trebui să fie privată şi să caracterizeze exclusiv proprietarul legal. Orice semnal digital extras dintr-un produs digital se presupune că este marcajul dacă şi numai dacă el este asociat cu o cheie printr-un algoritm bine stabilit. Această condiţie previne crearea unor marcaje contrafăcute, discutate de Craver pe larg în [CMYY98].
- *Detecţia/căutarea automată*: marcajele ar trebui să combine în mod facil o metodă de căutare care scanează automat orice domeniu accesibil în reţea.
- *Detecţia de încredere*: marcajele ar trebui să constituie o dovadă suficientă şi de încredere a proprietăţii asupra unui anume produs. Alarmele false ar trebui să apară foarte rar, de preferinţă niciodată. Un anumit marcaj este o dovadă credibilă pentru a demonstra posesia dreptului de autor atunci când probabilitatea de eroare la detecţie este nesemnificativă. Totuşi, detecţia cu un

nivel de certitudine scăzut poate fi făcută cu scopul de a reduce probabilitatea de refuz P_{rej} în timpul monitorizării pe *web*.

- *Invizibilitatea statistică*: marcajele nu ar trebui să poată să fie refăcute folosind metode statistice. De exemplu, proprietatea unui număr mare de produse digitale, marcate cu aceeaşi cheie, nu ar trebui să permită extragerea marcajului aplicând metode statistice. De aceea, marcajele ar trebui să depindă de conţinutul produsului.
- *Marcajele multiple*: ar trebui să fim capabili să înglobăm un număr suficient de marcaje în aceeaşi imagine. Fiecare marcaj ar trebui să fie detectabil folosind cheia unică corespunzătoare. Această caracteristică pare să fie necesară, deoarece nu putem preveni ca cineva să marcheze un produs deja marcat. Este de asemenea avantajos în cazurile în care dreptul de autor este transferat de la un proprietar la altul (un proces asemănător celui de amprentare). Menţionăm că proprietarul legal al imaginii este singurul care poate dispune de o copie a imaginii care conţine *doar* marcajul său.

Cerinţele de mai sus sunt legate una de alta. De exemplu, poate fi obţinut un marcaj transparent foarte robust prin modificări mari asupra datelor gazdă, pentru fiecare bit al marcajului transparent. Totuşi, modificările mari în datele gazdă sunt observabile, şi multe modificări la biţii de marcaj, vor limita cantitatea maximă de biţi ai marcajului transparent care pot fi stocaţi în obiectul gazdă. Deci, trebuie considerat un compromis între diferitele cerinţe, astfel putând fi dezvoltat un marcaj transparent optim pentru fiecare aplicaţie.

Dependenţele mutuale dintre cerinţele de bază sunt arătate în figura 1.16. Relaţia dintre cerinţele de bază pentru un marcaj transparent sigur, bine proiectat, sunt prezentate în figura 1.17.

Axa de impact perceptual reprezintă degradarea calităţii datelor din cauza marcării transparente. Cu cât este mai mare impactul perceptual, cu atât este mai gravă degradarea calităţii. Axa încărcăturii reprezintă cantitatea de date care poate fi plasată în date. Axa robusteţii reprezintă capacitatea sistemului de marcare transparentă de a rezista la atacuri. Securitatea unui marcaj transparent influenţează enorm robusteţea. Dacă un marcaj transparent nu este sigur, nu poate fi foarte robust.

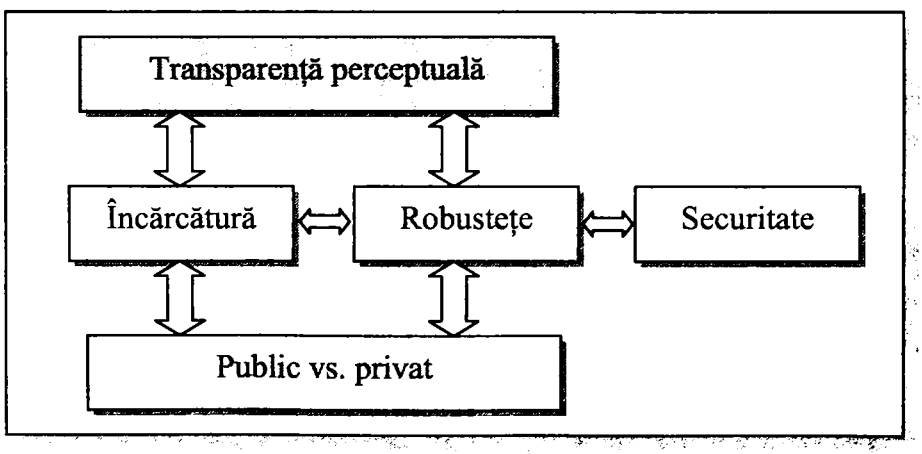


Fig. 1.16: Interdependenţele dintre cerinţele de bază pentru un marcaj eficient

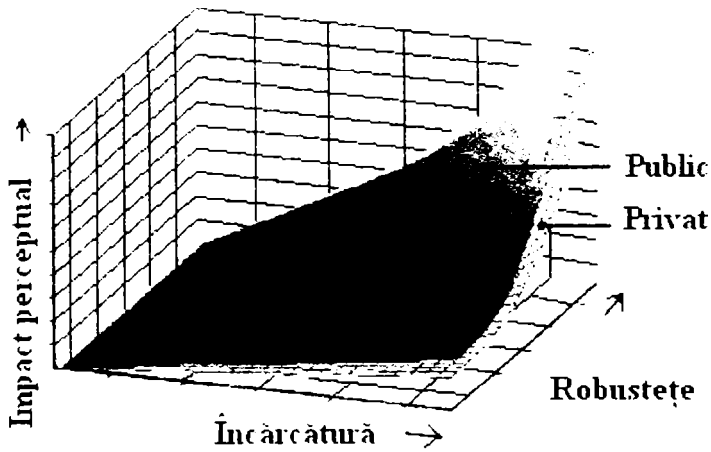


Fig. 1.17: Relaţia dintre cerinţele de bază pentru un marcaj sigur

1.6.2 Condiţii specifice impuse marcării

A. Protecţia dreptului de autor. Pentru a fi eficient, marcajul trebuie să fie dificil, teoretic imposibil de înlăturat. Dacă se dispune doar de o informaţie parţială despre marcaj (de exemplu, nu se cunoaşte cu exactitate localizarea marcajului în imagine), atunci încercările de înlăturare sau de distrugere a marcajului ar trebui să conducă la degradarea severă a calităţii imaginii. Evident, un marcaj folosit cu scopul de protejare a dreptului de autor ar trebui să fie detectabil, până în punctul în care calitatea produsului rămâne în limite acceptabile pentru orice tip de modificare. În particular, un marcaj ar trebui să fie robust la:

a. *Prelucrări obişnuite ale semnalului*: marcajul ar trebui să poată fi încă extras, chiar dacă imaginii i se aplică procesări obişnuite. Acestea pot fi conversii D/A, A/D, reeşantionare, compresie cu pierderi, precum şi îmbunătăţiri obişnuite aplicate unei imagini cum ar fi îmbunătăţirea contrastului, corecţia culorilor, egalizarea histogramei etc.
b. *Distorsiuni geometrice obişnuite (pentru imagini şi video):* marcajele din imagini şi video ar trebui să fie rezistente şi la operaţii geometrice cum ar fi rotire, translaţie, decupare, scalare.
c. *Atacuri de subterfugiu (prin înţelegere secretă/complot şi falsificare)*: marcajul ar trebui să fie robust împotriva atacului combinat, lansat de mai mulţi indivizi care posedă fiecare o copie marcată. Cu alte cuvinte, marcarea ar trebui să fie robustă împotriva combinării copiilor aceluiaşi original. De asemenea, dacă un marcaj urmează să fie folosit ca probă juridică, trebuie să fie imposibil pentru atacatori să combine imaginile lor pentru a genera un marcaj diferit, valid, cu intenţia de a înşela o terţă parte.

B. Verificarea conţinutului. Protecţia originalităţii conţinutului cere o invizibilitate perceptuală, complexitate a marcajului, validitate a cheii, detecţie de încredere şi invizibilitate statistică. În aplicaţiile în care trebuie detectate cele mai neînsemnate modificări făcute asupra produselor în care au fost înglobate sunt

cerute marcaje *fragile*. În cazurile în care modificările nu afectează autenticitatea este dorită *robusteţea*, adică:

1. *Compresia mare*
2. *Înlăturarea părţilor neinteresante*
3. *Alte modificări nesemnificative,* făcute pentru a introduce produsul într-un mediu multimedia.

1.7 Marcare şi înregistrare pentru o protecţie eficientă

Tehnicile de marcare dezvoltate până astăzi, prezintă diferite *dezavantaje* care împiedică formarea unui sistem de protecţie universal, de încredere, bazat exclusiv pe marcare. Principalele dezavantaje sunt [VP99]:

1-Instabilitatea în raport cu pierderea/furtul cheii : marcarea se bazează pe o cheie privată constantă. Când un atacator află sau găseşte o cheie privată, el are posibilitatea să înlăture marcajele corespondente cheii respective din toate produsele în mod direct. Ulterior, violarea dreptului de autor pentru toate produsele furnizorului respectiv devine o sarcină uşoară. De asemenea, pot fi distribuite produse falsificate.

2-Robusteţe/fragilitate eficientă: marcajele folosite pentru protecţia dreptului de autor ar trebui să fie robuste la toate modificările posibile. De asemenea, verificarea conţinutului necesită marcaje cu o fragilitate adecvată faţă de o varietate de procesări. Cererile de mai sus nu se ating cu uşurinţă.

3-Eficienţa marcajului împotriva tehnicilor noi de procesare sau atacuri: este testată robusteţea marcajului, securitatea şi rezistenţa lui la atacuri pentru tehnicile de procesare cunoscute până în prezent. Marcarea nu poate să îşi garanteze eficienţa în viitor. În viitor ar putea fi dezvoltate noi tehnici de compresie sau de filtrare, care să înlăture cu uşurinţă marcajele din produsele deja distribuite.

4-Detecţia publică nesigură: detecţia marcajului folosind chei publice este esenţială pentru verificarea conţinutului. Totuşi, detecţia publică poate crea dificultăţi în dezvoltarea tehnicilor de marcare sigure şi eficiente împotriva atacurilor pirat. Din cauza problemelor menţionate anterior, marcarea nu poate asigura singură o protecţie eficientă. Totuşi, ea poate constitui o parte importantă a unei metode de ansamblu de protecţie.

Înregistrarea produselor la o autoritate de încredere este o cale bine cunoscută pentru protejarea drepturilor de proprietate intelectuală (pentru cărţi, software, etc). Informaţiile de înregistrare pot fi folosite ca o dovadă inatacabilă a proprietăţii şi drepturilor legale. Un sistem de protecţie bazat pe înregistrarea produsului necesită următoarele acţiuni:

1. Furnizorul este o autoritate de încredere, care furnizează o cheie de marcare unică.
2. Înglobarea marcajului se face folosind cheia înregistrată.
3. Produsul marcat este înregistrat la autoritatea de încredere înainte de a fi distribuit.

Copia înregistrată este datată, fiind marcate atât originalitatea cât şi proprietatea legală. Înregistrarea după marcare poate contribui la o protecţie eficientă în diferite moduri. Se pot observa următoarele:

- Furnizorul face o căutare automată a marcajului în reţea. Când se foloseşte un nivel de certitudine scăzut, siguranţa unui rezultat pozitiv este refăcută căutând în biblioteca $\mathcal{L}$. Deţinerea unei copii înregistrate este dovada proprietăţii dreptului de autor, în faţa justiţiei.

- Verificarea conţinutului poate fi făcută de autoritatea de înregistrare şi de un server public destinat acestui scop. Utilizatorul care doreşte să îşi verifice conţinutul unui produs, ar trebui să acceseze acel server particular, la care produsul a fost înregistrat. Serverul poate verifica integritatea conţinutului făcând o marcare privată şi apoi trimiţând rezultatul către utilizator.

1.8 Modele de bază pentru watermarking

Dezvoltarea unei tehnici de marcare ia în considerare mai multe aspecte. Multe dintre tehnicile existente „împrumută" concepte din alte domenii de cercetare.

Figura 1.18 prezintă câteva din elementele avute în vedere de o tehnică de marcare. Alegerea acestor elemente pentru o metodă de marcare, pentru o aplicaţie dată, este încă neclară, deoarece pentru anumite aplicaţii, trebuie făcut un compromis între imperceptibilitate, robusteţe şi complexitate.

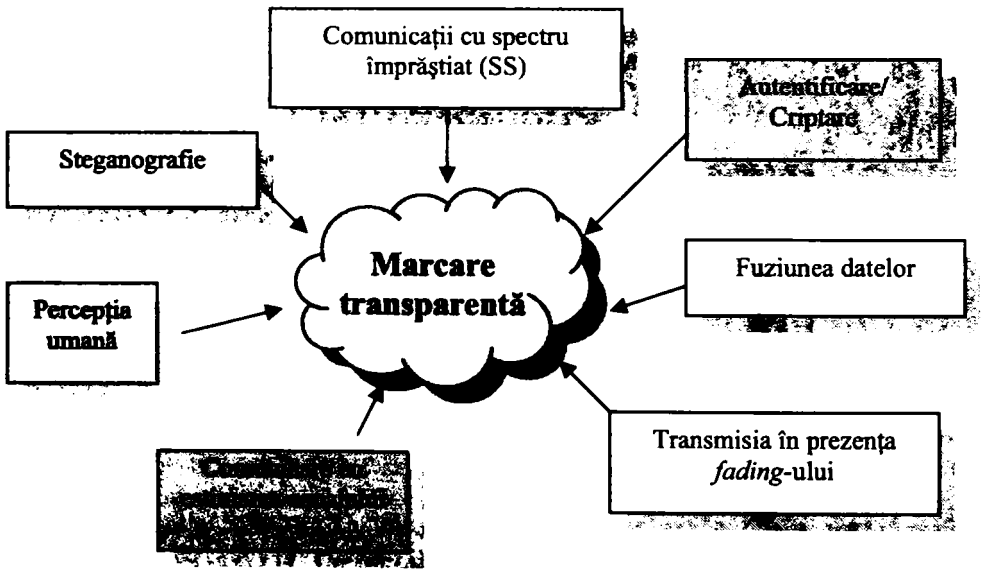


Fig. 1.18: Domeniile de cercetare care sunt în strânsă legătură cu marcarea semnalelor multimedia.

În cele ce urmează, se enumeră câteva domenii care au contact cu marcarea transparentă [Kun99].

1. *Steganografia* se referă la modul de comunicare ascunsă (*data hiding*). Problema principală este mascarea unui mesaj secret în orice tip de semnal gazdă (nu numai multimedia). Marcarea numerică şi steganografia se aseamănă foarte mult, exceptând faptul că în tehnicile de marcare, se pune accent pe robusteţea sau fragilitatea marcajului [CMB02].

2. *Comunicaţiile cu spectru împrăştiat* (*Spread Spectrum* - SS) sunt extrem de asemănătoare cu marcarea transparentă. Procedura de înglobare a marcajului se aseamănă cu transmiterea unui semnal SS (marcaj) printr-un mediu zgomotos (semnalul gazdă). Extragerea marcajului este

echivalentă cu detecţia semnalului SS dintr-un mediu cu interferenţe [CKLS97].

3. *Modelele perceptuale umane* sunt des folosite pentru codarea perceptuală a semnalelor multimedia. Se exploatează proprietatea de mascare a percepţiei umane, permiţându-se astfel o introducere mai eficientă a marcajului. Astfel, se îmbunătăţeşte robusteţea marcajului sau estimarea modificărilor făcute asupra semnalului [CMB02].

4. *Autentificarea şi criptarea* se folosesc în strânsă legătură cu tehnicile de marcare, într-un sistem de protecţie universal. De altfel, sistemele de marcare împrumută deseori modelele folosite în criptare, realizând o înglobare elegantă [VP99, CMB02, BB01].

5. *Fuziunea datelor* este o problemă fundamentală de compresie a informaţiei, în care mai multe semnale sunt „adunate" pentru a forma unul singur, conţinând informaţia cea mai relevantă de la fiecare din semnalele respective. Această problemă se aseamănă cu problema marcării, în care semnalul original şi semnalul de marcaj formează semnalul marcat, care trebuie să reţină proprietăţile perceptuale ale semnalului gazdă, dar şi informaţia marcajului [ZWL03, CM98].

6. *Transmisia semnalului în prezenţa fading-ului* este o problemă care se referă la comunicaţii fără fir, ce implică folosirea unor strategii pentru a combate atenuarea semnalului în timp [KH01]. În acest context, robusteţea marcajului poate fi considerată capacitatea lui de a rezista interferenţelor într-un canal cu *fading*.

7. *Estimarea canalului* este necesară în orice sistem de comunicaţii. Combaterea efectelor distorsiunilor canalelor este cu atât mai eficientă, cu cât sunt mai corecte şi exacte modelele de canale propuse, conform unor estimări prealabile. Caracterizarea atacurilor înainte de extragerea marcajului poate îmbunătăţi simţitor performanţa unui sistem de marcare [KH01]. Pentru sistemele de marcare fragile, caracterizarea atacurilor se foloseşte pentru a evalua credibilitatea semnalului modificat; pentru sisteme de marcare robuste, caracterizarea atacurilor se foloseşte pentru a creşte credibilitatea estimării marcajului.

1.9 Evaluarea performanţelor unei metode de marcare

Un algoritm de marcare este evaluat printr-o serie de măsurări. Din cauza aspectului subiectiv al problemei, nu toate criteriile de evaluare sunt cantitative. Se prezintă în cele ce urmează cele mai folosite criterii de evaluare pentru imagini.

1. *Imperceptibilitatea.* Marcajul nu ar trebui să fie vizibil, respectiv supărător [CKLS97]. Cu alte cuvinte, un utilizator nu ar trebui să fie capabil să facă distincţia între semnalul marcat şi cel original.

2. *Raportul dintre puterea maximă a semnalului şi puterea zgomotului (Peak Signal-To-Noise Ratio PSNR).* Pentru a stabili un criteriu mai obiectiv al imperceptibilităţii, este folosit şi PSNR pentru a măsura „zgomotul" adăugat

imaginii originale, ca rezultat al înglobării marcajului. Deşi această măsură nu este totdeauna cea mai potrivită, ea poate fi folositoare pentru a indica echilibrul între invizibilitatea marcajului şi eficienţa procesului de „ascundere" a datelor. PSNR se defineşte astfel:

$$PSNR(f,w)=10\log_{10}\left[\frac{\max_{\forall(m,n)}f^2(m,n)}{\frac{1}{N}\sum_{\forall(m,n)}\left(f_w(m,n)-f(m,n)\right)^2}\right] \tag{1.8}$$

unde f este semnalul gazdă, f_w este semnalul marcat, w este marcajul, (m,n) reprezintă localizarea unui anumit pixel, iar N este numărul de pixeli din f sau f_w. PSNR se măsoară în dB.

3. *Coeficientul de intercorelaţie*. Pentru a măsura similaritatea între marcajele original şi extras, se calculează coeficientul normalizat de intercorelaţie [CMB02, ZWL03, CMYY98]:

$$\rho(w,\hat{w})=\frac{\sum_{i=1}^{N_w}w(i)\hat{w}(i)}{\sqrt{\sum_{i=1}^{N_w}w^2(i)}\sqrt{\sum_{i=1}^{N_w}\hat{w}^2(i)}} \tag{1.9}$$

unde $w(i)$ şi $\hat{w}(i)$ reprezintă semnalele de marcare original şi, respectiv extras; N_w este lungimea marcajului. O metodă de marcare robustă încearcă să maximizeze acest coeficient de intercorelaţie, atunci când semnalul este distorsionat, iar o metodă de marcare fragilă încearcă să îl minimizeze, în cazul unor modificări majore.

4. *Distanţa Hamming normalizată.* Dacă marcajul este alcătuit din elemente binare, pentru a măsura similaritatea dintre cele două marcaje, se poate calcula distanţa Hamming normalizată dintre marcajele original şi extras [CMB02], în loc de coeficientul de intercorelaţie. Aceasta este dată de următoarea relaţie:

$$\rho_{\mathrm{HD}}(w,\hat{w})=\frac{1}{N_w}\sum_{i=1}^{N_w}w(i)\oplus\hat{w}(i) \tag{1.10}$$

unde w, $\hat{w}$ şi N_w sunt definite la fel ca şi în ecuaţia (1.2), iar operatorul $\oplus$ este SAU-EXCLUSIV (XOR).

5. *Probabilitatea unui fals pozitiv sau negativ.* În aplicaţiile de securitate informaţională, este necesară detecţia marcajului sau detecţia oricărui tip de modificare făcută cu scopul de a-l înlătura. Probabilitatea ca marcajul sau modificarea semnalului marcat să nu fie detectate se numeşte *probabilitatea unui fals negativ*. Asemănător, probabilitatea ca un marcaj să fie detectat, când el nu există se numeşte *probabilitatea unui fals pozitiv* [VP99, CMB02].

6. *Complexitatea de calcul.* În funcţie de aplicaţia cerută, complexitatea de calcul poate fi un factor semnificativ în estimarea performanţelor unui algoritm de marcare [CMB02]. De exemplu, extragerea marcajului la un DVD-player trebuie realizată în timp real, dar în marcarea imaginilor pentru protejarea proprietăţii intelectuale, acest fapt poate să nu aibă o importanţă foarte mare.

1.10 Marcarea robustă

Robusteţea se referă la capacitatea marcajului de a fi recuperat după procesări de semnal obişnuite şi depinde de aplicaţie. Astfel de procesări pot fi: compresia cu pierderi, conversia numerică, atacul de imprimare şi scanare (*printing and scanning*), înregistrarea analogică (casete VHS), reducerea zgomotului, conversia dintr-un format în altul (exemplu trecerea de la NTSC la PAL). Robusteţea este limitată de o serie de parametri, dintre care cei mai importanţi sunt costul de calcul al algoritmului de marcare, încărcătura marcajului (*payload*) şi fidelitatea impusă semnalului marcat faţă de cel original.

Spre exemplu în aplicaţia de monitorizare a transmisiilor TV (*broadcast monitoring*) marcajul trebuie să fie robust la conversii D-A şi A-D, compresie cu pierderi, jitter, dar nu este necesar să fie robust la rotaţie, înregistrare analogică, conversie dintr-un format în altul. De asemenea costul erorilor diferă în aplicaţii: costul de fals negativ este mare pentru broadcast monitoring, în timp ce costul de fals pozitiv este mare pentru controlul copierii (copy control).

1.10.1 Problema detecţiei optime

Dacă se ia un exemplu simplu, de sistem de marcare [CMB02], în care $\mathbf{c_0}$ este imaginea originală, $\mathbf{w}$ - marcajul, α - intensitatea marcajului, imaginea marcată va fi:

$$\mathbf{c}_w = \mathbf{c}_0 + \alpha \mathbf{w} . \qquad (1.11)$$

Fiind dată imaginea posibil marcată $\mathbf{c}$, şi $\mathbf{c_0}$ imaginea originală, se extrage marcajul

$$\mathbf{w}_n = \mathbf{c} - \mathbf{c}_0 \approx \alpha \mathbf{w} \text{ dacă marcajul este prezent} .$$

Se poate folosi corelaţia liniară pentru a determina dacă $\mathbf{w}_n \cong \alpha \mathbf{w}$:

$$z_{lc}(\mathbf{w}_n, \mathbf{w}) = \frac{1}{N}\mathbf{w}_n \cdot \mathbf{w} = \frac{1}{N}\sum_{x,y}\mathbf{w}_n[x,y]\cdot\mathbf{w}[x,y], \qquad (1.12)$$

unde N este numărul de pixeli din imagine.
Imaginea originală, posibil afectată de zgomot AWGN, este:

$$\mathbf{c} = \mathbf{c}_0 + \mathbf{n} \qquad (1.13)$$

Dacă marcajul nu este prezent în imaginea originală, atunci valoarea corelaţiei liniare devine:

$$z_{lc}(\mathbf{w}_n, \mathbf{w}) \cong 0,$$

iar dacă marcajul este prezent, şi imaginea marcată a fost afectată de zgomot:

$$\mathbf{c}_w = \mathbf{c}_0 + \alpha\mathbf{w} + \mathbf{n}.$$

Atunci

$$z_{lc}(\mathbf{w}_n, \mathbf{w}) = \alpha z_{lc}(\mathbf{w}, \mathbf{w}) \quad \text{(marcajul este prezent).}$$

Dacă **w** este ales astfel încât corelaţia între $\mathbf{c_0}$ şi **w** este apropiată de 0 (**w** este zgomot alb), atunci $z_{lc}(\mathbf{c}, \mathbf{w}) \cong z_{lc}(\mathbf{w}_n, \mathbf{w})$. Prin urmare detecţia se poate face şi *neinformat* (fără a cunoaşte imaginea originală).

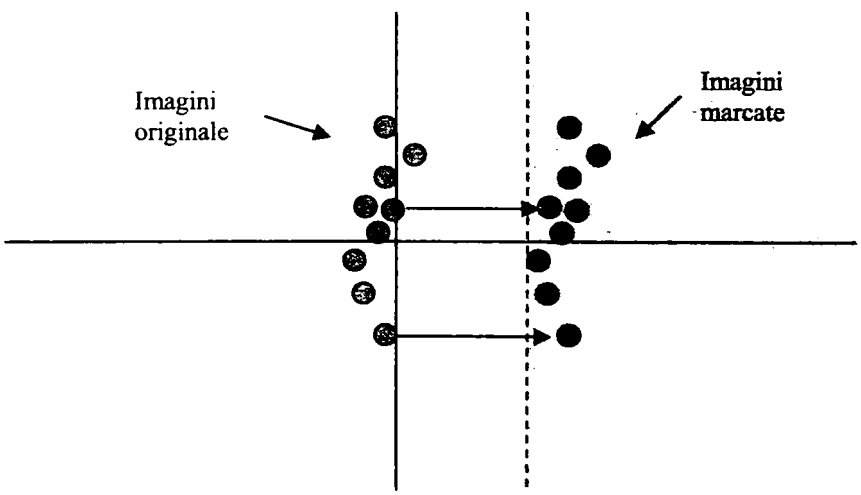


Fig. 1.19: Interpretarea geometrică a corelaţiei liniare.

Fie spaţiul media un spaţiu multidimensional, în care fiecare imagine are asociat un punct, iar pentru simplitate se poate considera că acesta are doar două dimensiuni. Corelaţia liniară este produsul scalar între **c** şi **w** scalat cu $1/N$, adică:

$$z_{lc}(\mathbf{c},\mathbf{w}) = \frac{1}{N}\mathbf{c}\cdot\mathbf{w} = \frac{1}{N}|\mathbf{c}|\cdot|\mathbf{w}|\cos\measuredangle(\mathbf{c},\mathbf{w}) \tag{1.14}$$

Dacă $|\mathbf{w}| = 1$, atunci corelaţia liniară este chiar proiecţia lui **c** pe direcţia lui **w**.

Prin urmare, dacă se compară $z_{lc}(\mathbf{c},\mathbf{w})$ cu un prag, se ajunge la o regiune de detecţie de tip plan [CMB02, Cox05].

Zgomotul AWGN. Dacă imaginea este coruptă de zgomot AWGN,

$$\mathbf{c}_{wn} = \mathbf{c}_w + \mathbf{n}$$

atunci corelaţia liniară (filtrare adaptată) este optimală după criteriul Neyman-Pearson [Kay93]:

$$z_{lc}(\mathbf{w},\mathbf{c}_{wn}) = \frac{1}{N}(\mathbf{w}\cdot\mathbf{c}_w + \mathbf{w}\cdot\mathbf{n}) \tag{1.15}$$

Contrastul imaginii. Dacă se schimbă contrastul imaginii, atunci imaginea devine $\mathbf{c}_{wn} = \upsilon\mathbf{c}_w$, unde υ este o valoare reală. Rezultă corelaţia liniară :

$$z_{lc}(\mathbf{c}_{wn},\mathbf{w}) = \upsilon z_{lc}(\mathbf{c}_w,\mathbf{w}) \tag{1.16}$$

Daca $\upsilon < 1$ valoarea corelaţiei poate scădea sub valoarea de prag. Pentru creşterea probabilităţii de detecţie, se poate recurge la corelaţia normalizată:

$$z_{nc}(\mathbf{c},\mathbf{w}) = \frac{\mathbf{c}\cdot\mathbf{w}}{|\mathbf{c}|\cdot|\mathbf{w}|} \tag{1.17}$$

Atunci, ajustarea contrastului nu are efect asupra detectorului [Cox05]:

$$z_{nc}(\nu\mathbf{c},\mathbf{w}) = \frac{\upsilon\mathbf{c}\cdot\mathbf{w}}{\upsilon|\mathbf{c}|\cdot|\mathbf{w}|} = z_{nc}(\mathbf{c},\mathbf{w})$$

Interpretarea geometrică a detectorului cu corelaţie normalizată. Corelaţia normalizată este cosinusul unghiului dintre cei doi vectori. Prin urmare, compararea lui $z_{nc}(\mathbf{c},\mathbf{w})$ cu un prag este echivalentă cu compararea unui unghi cu un prag, ceea ce duce la o regiune de detecţie de formă conică [CMB02, Cox05].

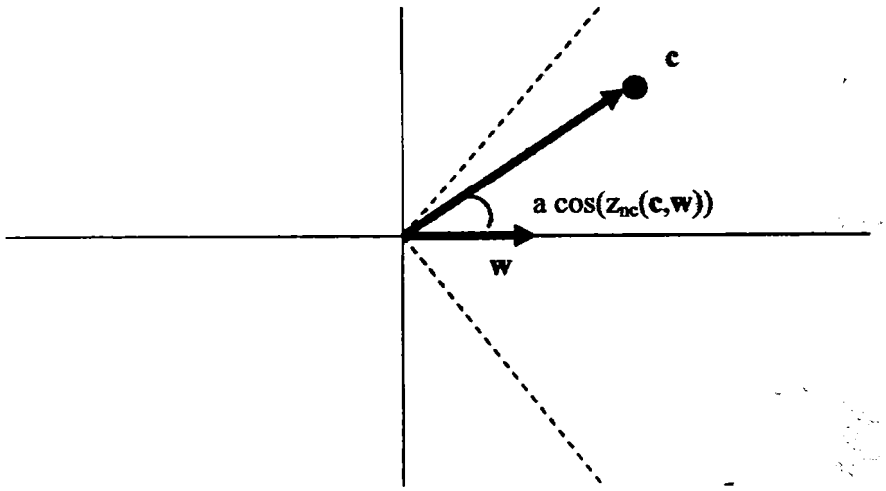


Fig. 1.20: Interpretarea geometrică a corelaţiei normalizate.

Cuantizarea, care are loc în timpul compresiei semnalului multimedia, nu poate fi modelată ca un zgomot alb aditiv AWGN; în prezent se fac eforturi pentru modelarea zgomotului de cuantizare [CMB02].

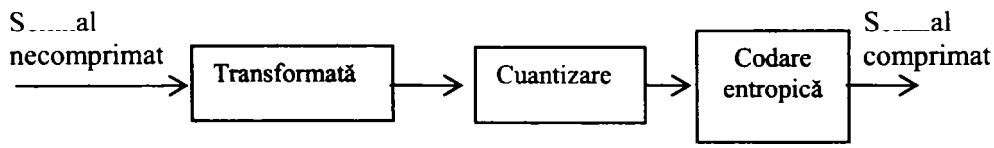


Fig. 1.21: Reprezentarea canonică a compresiei folosind o transformată.

Desincronizarea marcajului extras faţă de cel original, care poate fi produsă de distorsiuni geometrice pentru imagini, respectiv de distorsiuni temporale pentru semnale audio şi video, nu poate fi nici ea modelată ca zgomot AWGN. Există metode pentru a compensa efectul desincronizării marcajului.

Un *marcaj de referinţă* este înglobat în plus faţă de cel care poartă efectiv informaţia. Înainte de detecţia marcajului propriu-zis, trebuie „căutat" marcajul de referinţă; este posibilă detecţia prin autocorelaţie. Această abordare are un impact negativ asupra fidelităţii si securităţii.

O altă modalitate este *sincronizarea implicită*, sau *folosirea proprietăţii de invarianţă*. De exemplu, modulul transformatei Fourier este invariant la translaţie. Dacă imaginea este translatată, valoarea de detecţie depinde de autocorelaţia marcajului, care, pentru zgomotul alb este aproape de zero. De aceea, marca este puţin probabil să fie detectată. Astfel, în loc de domeniul spaţial, o soluţie ar fi folosirea unei transformate invariante la translaţie.

Sistemul de marcare poate fi privit ca fiind compus din două părţi [CMB02]:

- procesul de *extragere* a marcajului care proiectează elementele din domeniul media, în domeniul marcajului,
- un sistem de *marcare* simplu în domeniul marcajului, aşa cum este descris mai sus.

Domeniul marcajului poate fi această transformată $\mathcal{T}$. Procesul de extragere a marcajului creşte robusteţea pentru că se trece într-un spaţiu invariant la distorsiuni, care le inversează şi care reduce zgomotul; de asemenea, dacă se foloseşte o cheie, se reduce complexitatea de calcul si creşte gradul de securitate. Dacă transformata $\mathcal{T}$ este liniară şi conservă energia atunci corelaţia liniară va fi:

$$z_{lc}\left(\mathcal{T}(\mathbf{c}),\mathbf{w}\right)=z_{lc}\left(\mathbf{c},\mathcal{T}^{-1}(\mathbf{w})\right). \qquad (1.18)$$

Rezultă că un sistem de marcare în domeniul transformatei $\mathcal{T}$ este echivalent cu un sistem în domeniul spaţial, care foloseşte un model diferit de marcare. Sistemul este diferit tocmai prin *neliniaritatea procesului de extragere* a marcajului.

Un exemplu simplu de *neliniaritate a sistemului* este *mascarea perceptuală*, care amplifică marcajul în zone în care zgomotul este mai puţin vizibil [CMB02].

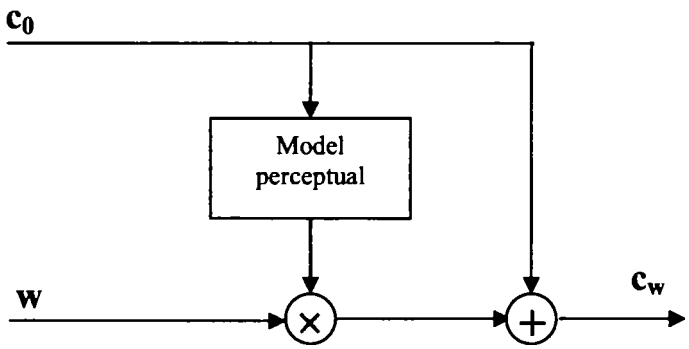


Fig. 1.22: Mascare perceptuală în înglobarea marcajului.

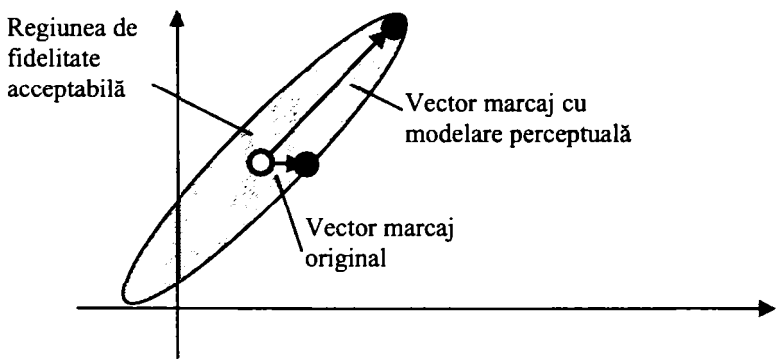


Fig. 1.23: Interpretarea geometrică a modelării perceptuale.
Marcajul obţinut prin modelare perceptuală poate fi multiplicat cu o valoare mai mare a intensităţii, fără depăşirea nivelului de distorsiune acceptabilă, ceea ce duce la o valoare de detecţie mai mare.

Detecţia se poate face inversând modelarea (mascarea) perceptuală la detector. Cu toate acestea, s-a constatat mai târziu că acest pas nu este necesar: distorsiunea modelului de marcaj degradează şi valoarea de detecţie, pentru un

parametru α dat; dar se pot folosi valori mai mari ale intensităţii de marcare α, dat fiind faptul că marcajul este mai puţin vizibil [Cox05].

1.10.2 Soluţii pentru asigurarea robusteţii

Există mai multe soluţii pentru a asigura robusteţea:

- *Folosirea unor proprietăţi invariante* la înserare, pentru ca marcajul să rămână neschimbat. Marcarea invariantă asigură că marcajul nu va fi schimbat de prelucrări de semnal folosind proprietăţi invariante (cum ar fi o transformată); se foloseşte câteodată pentru distorsiunile geometrice, dar este mai potrivită pentru alte tipuri de distorsiuni, cum ar fi filtrarea trece-jos. Soluţia este înglobarea marcajului în coeficienţii de joasă frecvenţă.

- *Inversarea distorsiunii la detector*. Distorsiunile pot fi inversate la detector, fiindcă multe din acestea sunt inversabile: rotirea, translaţia, redimensionarea. O altă soluţie este distorsionarea marcajului original înainte de corelaţie, dar dificultatea majoră este găsirea parametrilor de distorsiune.

- *Pre-inversarea distorsiunii la înglobare*. În unele aplicaţii se cunoaşte tipul de distorsiuni ce pot interveni. Se poate înfloba un marcaj "anti-distorsionant", astfel încât după distorsiune marcajul este similar cu cel original. Spre exemplu, raportul de aspect se schimbă din 16:9 în 4:3 dacă se trece din format DVD sau HDTV la SDTV (în cazul video).

- *Înglobarea marcajului în mod redundant*. Înglobarea redundantă a marcajului se poate face în domeniul spaţial, combinând repetiţiile apoi testând, sau invers, testând fiecare parte redundantă apoi combinând rezultatele [KH01]. Alte posibilităţi de înglobare redundantă sunt codurile corectoare de erori, marcarea folosind comunicaţiile cu spectru împrăştiat, etc.

- *Înglobarea marcajului în coeficienţii de robusteţe cunoscută*. Înglobarea se poate face în coeficienţi mai robuşti; această sensibilitate se poate modela sau se poate obţine experimental [CKLS97, NB05, NC05b, NC05a, NIB05].

- *Înglobarea marcajului în regiuni semnificative perceptual*. O altă abordare este înglobarea marcajului în zone semnificative perceptual deşi, în mod logic, acest lucru duce la scăderea valorii comerciale a produsului respectiv. În acest scop, se pot folosi tehnicile de tip *spread-spectrum* [CKLS97]. Rezultatul este că marcajul nu va fi distrus în urma compresiei, care înlătură părţile perceptual nesemnificative.

1.10.3 Marcarea informată

În Figurile 1.24-1.26 se prezintă procesul de *înglobare a marcajului*, funcţie de tipul de *codare* şi de *formare* a acestuia: *informat* respectiv *neinformat* [Cox05]. Marcarea informată foloseşte informaţii despre imaginea originală în codarea marcajului, şi pentru formarea marcajului (Figura 1.26).

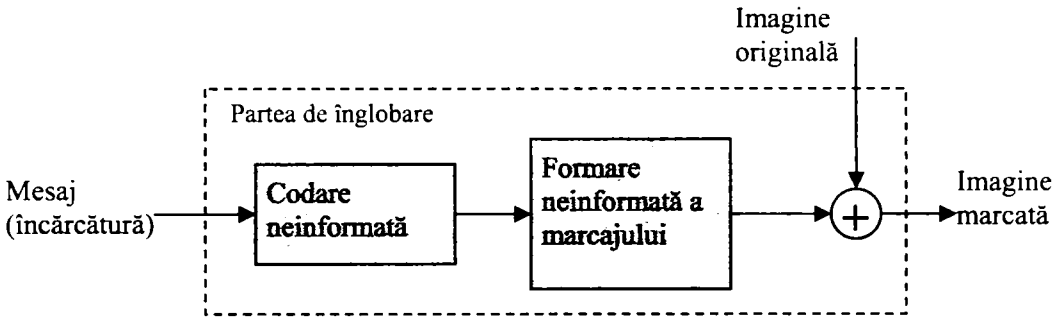


Fig. 1.24: Codare neinformată şi formare neinformată a marcajului.

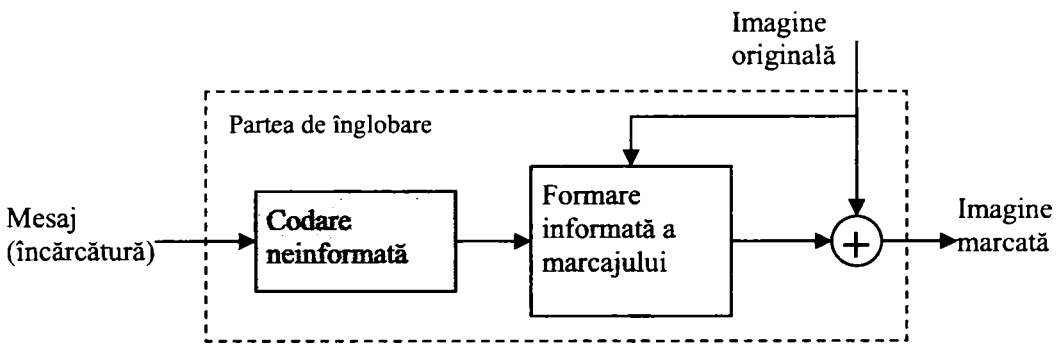


Fig. 1.25: Codare neinformată şi formare informată a marcajului (mascare perceptuală).

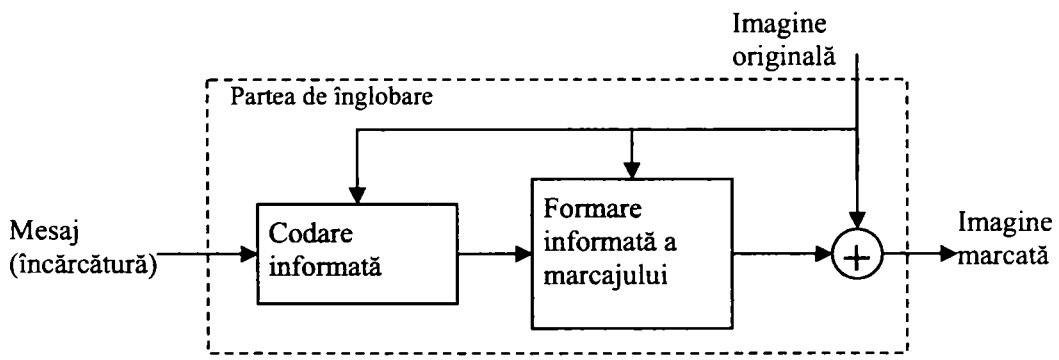


Fig. 1.26: Codare informată şi formare informată a marcajului (mascare perceptuală).

Marcarea cu înglobare informată şi detector neinformat poate fi privită ca şi o formă de *comunicare cu informaţie ascunsă la transmiţător* [CMB02]. În modelul lui Shannon, transmiţătorul cunoaşte modelul de canal. În marcarea transparentă, imaginea originală este considerată ca o sursă de zgomot, deci rezultatele teoretice ale acestui model ar trebui să fie aplicabile în acest caz.

În consecinţă *mascarea perceptuală* permite controlul raportului fidelitate/robusteţe. Pe de altă parte, *codarea informată şi mascarea perceptuală* permit creşterea încărcăturii (*payload*) pentru un raport fidelitate/robusteţe dat, respectiv îmbunătăţesc acest raport pentru o încărcătură dată.

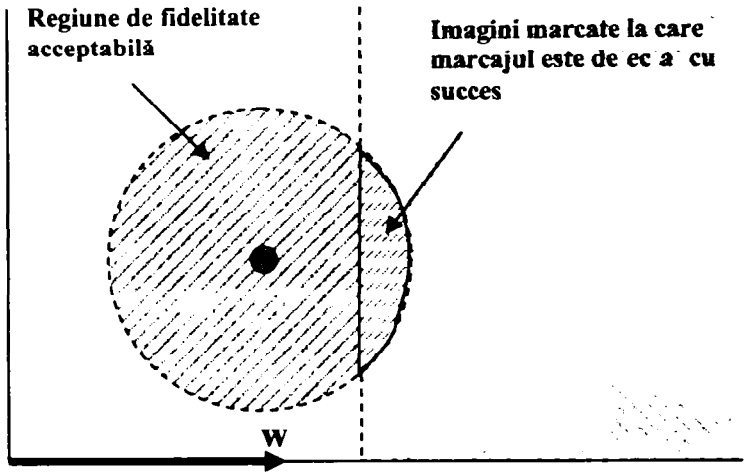


Fig. 1.27: Intersecţia regiunii de detecţie cu cea de fidelitate acceptabilă.

Obiectivul este producerea unei imagini care se află la intersecţia regiunii de fidelitate acceptabilă şi a regiunii de detecţie. Problema care apare în cazul folosirii mascării perceptuale este că imaginea marcată rezultată poate fi în afara regiunii de detecţie.

Există două posibilităţi pentru a soluţiona această problemă: fie se maximizează robusteţea pentru o fidelitate dată, fie se maximizează fidelitatea pentru o robusteţe dată. Ambele variante necesită estimarea fidelităţii sau a robusteţii.

În condiţiile în care se presupune că eroarea medie pătratică, MSE, este un bun estimator al fidelităţii, şi că robusteţea este o funcţie monotonă de corelaţia liniară, prin înglobare neinformată se ajunge la o robusteţe maximă pentru o fidelitate dată. Pe de altă parte impactul negativ asupra fidelităţii poate fi minimizat pentru o robusteţe dată.

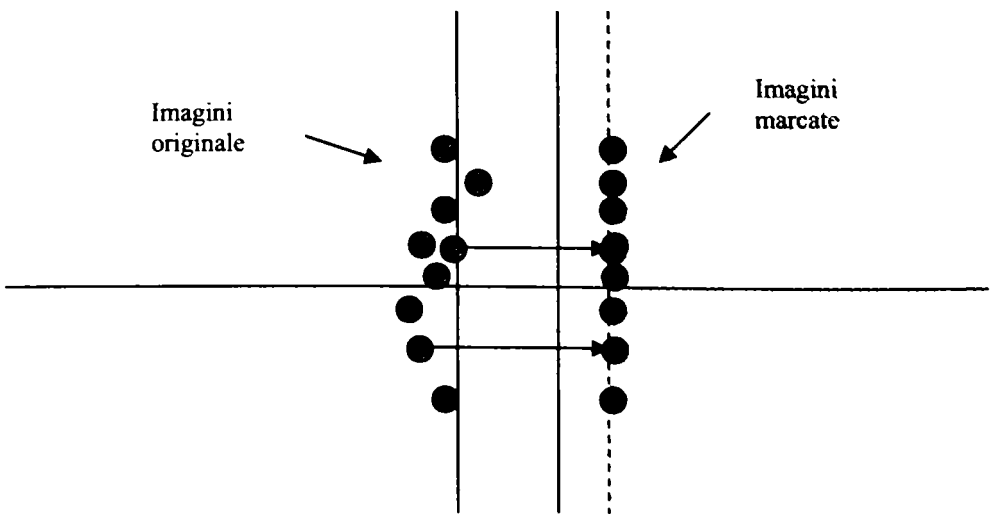


Fig. 1.28: Maximum de fidelitate pentru o robusteţe dată

O altă problemă este estimarea robusteţii în cazul mascării perceptuale (informate). Se poate pleca de la o premiză simplă, şi anume că robusteţea este o funcţie monotonă de valoarea de detecţie, lucru adevărat în cazul corelaţiei liniare, dar neadevărat pentru corelaţia normalizată [Cox05]. În cazul corelaţiei normalizate, rezultatele obţinute la detecţie sunt îmbunătăţite, dacă robusteţea se estimează ca fiind puterea zgomotului alb care poate fi adăugat la imaginea marcată, înainte ca marcajul să fie nedetectabil [CMB02].

1.10.4 Codarea informată

Încărcătura (*payload*-ul) marcajului poate fi crescută semnificativ în cazul în care codarea mesajului se face funcţie de imaginea originală. Acest lucru este în conformitate cu teoria lui Costa, descrisă în lucrarea sa *Writing on dirty paper* [Cos83], aplicabilă şi în marcarea transparentă.

Costa a studiat canalul *dirty-paper* [Cos83]. Informaţia se transmite printr-un canal zgomotos cu două surse de zgomot, prima fiind cunoscută la transmiţător. El a demonstrat că prima sursă de zgomot, fiind cunoscută, nu afectează comunicaţia.

Această problemă poate fi asemănată cu transmiterea unui mesaj scris cu cerneală pe o hârtie care este afectată de praf distribuit normal. "Puterea" cernelii este limitată. Mesajul este transmis, şi astfel se mai acumulează praf pe traseu. Problema este că receptorul nu poate distinge între praf şi cerneală, deci câtă informaţie poate fi transmisă?

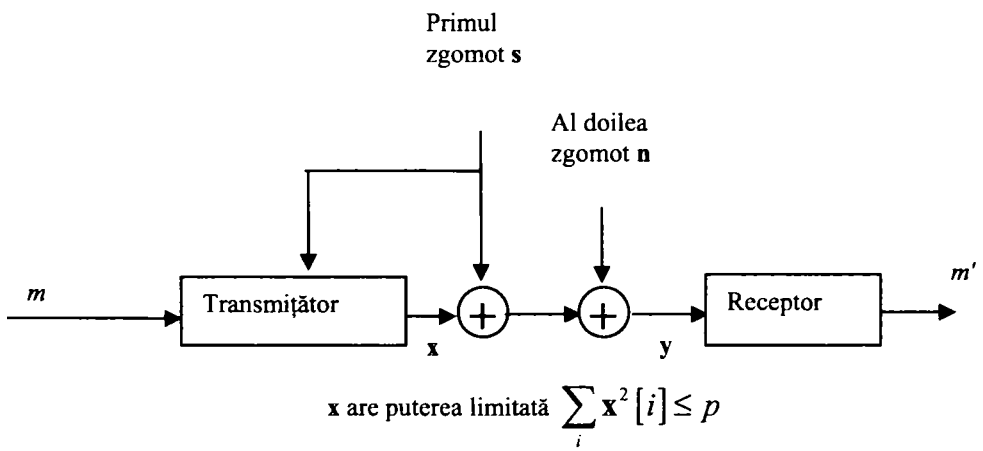


Fig. 1.29: Schema lui Costa pentru canalul dirty-paper [Cos83].

Rezultatele obţinute de Costa demonstrează faptul că prima sursă de zgomot nu are efect asupra capacităţii canalului. Această analogie este aproape similară cu marcarea transparentă cu detecţie neinformată. Hârtia „murdară" **s** este echivalentă cu semnalul original, semnalul transmis **x** cu marcajul adăugat, iar limitarea puterii lui **x** este echivalentă cu conservarea fidelităţii. A doua sursă de zgomot este echivalentă cu distorsiunile suferite de semnalul multimedia. Deoarece canalul *dirty-paper* este atât de asemănător cu marcarea transparentă, rezultatele lui Costa sunt foarte interesante, în sensul că, dacă un sistem de marcare are o comportare apropiată cu cea a canalului *dirty-paper*, atunci încărcarea maximă nu ar trebui să depindă de semnalul gazdă (original). Dar există o mare diferenţă între

canalul *dirty-paper* şi un sistem adevărat de marcare transparentă, în sensul că cele două surse de zgomot sunt foarte rar gaussiene. Funcţia densităţii de probabilitate a semnalelor multimedia nu e gaussiană, iar zgomotul depinde de semnalul original. În plus, controlul distorsiunii, ca o limitare a puterii, implică folosirea erorii medii pătratice, care nu este cel mai potrivit estimator al distanţei perceptuale. Moulin şi O'Sullivan [MOS03] au studiat modele de canale mai potrivite pentru marcarea transparentă. Ei au înlocuit a doua sursă de zgomot cu semnalul furnizat de un adversar care încearcă să elimine intenţionat marcajul. S-a demonstrat că dacă semnalul gazdă are o distribuţie gaussiană şi constrângerea de fidelitate este exprimată funcţie de constrângerea de putere, rezultatele obţinute de Costa sunt valabile: capacitatea canalului este independentă de dispersia semnalului nemarcat. Dacă distribuţia semnalului original nu este gaussiană, rezultatele sunt adevărate doar dacă maximul puterii p este mic în comparaţie cu dispersia semnalului original.

Bazându-se pe aceasta concluzie obţinută de Costa, s-au construit pentru codarea informată a mesajului, *codurile dirty-paper* [CMB02]. Acestea sunt coduri în care fiecare mesaj este reprezentat prin vectori de cod alternativi. Din setul de vectori care reprezintă mesajul dorit se alege unul, **u**, cel mai aproape de primul zgomot, adică în acest caz, de imaginea originală. Codul lui Costa este generat aleator şi cere o căutare exhaustivă pentru codare şi decodare, fiind convenabil numai pentru secvenţe de intrare scurte.

Cele mai studiate în practică sunt *codurile latice* [CW98, EBTG02], unde fiecare cuvânt de cod este un punct al unei latice regulate. Punctele într-o latice N-dimensională pot fi construite prin însumarea multiplilor întregi a N vectori distincţi. Astfel mesajul $\mathbf{w}_m$, fiind un punct în această latice, poate fi descris ca suma unuia sau a mai multor marcaje de referinţă $\mathbf{w}_{r0},\ldots\mathbf{w}_{rN}$, înmulţite cu nişte întregi, $z[0]$, $z[1],\ldots,z[N]$:

$$\mathbf{w}_m = \sum_i z[i]\mathbf{w}_{ri}$$

Fiecare dimensiune în spaţiul de marcare codează un simbol, de obicei un bit. Acesta este codat alegând între două puncte de cuantizare.

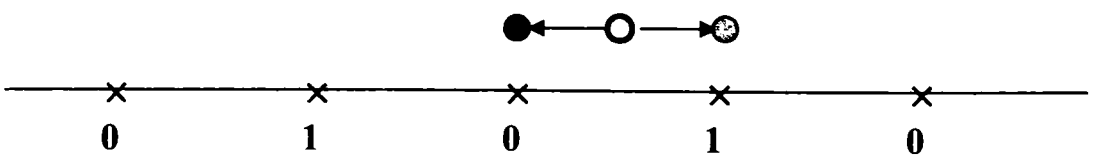


Fig. 1.30: Codare latice, pentru N=1.

Aceste sisteme sunt cunoscute sub denumirea de sisteme de *marcare QIM* bazate pe modulaţia prin cuantizarea indexată. Cea mai simplă formă de marcare QIM cuantizează semnalul gazdă, folosind un cuantizor indexat de mesajul de marcaj. Dacă se notează cu s semnalul marcat, cu m mesajul şi cu x semnalul gazdă, atunci $s(x,m) = q_m(x)$. Semnalul rezultat va fi compus numai din valori din setul posibil al ieşirilor cuantizorului. Acest tip de marcare este adecvat mai ales în cazul în care semnalul rezultat va fi ulterior cuantizat, de exemplu prin compresie. Modulaţia de *dither* poate produce un semnal care conţine toate valorile din semnalul gazdă. Din valorile cuantizate sunt translatate cu un nivel variabil de *dither*, d, de exemplu cu relaţia $s(x,m) = q_m(x + d) - d$.

Sistemele de marcare care folosesc *coduri latice* au o capacitate mult mai mare decât sistemele bazate pe corelaţie (de obicei peste 1000 de biţi), dar nu sunt atât de robuste ca cele din urmă. Sistemele bazate pe corelaţie au raport mai bun încărcare/robusteţe atunci când zgomotul este mare, pe când cele care folosesc coduri latice sunt susceptibile la schimbarea contrastului. *Codurile convoluţionale* sunt o alternativă la codurile latice, fiind construite să fie robuste la ajustarea contrastului.

2. TEHNICI DE MARCARE

2.1 Clasificarea tehnicilor de marcare

În Figura 2.1 este dată o clasificare a tehnicilor de marcare existente:

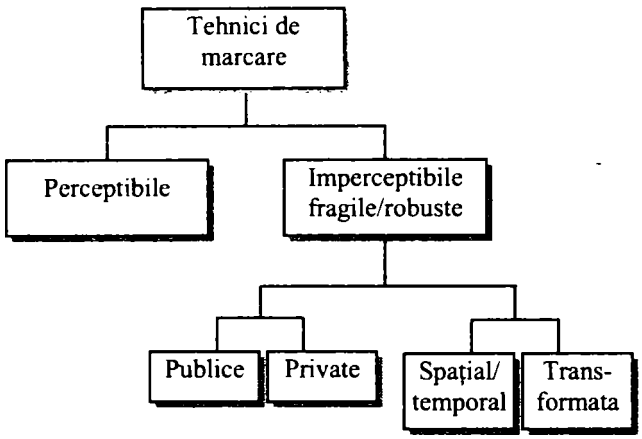


Fig. 2.1: Clasificarea tehnicilor de marcare.

Marcajele pot fi:

- *perceptibile*
- *imperceptibile*

Marcajele perceptibile creează schimbări sesizabile în semnalul original, atunci când sunt înglobate, dar nu împiedică semnalul marcat să comunice mesajul original. Deşi marcarea perceptibilă nu este atât de răspândită, deoarece poate fi supărătoare pentru sistemul vizual uman, ea a fost implementată cu succes pentru imagini în [BMM96], prin înglobarea unui *logo* vizibil, care permite ca toate detaliile semnificative ale imaginii să fie văzute.

Marcajele imperceptibile au fost prezentate sumar în capitolul 1, dar *subiectul acestei teze fiind marcarea transparentă adică imperceptibilă a imaginilor statice*, acest subiect va fi tratat în continuare. Marcajele imperceptibile pot fi, în funcţie de aplicaţie:

- *fragile*
- *robuste*.

Marcajele fragile sunt înglobate în semnalul multimedia astfel încât aproape orice transformare nedorită a semnalului marcat va duce la alterarea acestuia, oferind în acest fel informaţii despre modificări ale semnalului făcute cu rea voinţă [PW02].

Marcajele robuste sunt înglobate în semnalul gazdă astfel încât eliminarea lor să fie dificil de făcut, în contrast cu marcajele fragile. Acestea trebuie să fie

rezistente împotriva *atacurilor* intenţionate. Un *atac* este orice fel de modificare a semnalului multimedia marcat care poate afecta calitatea marcajului extras.

În cadrul tehnicilor de marcare robuste, se pot defini două tipuri de marcare [CM97], după modul în care se utilizează sau nu semnalul original la detecţia marcajului:

- *marcarea publică* [AP98, KH98,NP98] foloseşte semnalul multimedia marcat şi o cheie de marcare pentru detecţia respectiv extragerea marcajului, fără să fie nevoie de semnalul multimedia original. Estimarea marcajului este mai puţin robustă, dar volumul de calcul este mult mai redus.
- *marcarea privată* [ZWL03, CKLS97, KM99, CM98] foloseşte atât semnalul multimedia marcat, cât şi cel original, pentru detecţia şi extragerea marcajului. Estimarea marcajului este mai robustă, dar mai lentă. Nu este potrivită în aplicaţiile unde se cere viteză şi eficienţă, cum sunt căutările automate, în baze de date, ale produselor multimedia furate [CMB02].

Tehnicile de marcare robuste se pot clasifica în funcţie de locul de înserare a marcajului, astfel:

- tehnici în *domeniul spaţial/temporal* unde marcajul este înglobat în domeniul spaţial pentru imagini, respectiv, în domeniul temporal pentru semnale audio [NP98],
- tehnici în *domeniul transformatelor,* unde se lucrează asupra transformatelor cosinus, Fourier sau *wavelet* ale semnalului gazdă [SK01, ZWL03, CKLS97, CMYY98, KH98, NP98, KM99, CM98, PW02, NI03, NBK04, NC04b, NB05, NC05b, NC05a, NIB05].

Multe dintre aceste metode sunt asemănătoare şi diferă în anumite aspecte cum sunt formarea semnalului de marcaj, înserarea şi detecţia.

Semnalul de marcaj. De obicei, informaţia înserată nu este importantă în sine, dar există metode care nu folosesc o secvenţă de informaţie aleatoare, ci înserează, respectiv extrag, cuvinte de cod din dicţionare [CKLS95], [KH98]. În alte scheme se modulează codurile din dicţionar, cu biţi de informaţie aleatori. Deşi unii autori fac distincţie între cele două tipuri de metode, ele sunt foarte apropiate conceptual.

Semnalul de marcare tipic este un semnal pseudoaleator, cu amplitudine mică în comparaţie cu cea a imaginii; de obicei se distribuie spaţial 1 bit pe mai multi pixeli. Semnalul de marcaj este construit adesea ca fiind un zgomot pseudo-aleator alb [TRSH93], [STO94] sau colorat, cu o distribuţie gaussiană [CKLS95], uniformă sau bipolară [KH98], [Kut98], [NP96], [TRSH93]. Pentru a face marcajul imperceptibil, se poate aplica mascarea implicită sau explicită în domeniul spaţial, [BMYY97], [KRR98], [WPD99], sau spectral pentru a atenua marcajul în zonele unde acesta ar putea deveni vizibil. Semnalul de marcaj rezultant este uneori împrăştiat şi lasă pixeli din imagine neschimbaţi [KJB98], dar de cele mai multe ori este dens şi alterează toti pixelii din imagine.

Inserarea semnalului de marcaj. Semnalul de marcaj este deseori înserat în domeniul spaţial, dar şi în domeniul unei transformate, precum trasformata cosinus discretă, DCT [CKLS95], sau transformata DCT pe blocuri [KZ95].

Înserarea marcajului poate fi făcută prin adunare [LLL97, NP96, STO94] sau printr-o adunare adaptivă după forma semnalului [BBPC98a]; de cele mai multe ori, este afectat numai canalul de luminanţă, sau numai canalele de culoare [KJB97]. Adunarea poate avea loc în domeniul spaţial sau în domeniul unei transformate: transformata Fourier discretă DFT [RDB96], DCT pe imagine, [BBPC98c, CKLS95, PBBC97], DCT pe blocuri [BMYY97, HG96, KZ95, LLL97, PZ98, XBA97], în domeniul

wavelet [Kun99, KH98], fractal [DS96, CBD98, PJ96], Hadamard [RAA99a], Fourier Mellin [RP97, RP98], Radon [WMBC99], Ridgelet [CKN04].

De multe ori se argumentează că înserarea în domeniul unei transformate (de cele mai multe ori DCT sau wavelet) poate fi avantajoasă din punctul de vedere atât al imperceptibilităţii cât şi al securităţii [BBPC98c].

Unii autori sugerează ca marcajul să fie plasat în zonele de frecvenţă joasă ale imaginii [CKLS95, RP97], alţii susţin că trebuie înserat în frecvenţele medii [BBPC98c] sau înalte. De fapt, s-a demonstrat [SG99] că pentru o robusteţe maximă dorită, marcajul ar trebui să fie înserat adaptiv, în componentele spectrale pe care le are semnalul gazdă. Pentru imagini şi video, acestea sunt în general, frecvenţele joase.

Detecţia semnalului de marcaj. Aşa cum am menţionat mai înainte, generarea semnalului de marcaj precum şi înserarea acestuia sunt tratate de obicei împreună. În unele metode, acestea nu pot fi privite separat, în special dacă marcajul este adaptat la forma semnalului [BBPC98c, CW98, CW01a, CW01b, LLL97].

Recuperarea marcajului este de obicei făcută cu o metodă bazată pe corelaţie, un corelator sau un filtru adaptat. Deoarece semnalul de marcaj este de obicei construit fără cunoştinţe despre semnalul gazdă, interferenţa dintre semnalul de marcaj şi semnalul gazdă este obişnuită în marcarea transparentă. Pentru a elimina interferenţa cauzată de semnalul gazdă, multe metode cer ca acesta să fie cunoscut la detecţie, pentru a-l scădea înainte de extragerea marcajului. Alte metode aplică o prefiltrare [DKL98, KJB97, LLL97, STO94] în loc să scadă semnalul original nemarcat. În alte cazuri, această interferenţă nu se elimină [PBBC97]. Unii cercetători propun folosirea unor detectoare mai sofisticate în locul detectoarelor bazate pe corelaţie, de exemplu un detector MAP, maximum a-posteriori [BBCP98c]. Pentru extragerea marcajului au fost propuse mai multe domenii, de multe ori aceleaşi de la înserarea sau formarea marcajului. Există mai puţine publicaţii în care marcarea şi extragerea au loc în domenii diferite.

Tehnicile de marcare transparentă pot fi clasificate conform câtorva criterii, după cum urmează:

- Selecţia locaţiilor unde marcajul va fi înserat marcajul, folosind modelul vizual uman, sau o cheie generată aleator respectiv pseudo-aleator,
- Domeniul în care este înserat marcajul: spaţial/temporal sau al unei transformate (DCT, DWT, DFT, etc),
- Codarea mesajului de marcaj, folosind coduri corectoare de erori (ECC), transmisia spread spectrum (SS), multiplexarea cu diviziune în timp/spaţiu, multiplexarea în cod,
- Formarea semnalului marcat: prin adunare sau cuantizare,
- Detectarea/decodarea marcajului: cu corelatoare, etc.

2.1.1 Alegerea locaţiilor unde se înserează marcajul

Cox, ş.a. [CKLS97] argumentează că marcajul ar trebui înserat în regiuni perceptuale semnificative, care vor supravieţui compresiei. Pe această idee au fost propuse numeroase metode.

Pe de altă parte, dacă se consideră un algoritm de marcare public, eliminarea marcajului ar trebui prevenită doar prin secretizarea cheii. Aceasta este o implicaţie directă a principiului lui Kerckhoff. De exemplu, o cheie secretă poate iniţializa un generator de numere pseudo-aleatoare pentru selecţia locaţiilor

marcajului [BGM95]. Câţiva algoritmi au propus recuperarea publică a marcajului [HG97], unde doar o parte din cheia secretă este cunoscută în partea de decodare (S^{pub}).

2.1.2 Domeniul de marcare

2.1.2.1 Domeniul spaţial

Multe tehnici în domeniul spaţial sunt bazate pe adunarea la o imagine a unei secvenţe de zgomot pseudo-aleator. În acest caz, operatorii din capitolul 1, $\mathcal{E}$ şi $\mathcal{D}$ sunt pur şi simplu adunarea şi scăderea. Considerăm o imagine de mărime NxM, în care fiecare pixel este reprezentat de un număr zecimal, în domeniul determinat de numărul de biţi folosiţi. Într-o imagine cu nivele de gri, cu 8 biţi per pixel, fiecare pixel poate avea o valoare între [0, 255] şi fiecare pixel D poate fi reprezentat ca fiind:

$$D = \sum_{i=0}^{7} b_i \cdot 2^i .$$

Această proprietate permite descompunerea unei imagini într-o colecţie de imagini binare, separând valorile b_i în $n=8$ planuri de biţi.

Metodele de marcare în domeniul spaţial înglobează marcajul modificând în mod direct valorile pixelilor din imaginea originală. De obicei, se modifică biţii cei mai puţin semnificativi ai imaginii gazdă LSB. Mesajul secret este înserat în planul de biţi cel mai puţin semnificativ al imaginii gazdă, fie prin înlocuirea directă a biţilor, fie modificând aceşti biţi LSB conform unei funcţii inverse. Strategia de înserare poate fi bazată pe înserarea secvenţială sau selectivă a mesajului, în ariile mai „zgomotoase" ale imaginii, sau prin împrăştiere aleatoare prin imagine.

Dată fiind capacitatea extraordinar de mare a canalului LSB prin metoda folosirii întregii imagini purtătoare pentru transmisie, un obiect mai mic poate fi integrat de mai multe ori. Chiar dacă majoritatea acestor obiecte se pierd din cauza atacurilor, un singur marcaj supravieţuitor poate fi considerat un succes.

Imperceptibilitatea este atinsă fiindcă planul LSB este nesemnificativ din punct de vedere vizual. Astfel, principalul avantaj al unei astfel de tehnici este că modificarea planului LSB nu afectează calitatea imaginii, din cauză că variaţia amplitudinii pixelilor este limitată la ±1. Proprietăţile de mascare a sistemului vizual uman permit înserarea unor cantităţi semnificative de informaţie care vor fi imperceptibile unui observator uman, în condiţii de vizualizare normale. Mascarea se referă la fenomenul la care un semnal este imperceptibil unui observator în prezenţa altui semnal. O expunere detaliată a acestor tehnici poate fi găsită în [LD99b], [YM97], [MW98].

Alte avantaje alte tehnicilor de marcare bazate pe LSB includ capacitatea mare şi complexitatea de calcul mică. De aceea, este de aşteptat ca ele să fie puse în practică mai uşor, atunci când este vorba de marcare în timp real. Principalul dezavantaj este lipsa de robusteţe la falsificare, atacuri geometrice, filtrare şi compresie.

Metoda substituirii LSB-urilor prezintă o serie de neajunsuri, în ciuda simplităţii ei. Deşi poate supravieţui transformărilor ca decuparea, orice adăugare de zgomot sau compresie cu pierderi cauzează, mai mult ca sigur, pierderea marcajului. Un atac chiar mai bun este substituirea bitului LSB al fiecărui punct din imagine cu „1", pierzându-se în totalitate posibilitatea recuperării marcării, cu un

impact neglijabil asupra imaginii gazdă. Mai departe, odată descoperit algoritmul, marcajul poate fi modificat uşor.

Dacă se doreşte un marcaj fragil, astfel de tehnici nu pot localiza modificări ale semnalului decât spaţial, nu şi spectral.

O îmbunătăţire a tehnicii substituirii LSB-ului, ar fi folosirea unui generator de numere pseudo-aleatoare, pentru a determina pixelii din imagine care urmează să fie folosiţi pentru integrarea marcajului, pe baza unei „chei" date. Securitatea marcării este îmbunătăţită din moment ce marcajul nu poate fi găsit cu uşurinţă de persoane intermediare. În schimb algoritmul rămâne în continuare vulnerabil la atacul prin substituţia LSB-ului cu o constantă. Chiar şi în locurile care nu s-au folosit pentru biţi de marcare, efectul substituirii este neglijabil asupra imaginii purtătoare. Modificarea LSB-ului se dovedeşte a fi o metodă simplă şi puternică pentru steganografie, totuşi lipseşte robusteţea de bază cerută de aplicaţiile de marcare transparentă.

Aceste tehnici presupun uneori transformarea mesajului de marcaj într-o secvenţă PN, care este apoi inserată în imagine, o singură dată, sau de mai multe ori dacă marcajul este mult mai mic decât imaginea gazdă. Detecţia se face prin obţinerea imaginii de marcare şi compararea ei cu cea originală, sau folosind un corelator.

2.1.2.2 Domeniul unei transformate

Tehnicile descrise anterior pot fi aplicate şi în domeniul unor transformate ale imaginii, unde se poate ţine cont de criteriile perceptuale în procesul de înserare a marcajului, şi în construirea unor tehnici de marcare robuste la tehnici de prelucrare obişnuite. Fiecare domeniu de transformare are avantajele şi dezavantajele sale.

Pentru a înţelege avantajele unei metode de marcare în domeniul transformatelor, în cele ce urmează se analizează etapele prin care trece un semnal multimedia (imagine sau semnal audio) în timpul copierii. În Figura 2.3, prin „transmisia" semnalului înţelegem codarea sursei sau a canalului, şi/sau criptarea datelor. Majoritatea prelucrărilor sunt fără pierderi, dar multe din metodele de compresie ale datelor sunt cu pierderi. Acestea din urmă (JPEG, MPEG, etc.) pot degrada calitatea datelor, printr-o pierdere iremediabilă a informaţiei. O schemă de marcare ar trebui să fie rezistentă la distorsiunile introduse de aceste prelucrări.

Compresia cu pierderi este o operaţie care elimină de obicei componentele mai puţin semnificative ale unei imagini sau ale unui sunet. Majoritatea procesărilor de acest tip au loc în domeniul frecvenţă. De fapt, pierderile de date au loc în componentele cu frecvenţe înalte.

După recepţie, o imagine suferă o serie de transformări obişnuite care pot fi clasificate în distorsiuni geometrice, sau distorsiuni ale semnalului. Distorsiunile geometrice sunt specifice imaginilor şi semnalelor video, şi se referă la operaţii cum ar fi rotirea, translaţia, scalarea şi decuparea. Prin determinarea manuală a minim patru sau nouă puncte corespondente dintre marcajul original şi cel distorsionat, este posibilă îndepărtarea oricărei transformări afine, bi- sau tri-dimensionale [CKLS97]. O scalare afină, sau micşorare a imaginii duce la o pierdere a datelor în componentele de frecvenţe înalte ale imaginii. Decuparea sau tăierea porţiunilor din imagine duc la pierderi irecuperabile ale datelor, care pot degrada serios orice marcaj aplicat în domeniul spaţial. Dar o metodă bazată pe o transformare în frecvenţă, ca DCT, împrăştie marcajul în întreg domeniul spaţial al imaginii, şi este mai puţin probabil ca el să fie afectat de decupare.

Distorsiuni obişnuite ale semnalului sunt conversiile D/A, A/D, reeşantionarea, recuantizarea, precum şi îmbunătăţirile aduse semnalului cum ar fi creşterea contrastului sau a intensităţii culorilor pentru imagini, sau egalizarea în frecvenţă pentru semnale audio.

Multe dintre aceste distorsiuni sunt neliniare, deci este dificil de analizat efectul lor asupra metodelor de marcare în domeniul spaţial sau al transformatei. Dar cunoşterea imaginii originale permite ca multe transformări să fie reversibile, cel puţin aproximativ.

Nu în ultimul rând, imaginea copiată poate să nu rămână în formatul digital original. Este foarte probabil ca imaginea să fie imprimată pe hârtie, sau în cazul semnalelor audio şi video, ele pot fi copiate pe casete audio, respectiv video. Aceste reproduceri pot introduce degradări adiţionale asupra imaginii, la care metoda de marcare trebuie să fie robustă.

Din motivele enumerate mai sus, se poate deduce că marcajul nu ar trebui să fie plasat în regiunile sau componentele spectrale *nesemnificative* ale imaginii, deoarece multe prelucrări şi distorsionări obişnuite ale semnalului pot afecta aceste componente. De exemplu, un marcaj plasat în frecvenţele mai înalte ale imaginii poate fi foarte uşor eliminat printr-o filtrare trece-jos. Evident că poate fi afectată orice componentă spectrală, cu condiţia ca modificările făcute să fie mici. Dar schimbările mici pot fi foarte sensibile la zgomot.

Problema care se pune este cum să se introducă marcajul în regiunile de percepţie maximă ale spectrului, păstrând fidelitatea semnalului original.

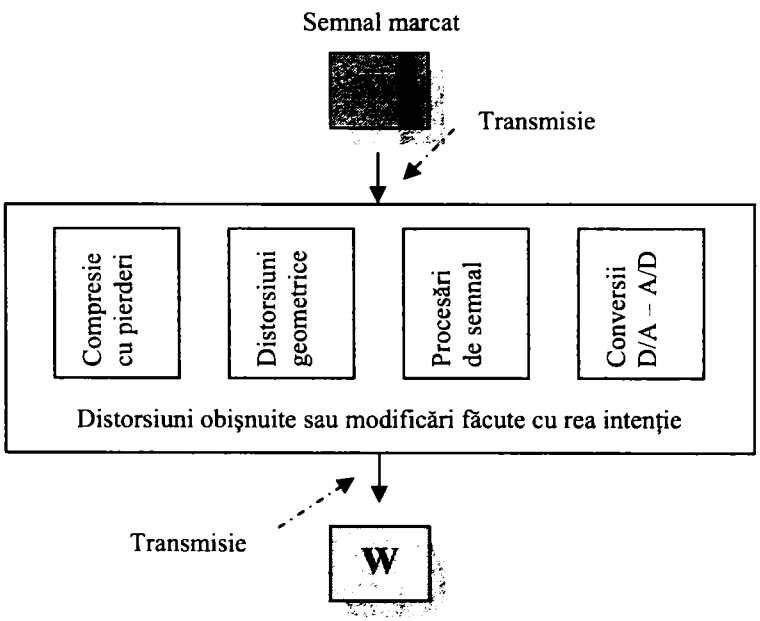


Fig. 2.2: Prelucrări obişnuite ale unui produs multimedia

Există multe lucrări care abordează problema marcării, prin analogie cu problema comunicaţiilor cu spectru împrăştiat, SS (Spread Spectrum). În [CKLS97], autorii tratează domeniul transformatei DCT a imaginii ca un *canal de comunicaţii* şi

corespunzător, marcajul este văzut ca un semnal care trebuie transmis prin acest canal de comunicaţii. Atacurile şi distorsiunile neintenţionate ale semnalului sunt tratate ca un zgomot la care semnalul trebuie să fie imun.

În comunicaţiile cu SS, se transmite un semnal de bandă îngustă într-o bandă mult mai largă de frecvenţă, astfel încât energia oricărei componente spectrale a semnalului să fie foarte mică şi aproape nedetectabilă. Marca este împrăştiată în multe componente spectrale, astfel încât energia ei din fiecare componentă să nu fie detectabilă. Deoarece în procesul de detecţie a marcajului se cunoaşte localizarea şi conţinutul marcajului, este posibil ca la recepţie să se concentreze aceste semnale numeroase cu energie scăzută într-un singur semnal, al cărui raport semnal pe zgomot să fie mare. Pentru a distruge un astfel de marcaj, ar trebui adăugat zgomot cu amplitudine mare în *toate* componentele spectrale.

Împrăştierea marcajului în tot spectrul imaginii asigură o robusteţe mare faţă de atacuri, intenţionate sau nu, deoarece nu se cunoaşte localizarea marcajului. În plus, pot fi selectate anumite zone de frecvenţă, a căror atacare ar conduce la degradări severe ale imaginii.

Un marcaj bine plasat în componentele spectrale ale semnalului va fi imposibil de văzut la imagini, respectiv de auzit la sunete. Afirmaţia este adevărată dacă energia marcajului este suficient de mică în oricare componentă spectrală. În plus, energia marcajului prezentă în unele componente spectrale poate fi mărită, folosind cunoştinţele despre *fenomenul de mascare* al simţului auditiv, respectiv vizual al omului.

Este cunoscut faptul că HAS şi HVS disting cu o rezoluţie mai mare zonele cu energie mai mare şi frecvenţe mai joase, din imagine sau sunet. Mai mult, majoritatea informaţiei este localizată în regiunile cu frecvenţe mai joase [CKLS97].

Mascarea perceptuală se referă la situaţia în care anumite informaţii care ar putea fi distinse de observatorul uman când sunt prezentate izolat, vor fi observate cu dificultate sau deloc, când se adaugă alte informaţii (o imagine puternic texturată, sau un sunet învecinat mai puternic). Astfel, prezenţa unui semnal poate fi ascunsă sau mascată de prezenţa altui semnal. Mascarea este o măsură a răspunsului la un stimul a unui observator, când este prezent un al doilea stimul, cel de mascare [CMB02, CKLS97].

2.1.2.2.a Metode bazate pe transformata Fourier discretă

În [RDB96], este folosită faza valorilor transformării Fourier discrete, DFT, pentru plasarea marcajului, deoarece, pentru inteligibilitatea imaginii, este mai importantă faza decât amplitudinea valorilor DFT. Plasarea marcajului în cele mai importante componente ale imaginii, îmbunătăţeşte robusteţea marcajului, deoarece modificarea acestor componente importante de imagine, cu scopul eliminării marcajului, ar degrada calitatea imaginii. Al doilea motiv pentru folosirea fazei valorilor DFT este că modulaţia de fază prezintă imunitate superioară la zgomot în comparaţie cu modulaţia de amplitudine.

Multe tehnici de marcare folosesc modulaţia de amplitudine în DFT, din cauza proprietăţii de invarianţă la translaţii sau deplasări [LWBC01, RP98]. Deoarece translaţia ciclică a imaginii în domeniul spaţial nu afectează amplitudinile coeficienţilor DFT, marcarea plasată în acest domeniu va fi invariantă la translaţii.

În cazul folosirii unui marcaj CDMA (Code Division Multiple Access), metoda poate fi rezistentă la decupare. Marcajul poate fi plasat direct în frecvenţele medii cele mai importante, deoarece modulaţia coeficienţilor de frecvenţă joasă generează efecte vizibile, iar coeficienţii frecvenţelor înalte sunt foarte vulnerabili la zgomot,

filtrare şi compresie cu pierderi. În final, marcajul poate fi făcut dependent de conţinutul imaginii, prin modularea coeficienţilor de amplitudine DFT, |I(u,v)| în modul următor [CKLS95]:

$$\left|I_W(u,v)\right| = \left|I(u,v)\right|\left(1 + k \cdot W(u,v)\right). \tag{2.1}$$

Aici, W(u,v) reprezintă un marcaj CDMA, un model pseudo-aleator bidimensional (2D) şi *k* reprezintă factorul de câştig. Modificarea coeficienţilor DFT nu este fixă, ci proporţională cu amplitudinea coeficienţilor DFT. Coeficienţii DFT mici sunt foarte puţin afectaţi, dar coeficienţii DFT mai mari sunt modificaţi mai mult. Acest lucru este în conformitate cu legea lui Weber [Jai81]. Sistemul vizual uman (HVS) nu percepe modificările egale în imagini egale, dar sensibilitatea vizuală este aproape constantă în privinţa schimbărilor relative dintr-o imagine. Dacă ΔI este o diferenţă uşor vizibilă, atunci ΔI/I=constantă. Rescrierea relaţiei (2.1) conduce la:

$$\frac{\left|I_W(u,v)\right| - \left|I(u,v)\right|}{I(u,v)} = \frac{\Delta I(u,v)}{\left|I(u,v)\right|} = k \cdot W(u,v) \cong \text{constant} \tag{2.2}$$

Deoarece în acest caz marcajul este plasat în majoritate în coeficienţii DFT mai mari, adică în componentele cele mai semnificative ale imaginii din punct de vedere perceptual, robusteţea marcajului este îmbunătăţită. Este de menţionat că simetria coeficienţilor Fourier trebuie păstrată, pentru a asigura ca datele de imagine să fie de valoare reală după transformarea inversă la domeniul spaţial. Dacă coeficientul |I(u,v)| într-o imagine cu NxM pixeli este modificat conform relaţiei (2.1), corespondentul lui, |I(N-u,M-v)|, trebuie modificat şi el în acelaşi mod.

Fig. 2.3: Marcajul înserat în amplitudinea coeficienţilor Fourier
(a) Imaginea originală, (b) Imaginea marcată, (c) Diferenţa W(x,y)=I-I_W, scalată pentru a fi vizibilă, (d) Imagine puternic marcată

În figura 2.3(b) este prezentată, ca exemplu, o imagine în care marcajul este plasat folosind toţi coeficienţii de amplitudine DFT, în conformitate cu relaţia (2.2) şi folosind un factor de câştig *k* relativ mic. Figura 2.3(c) prezintă diferenţa, puternic amplificată, dintre imaginea originală şi cea marcată, iar figura 2.3(d) arată o imagine marcată, folosindu-se o valoare mare pentru factorul de câştig *k*.

Transformata DFT este mai adesea folosită în formele ei derivate, cum ar fi transformata cosinus discretă, DCT sau transformata Fourier-Mellin.

2.1.2.2.b Metode bazate pe transformata cosinus discretă

Domeniul transformării cosinus discrete, DCT, este deseori folosit pentru plasarea marcajului. DCT este o transformată reală, care reprezintă imaginea prin coeficienţi ai unor semnale cosinusoidale, de diferite frecvenţe (care constituie baza acestei transformate). Transformata DCT a imaginii este calculată pe blocuri 8x8 ale imaginii, care apoi sunt transformate individual. Transformata 2D-DCT, a unei imagini, este matricea rezultată astfel încât, colţul din stânga sus reprezintă frecvenţa joasă, iar colţul din dreapta jos reprezintă frecvenţa înaltă. DCT stă la baza algoritmului de compresie, care este unul dintre cele mai răspândite formate de memorare a datelor la ora actuală. Marcajele înserate, în domeniul transformatei DCT, sunt capabile să supravieţuiască unor forme de prelucrări precum filtrarea trece-jos, trece-sus, filtrarea mediană, etc.

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Fig. 2.4: Valori de cuantizare folosite la compresia JPEG

Folosind DCT, o imagine poate fi împărţită cu uşurinţă în benzi de pseudo-frecvenţă, în aşa fel încât marcajul să poată fi plasat convenabil în cele mai importante frecvenţe medii. În plus, a fost intens studiată sensibilitatea sistemului vizual uman la imaginile de bază DCT, rezultând tabela de cuantizare JPEG (figura 2.4) [PM93].

Aceste rezultate pot fi folosite pentru predicţia şi minimizarea impactului vizual la distorsiunile cauzate de marcaj. În final, pentru compresia imaginilor şi materialelor video este folosită pe scară largă DCT pe bază de blocuri.

Prin plasarea marcajului în acelaşi domeniu cu al schemei de compresie utilizată pentru procesarea imaginii, domeniul DCT în acest caz, se poate anticipa compresia cu pierderi, pentru că se pot anticipa coeficienţii DCT care vor fi eliminaţi

de către algoritmul de compresie. Descompunerea DCT se poate exploata şi pentru a crea aplicaţii de marcare în timp real.

În figura 2.5(a) este dat un exemplu pentru o imagine în care este plasat un marcaj CDMA bidimensional, W, în frecvenţele medii a blocurilor DCT de 8x8. Coeficienţii DCT de 8x8, F(u,v), sunt modulaţi conform:

$$I_{W_{x,y}}(u,v)=\begin{cases} I_{x,y}(u,v)+k\cdot W_{x,y}(u,v), & u,v\in F_M \\ I_{x,y}(u,v), & u,v\notin F_M \end{cases}, \quad x,y=1,8,16,... \qquad (2.3)$$

Aici F_M înseamnă frecvenţele medii, *k* factorul de câştig, (x,y) locaţia spaţială a unui bloc 8x8 de pixeli în imaginea I, şi (u,v) coeficientul DCT, în blocul DCT de 8x8 corespunzător (figura 2.6).

În figura 2.5(c) este prezentată diferenţa, puternic amplificată, dintre imaginea originală şi imaginea marcată. Figura 2.5(d) arată spectrul Fourier al marcajului. Se poate vedea că marcajul afectează doar frecvenţele medii (regiunile albe), lăsând componentele de frecvenţă joasă şi înaltă relativ neafectate (regiunile întunecate).

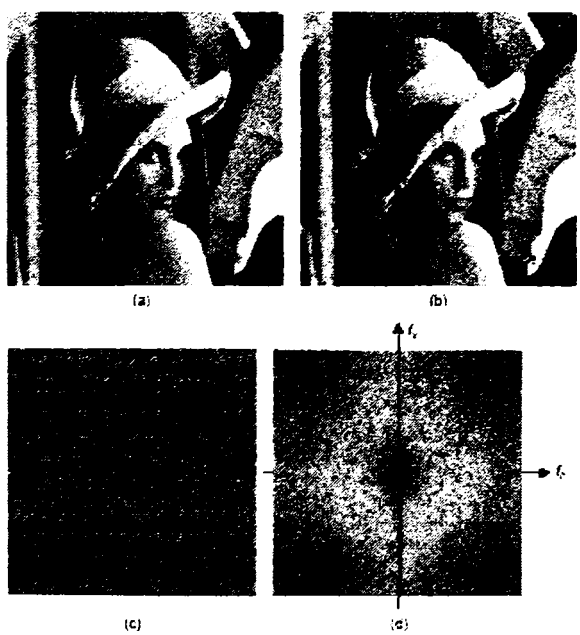


Fig. 2.5: Un marcaj DCT de 8x8, de bandă medie, independent de conţinutul imaginii. (a) Imaginea marcată, (b) Imaginea puternic marcată, (c) Diferenţa W(x,y)=I(x,y)-I_W(x,y), şi (d) Spectrul Fourier W(u,v)

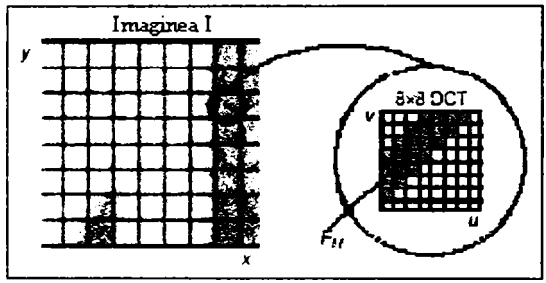


Fig. 2.6: Definirea benzii de frecvenţe medii într-un bloc DCT

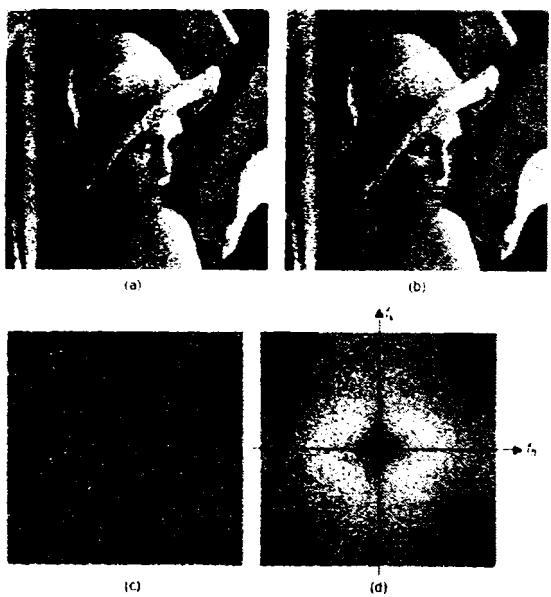


Fig. 2.7: Un marcaj DCT de 8x8, de bandă medie, dependent de conţinutul imaginii. (a) Imaginea marcată, (b) Imaginea puternic marcată, (c) Diferenţa W(x,y)=I(x,y)-I_W(x,y), şi (d) Spectrul Fourier W(u,v)

Marcajul poate fi făcut dependent de imagine prin schimbarea funcţiei de modulaţie cu:

$$I_{W_{x,y}}(u,v)=\begin{cases} I_{x,y}(u,v)(1+k\cdot W_{x,y}(u,v)), & u,v\in F_M \\ I_{x,y}(u,v), & u,v\notin F_M \end{cases}, \; x,y=1,8,16... \qquad (2.4)$$

Dacă este aplicată această funcţie de modulaţie, rezultatele din figura 2.5 se vor schimba în rezultatele prezentate în figura 2.7. Din figura 2.7(b) şi (c) reiese că majoritatea distorsiunilor introduse de marcaj sunt localizate în jurul marginilor şi în porţiunile cu „textură".

Îmbunătăţiri suplimentare pentru performanţele sistemelor de marcare în domeniul DCT, pe bază de corelaţie, pot fi obţinute prin folosirea detectoarelor de marcaj pe baza modelelor gaussiene generalizate şi nu pur gaussiene [HAPG00].

2.1.2.2.c Metode bazate pe transformata wavelet

Aceste tehnici implică înserarea informaţiei în benzile LH şi HH ale transformatei wavelet ale imaginii. Schimbările în aceste regiuni nu sunt sesizabile de către observatorii umani, din cauza caracteristicilor sistemului vizual uman [HW00, KH98, KH03, NI03, NBK04, KM99, KKK02, CM98, CN04]. Dacă tehnicile de marcare pot exploata caracteristicile HVS, este posibilă ascunderea marcajelor într-o imagine cu mai multă energie, lucru care creşte robusteţea marcajelor. Din acest punct de vedere transformarea wavelet discretă, DWT, este foarte atractivă, deoarece este mai eficientă din punctul de vedere al calculelor. Se pare că ochiul uman este mai puţin sensibil la zgomot în benzile DWT de rezoluţie înaltă şi în benzile DWT cu orientare de 45° (banda HH). În plus, codarea DWT a imaginilor şi a materialelor video, cum ar fi codarea EZW (Embedded Zero-tree Wavelet), este inclusă în standardele de compresie video şi de imagine, ca JPEG2000. Prin plasarea marcajului în acelaşi domeniu (domeniul DWT) se poate anticipa compresia EZW cu pierderi, deoarece se pot anticipa care benzi DWT vor fi afectate de schema de compresie. Mai departe, se poate exploata descompunerea DWT pentru a crea aplicaţii de marcare în timp real.

În figura 2.8(a) este dat un exemplu pentru o imagine în care este plasat un marcaj CDMA bidimensional, W, în benzile DWT: LH_1, HH_1, şi HL_1, folosind un factor de câştig *k* mare. Figura 2.8(b) arată diferenţa puternic amplificată, dintre imaginea originală şi cea marcată. Coeficienţii DWT din cele trei benzi DWT sunt modulaţi folosind relaţia:

$$I_W(u,v) = I(u,v) + k \cdot W(u,v) \tag{2.5}$$

(a) (b)

Fig. 2.8: Marcaj DWT independent de conţinutul imaginii.
(a) Imagine puternic marcată, şi (b) Diferenţa $W(x,y)=I(x,y)-I_W(x,y)$

Marcajul DWT poate fi făcut dependent de imagine, prin modularea coeficienţilor DWT în fiecare dintre cele trei benzi DWT conform ecuaţiei de mai jos:

$$I_W(u,v) = I(u,v)(1 + k \cdot W(u,v)). \tag{2.6}$$

În figura 2.9(a) este dat un exemplu pentru o imagine în care este plasat acelaşi marcaj CDMA, W, în benzile DWT: LH_1, HH_1, şi HL_1, conform relaţiei (2.6), cu un factor de câştig *k* mare.

(a) (b)

Fig. 2.9: Marcaj DWT dependent de conţinutul imaginii.
(a) Imagine puternic marcată, şi (b) Diferenţa $W(x,y)=I(x,y)-I_W(x,y)$

2.1.2.2.d Metode bazate pe transformata Fourier-Mellin

Aceste metode, relativ noi, au apărut din nevoia ca marcajul să fie invariant la atacuri geometrice (rotaţii, scalări şi translaţii, sau altfel spus invariant RST). Ele presupun crearea unei coordonate polare logaritmice a amplitudinii transformării DFT pentru imaginea originală, unde are loc înserarea. Acest tip de metode este extrem de rezistent, adică invariant, la atacurile de tip RST [LWBC01, RP98].

2.1.3 Codarea marcajului

Transmisia cu spectru împrăştiat SS este des folosită în domeniul marcării transparente, majoritatea tehnicilor bazându-se pe acest principiu. Avantajele de bază ale transmisiunilor cu SS sunt: reducerea efectelor interferenţelor şi prevenirea interceptării semnalului. Principial, comunicaţiile cu SS constă din transmiterea unui semnal de bandă îngustă, pe un canal de bandă largă, cu interferenţe. În acest caz semnalul de bandă îngustă este marcajul I, iar canalul de bandă largă este semnalul X, audio sau video.

Având în vedere că marcajele trebuie să aibă o putere mică pentru a atinge imperceptibilitatea, marcarea poate fi văzută ca o comunicaţie printr-un canal foarte zgomotos. Aproape toate schemele de marcare reprezintă încărcătura utilă (payload) sub forma unei secvenţe pseudo-aleatoare (PN). Numărul aleator folosit la generarea secvenţei devine cheia marcajului. Aceste scheme sunt private, deoarece pentru a detecta marcajul, decodorul trebuie să cunoască cheia [CKLS97, RP98].

Cele două etape ale marcării sunt:

-*Înserarea marcajului:* informaţia de marcaj, I, se împrăştie prin modulare cu un zgomot pseudo-aleator PN (Pseudo-Noise) care constituie cheia K, asigurând astfel mascarea zonelor din semnalul original afectate de marcaj. Folosirea tehnicii cu SS protejează eficient marcajul, mai ales împotriva manipulărilor neintenţionate, proprii procesărilor uzuale (compresie, scalare), de la transmiterea şi stocarea datelor.

-Detecţia marcajului: în cazul marcării bazate pe SS, detecţia autorizată (se cunoaşte K) este uşor de făcut şi fără originalul X, utilizând un receptor cu corelator. Desincronizările care pot să apară vor putea fi compensate prin utilizarea unui corelator cu fereastră glisantă, care va găsi prin alunecare, valoarea maximă a funcţiei de corelaţie şi deci va detecta valoarea adevarată a informaţiei I de marcaj. Detecţia marcajului conduce la decizia dacă datele au fost marcate folosind o anumită cheie sau nu.

Detectorul produce o anumită ieşire binară. Pentru a analiza corectitudinea funcţionării unui detector, avem doi parametri importanţi:

P_D=probabilitatea detecţiei corecte şi

P_{fa} = probabilitatea de alarmă falsă.

Pentru ca o metodă să fie cât mai bună, ea trebuie să aibă P_D cât mai mare şi P_{fa} cât mai mic. Aceşti parametri se pot folosi de asemenea şi pentru compararea diverselor metode de marcare transparenta.

În general pentru detecţie este folosită o versiune a marcajului, generată local. Acest marcaj este corelat cu datele recepţionate. Dacă la receptor, cheia folosită este cea corectă, atunci valoarea corelaţiei este mare. După detecţia corectă a prezenţei marcajului este posibilă extragerea acestuia cu ajutorul intercorelaţiei. În acest caz se ia o decizie independentă asupra fiecărui bit în parte.

O metodă îmbunătăţită de marcare, ISS, folosind SS, este propusă de Malvar şi Florencio [MF03]; ea înlătură semnalul ca sursă de interferenţă. Câştigul este similar cu cel obţtinut de QIM, dar ISS nu suferă de aceeaşi sensibilitate la scalare. Înserarea marcajului se face cu relaţia:

$$\mathbf{s} = \mathbf{x} + \mu(x,b)\mathbf{u},$$

unde funcţia $\mu(x,b)$ modulează secvenţa de marcaj, **u**. Parametrul b este intensitatea din algoritmul SS clasic, iar x este dat de $x \triangleq \langle \mathbf{x},\mathbf{u} \rangle / \|\mathbf{u}\|$. Autorii analizează cazul liniar:

$$\mathbf{s} = \mathbf{x} + (\alpha b - \lambda x)\mathbf{u},$$

spre deosebire de abordarea tradiţională SS:

$$\mathbf{s} = \mathbf{x} + b\mathbf{u}$$

Parametrii α şi λ controlează nivelul de distorsiune şi înlăturarea semnalului gazdă din statistica de detecţie. Tehnica SS tradiţională este obţinută pentru $\alpha = 1$ şi $\lambda = 0$.

Creşterea încărcăturii marcajului. Din punctul de vedere al detectorului marcajului, o imagine I poate fi privită ca un zgomot gaussian, care distorsionează informaţia de marcaj W. Mai departe, imaginea marcată I_W poate fi privită ca ieşirea unui canal de comunicaţie afectat de zgomot gaussian, prin care se transmite informaţia de marcaj. Transmisia sigură a marcajului este teoretic posibilă, dacă rata de informaţie a marcajului nu depăşeşte capacitatea canalului [SW49]:

$$C = W_b \log_2\left(1 + \frac{\sigma_W^2}{\sigma_I^2}\right) bit/pixel. \qquad (2.7)$$

Aici C este dată în biţi (ai informaţiei de marcaj) per pixel de imagine, şi lăţimea de bandă disponibilă W_b egală cu un Hertz per pixel. Pentru sistemele reale, totuşi, poate fi determinată empiric o limită mai redusă:

$$C = W_b \log_2\left(1 + \frac{\sigma_W^2}{\alpha \cdot \sigma_I^2}\right) bit/pixel . \qquad (2.8)$$

Aici, α este un factor de scală tipic mai mare ca 1, în jurul valorii trei. Deoarece raportul semnal/zgomot σ_W^2/σ_I^2 este mult mai mic decât unu, relaţia de mai sus poate fi aproximată cu:

$$C \approx \frac{1}{\ln 2}\left(\frac{\sigma_W^2}{\alpha \cdot \sigma_I^2}\right) bit/pixel . \qquad (2.9)$$

Conform relaţiei de mai sus, este posibilă introducerea a mai mult de 1 bit de informaţie într-o imagine. De exemplu, un marcaj alcătuit din numerele întregi {-k,k}, adăugat la imaginea Lena de 512x512 pixeli, poate avea aproximativ 50, 200 sau 500 de biţi de informaţie pentru k=1,2,3 şi α=3. Cea mai simplă metodă, de a plasa un şir de *l* biţi de marcaj $b_0b_1...b_{l-1}$ într-o imagine, este împărţirea imaginii I în *l* subimagini $I_0I_1...I_{l-1}$, şi adăugarea unui marcaj la fiecare subimagine, unde fiecare marcaj reprezintă un bit al şirului [LLL97], [SC96], [HLR00]. Acest procedeu este descris în figura 2.10.

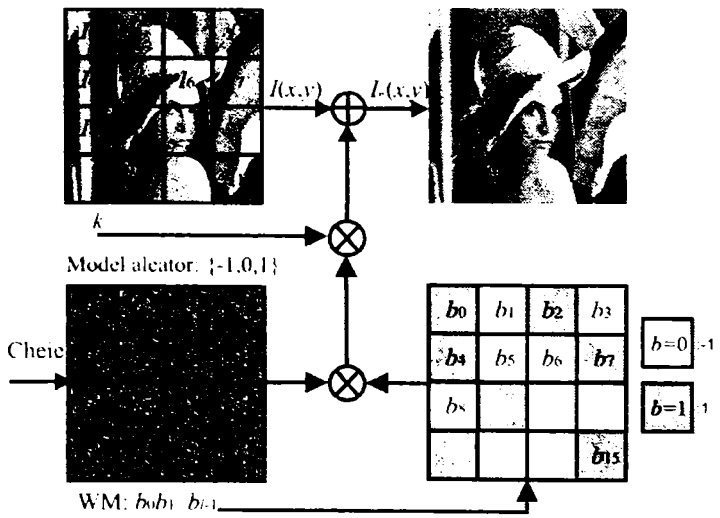


Fig. 2.10: Procedura de plasare a şirului biţilor de marcaj

Folosind relaţia (2.9) se pot calcula numărul de pixeli P, necesari per subimagine, pentru detecţia sigură a unui singur bit într-o subimagine:

$$P \approx \frac{\alpha\sigma_I^2 \ln 2}{\sigma_W^2} pixeli . \qquad (2.10)$$

Biţii de marcaj pot fi reprezentaţi în mai multe moduri. Dacă bitul de marcaj este 1, se adaugă o secvenţă pseudo-aleatoare, iar dacă este 0, subimaginea se

lasă neatinsă. În acest caz detectorul calculează corelaţia dintre subimagine şi secvenţa pseudo-aleatoare şi atribuie valoarea 1 bitului de marcaj, când corelaţia depăşeşte un anumit prag T, în caz contrar bitul de marcaj se consideră zero. Folosirea unui prag poate fi ocolită, prin adăugarea a două secvenţe pseudo-aleatoare diferite, RP_0 şi RP_1, pentru biţii de marcaj 0 şi 1. În acest caz detectorul calculează corelaţia dintre subimagine şi cele două modele. Bitului de marcaj i se asignează valoarea asociată secvenţei care generează corelaţia maximă. Cele două secvenţe pseudo-aleatoare pot fi alese astfel încât să difere doar prin semn, ca şi în [SC96]: RP_0=-RP_1. În acest caz, detectorul trebuie să calculeze doar o corelaţie dintre subimagine şi una dintre secvenţe; semnul corelaţiei determină valoarea bitului de marcaj.

Altă modalitate de a creşte încărcătura marcajului de bază este folosirea tehnicilor DS-CDMA (Direct Sequence-CDMA) [RP98a,b]. Pentru fiecare bit b_j din şirul biţilor de marcaj $b_0,b_1...b_{l-1}$ este generată o secvenţă pseudo-aleatoare diferită, stohastic independentă, RP_i , cu aceeaşi dimensiune ca imaginea. Acest model este independent de valoarea bitului b_j. Aici se foloseşte modelul $+RP_i$ dacă b_j reprezintă un 0, şi $-RP_i$ dacă b_j reprezintă un 1. Suma tuturor celor l secvenţe aleatoare $\pm RP_i$ formează marcajul. Înaintea adăugării la imagine, marcajul se poate scala cu un factor, sau se poate limita la un anumit domeniu. Un exemplu pentru generarea unui marcaj unidimensional este prezentat în figura 2.11. Sunt folosite şapte secvenţe pseudo-aleatoare diferite, pentru plasarea celor şapte biţi de marcaj 0011010.

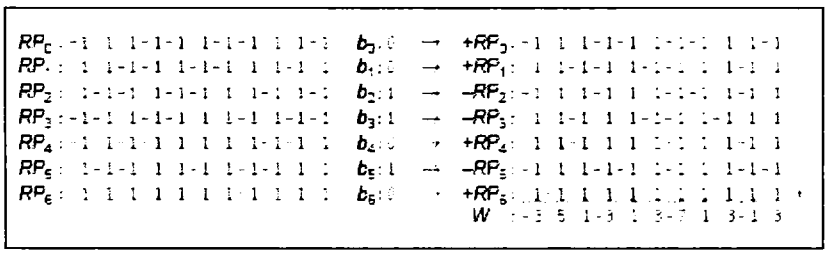


Fig. 2.11: Exemplu pentru generarea unui marcaj CDMA pentru 7 biţi $b_0,b_1...b_l$

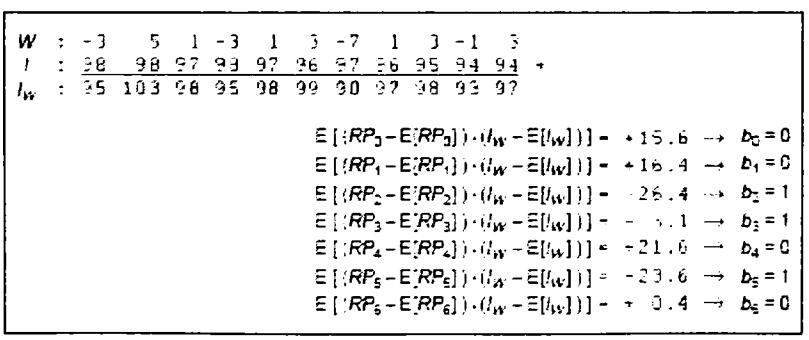


Fig. 2.12: Exemplu pentru extragerea marcajului CDMA

Fiecare bit b_j din şirul biţilor de marcaj $b_0,b_1...b_{l-1}$ poate fi extras prin calcularea corelaţiei dintre imaginea normalizată I_W' şi secvenţa pseudo-aleatoare corespunzătoare RP_i. Când corelaţia este pozitivă, este asignată bitului de marcaj valoarea 0, altfel se presupune că bitul de marcaj este 1. Figura 2.12 arată, extragerea biţilor de marcaj plasaţi în figura 2.11.

Metodele pentru creşterea încărcăturii marcajului descrise mai sus, şi anume, folosirea de porţiuni de imagine individuale pentru fiecare bit de marcaj şi folosirea CDMA, au avantajele şi dezavantajele lor. Dacă fiecare bit de marcaj are propria porţiune de imagine, nu există interferenţă între biţi, şi este necesar doar un număr mic de înmulţiri pentru calculul corelaţiei. Dar dacă se decupează o porţiune de imagine se pierd biţii de marcaj de la margine. Dacă se foloseşte tehnica CDMA, probabilitatea ca toţi biţii să fie recuperaţi după decuparea imaginii este mare. Totuşi, biţii de marcaj pot interfera între ei, şi este necesară efectuarea multor înmulţiri pentru calcularea corelaţiilor, deoarece fiecare bit este complet împrăştiat pe suprafaţa imaginii.

Biţii de marcaj plasaţi, folosind metodele menţionate, pot reprezenta orice: mesaje copyright, numere de serie, text simplu, semnale de control, etc. Conţinutul reprezentat de aceşti biţi poate fi comprimat, criptat şi protejat prin coduri corectoare de erori. În unele cazuri poate fi util un logo ca marcaj, în locul unui şir de biţi. Dacă imaginea marcată este distorsionată, logo-ul va fi afectat şi el. Pentru detectarea lui pot fi exploatate capacităţile HVS de recunoaştere a modelelor [Bra97], [HW96], [VP96].

Creşterea încărcăturii marcajului poate fi făcută, [CBM02], folosind multiplexarea cu diviziune în: timp/spaţiu (TDM/SDM), în frecvenţă (FDM), sau în cod (CDM). În primele două cazuri, imaginea este împărţită în componente spaţiale sau spectrale şi fiecare bit al marcajului este înserat în părţi separate ale imaginii, în spaţiu sau frecvenţă. În al treilea caz se foloseşte comunicaţia cu spectru împrăştiat cu diviziune prin cod şi secvenţă directă, DS-CDMA. Este generat pentru fiecare bit, câte un model diferit pseudo-aleator independent şi stohastic, RP_i depinzând de valoarea acestuia (de exemplu $+RP_i$ dacă b_j reprezintă un 0 şi $-RP_i$ dacă b_j reprezintă un 1). Suma celor *l* modele aleatoare $\pm RP_i$ reprezintă marcajul.

Codurile corectoare de erori sunt folosite pentru a creşte robusteţea unui marcaj. De obicei, încărcătura marcajului este codată, înainte de înserare [MDC02, AWS01, AP00, AGP02, BPGS01].

2.1.4 Formarea semnalului marcat

Cea mai simplă cale de marcare este *modulaţia* de amplitudine [LWBC01, RP98] sau de fază [RDB96] a imaginii originale şi a marcajului (ne referim la modulaţia de fază numai pentru domeniul unei transformate). Energia marcajului poate fi crescută dacă este folosită mascarea perceptuală. HVS este mai puţin sensibil la schimbări în zone cu luminanţă mare, contururi şi texturi într-o imagine. În tehnicile aditive, cea mai simplă formă de a creşte energia marcajului, fără a degrada calitatea imaginii marcate, este folosirea unui factor de câştig adaptat local [KM99, KKK02].

Un alt tip de înserare a marcajului este bazat pe *cuantizare* [CW01a, b], unde eşantioanele semnalului gazdă sunt cuantizate în funcţie de bitul de marcaj, rezultând astfel semnalul marcat. Decodorul cuantizează eşantioanele primite şi decide cărei cuante îi corespunde fiecare eşantion. Astfel, semnalul gazdă nu se mai comportă ca o interferenţă, spre deosebire de tehnicile spread spectrum.

Modulaţia prin cuantizare indexată QIM [CW99] este diferită de tehnicile LSB şi SS. Cea mai simplă formă de marcare QIM cuantizează semnalul gazdă folosind un cuantizor indexat de mesajul de marcaj. Dacă se notează cu *s* semnalul marcat, cu *m* mesajul şi cu *x* semnalul gazdă, atunci $s(x,m) = q_m(x)$. Semnalul rezultat va fi compus numai din valori din setul posibil al ieşirilor cuantizorului. Acest tip de marcare este adecvat mai ales în cazul în care semnalul rezultat va fi cuantizat, de

exemplu prin compresie. Modulaţia de dither (o schemă ordonată de corecţie) poate produce un semnal care conţine toate valorile din semnalul gazdă. Valorile cuantizate sunt translatate, cu un nivel variabil de dither, de exemplu cu relaţia $s(x,m) = q_m(x + d) - d$.

Aceste tehnici sunt mai robuste, şi optimale din punct de vedere al transmiterii informaţiei, decât metodele clasice de tip LSB sau SS. Dar metodele clasice QIM nu sunt robuste la scalare; o soluţie este utilizarea unui pas variabil de cuantizare, folosind un model perceptual [LC05].

Tehnicile SS de marcare, care folosesc pentru detecţia marcajului semnalul original, au în general performanţe mai bune decât cele care nu folosesc semnalul original. În majoritatea sistemelor SS de marcare private, secvenţa de zgomot pseudo-aleator alb este adăugată la semnalul original, şi detectată prin corelaţia cu semnalul marcat. Aceasta înseamnă că marcajul este înglobat în domeniul spaţial sau al transformatei semnalului printr-o adunare (operaţie liniară). De exemplu, dacă marcajul este adăugat în domeniul spaţial, atunci imaginea marcată este dată de relaţia:

$$f_w = f + w. \tag{2.11}$$

unde f şi f_w sunt semnalele original şi, respectiv, marcat, iar w este marcajul generat pseudo-aleator. Pentru a testa existenţa unui marcaj w_0 într-un semnal dat f_w, se calculează intercorelaţia dintre f_w şi w_0. Mai precis,

$$\rho(f_w, w_0) = \rho(f, w_0) + \rho(w, w_0) \tag{2.12}$$

unde $\rho(\cdot,\cdot)$ reprezintă coeficientul de intercorelaţie, aşa cum s-a definit în relaţia (2.2). Rezultatul are doi termeni: intercorelaţia dintre semnalul gazdă şi marcajul cunoscut şi intercorelaţia dintre marcajul extras şi cel cunoscut.

Dacă $\rho(f, w_0)$ are o valoare relativ mare, detectorul poate să nu fie de încredere. Dacă este cunoscut semnalul original, prima estimare a marcajului înglobat se poate face prin scăderea semnalului original din cel marcat. Apoi rezultatul este comparat cu marcajul cunoscut, cu ajutorul coeficientului de intercorelaţie, îmbunătăţindu-se astfel detecţia.

Dezavantajele marcării [KH01], prin analogie cu comunicaţiile cu SS, sunt:

- SS permite detecţia unui marcaj cunoscut, dar banda largă de frecvenţe cerută nu permite introducerea unei secvenţe lungi de biţi sau a unui *logo,* într-un semnal audio sau într-o imagine.
- Abordările SS sunt vulnerabile la problema *„near-far"*. Efectul *„near-far"* apare atunci când sursa de perturbaţii este mai aproape de receptor decât sursa de informaţii. În consecinţă, puterea zgomotului este mai mare decât cea a semnalului purtător de informaţie. Aceasta înseamnă pentru marcare că, dacă puterea marcajului scade datorită distorsiunilor cauzate de *fading*, rezultatul detecţiei prezintă un grad de încredere redus.
- Cele mai multe abordări SS nu sunt adaptive. Aceasta înseamnă că ele nu ţin cont nici de nestaţionaritatea spaţială a imaginii originale, cauzată de interferenţe, şi nici nu includ tehnici adaptive pentru a estima variaţiile statistice.
- Structura corelatorului, folosit pentru detecţia marcajului, nu este eficientă în prezenţa *fading*-ului. Deşi sistemele SS încearcă să

exploateze împrăştierea marcajului pentru a media *fading*-ul, acestea nu sunt gândite pentru a maximiza performanţa. În mediile în care predomină *fading*-ul, se foloseşte diversitatea spaţio-temporală pentru a elimina efectele acestuia.

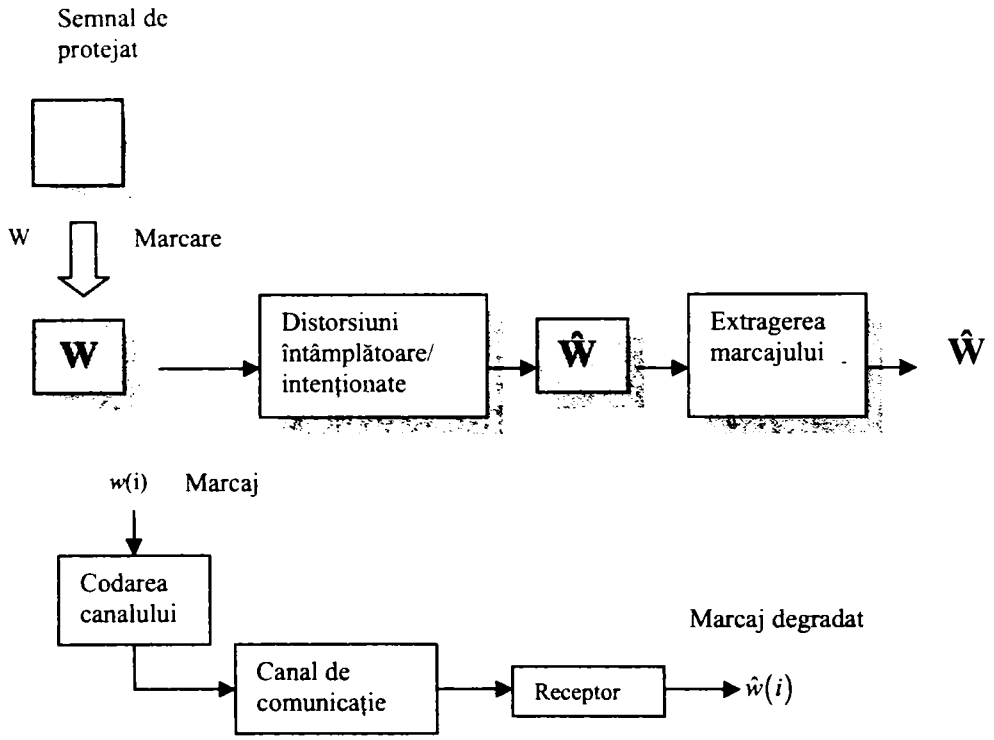


Fig. 2.13: Marcarea ca o problemă de comunicaţii. Înglobarea marcajului şi procesul de extragere pot fi interpretate ca o transmisie într-un mediu zgomotos cu fading.

În [KH01], autorii consideră că SS nu este cel mai adecvat pentru modelarea transmisiei marcajului printr-un canal de comunicaţie. Transmiterea marcajului poate fi asemănătoare cu transmisia semnalului printr-un canal asociat (Figura 2.4). Se presupune că distorsiunile obişnuite ale semnalului, decuparea, filtrarea, şi codarea perceptuală, nu sunt modelate adecvat, ca un zgomot de interferenţă de bandă îngustă, ci au un efect de *fading* asupra marcajului. Deci, folosind diversitatea şi caracterizările atacurilor, marcajul poate fi făcut mai robust [KH01].

Din cauza importanţei robusteţii pentru cazul distorsiunilor spaţiale şi spectrale, marcajul se înglobează în domeniul *wavelet*, care localizează astfel de degradări. Acest domeniu permite o marcare robustă mai eficientă şi, în cazul marcării fragile, este mai potrivit pentru a caracteriza modificările făcute cu rea intenţie.

2.1.5 Extragerea marcajului

Cea mai simplă metodă de a plasa un marcaj într-o imagine, este adăugarea unui zgomot pseudo-aleator la luminozitatea pixelilor imaginii. Multe metode se bazează pe acest principiu [BGM95], [STO94], [HG96], [Pit96], [WD96].

În general zgomotul pseudo-aleator constă din numerele întregi {-1,0,1}; dar pot fi folosite şi numere care nu sunt întregi. Zgomotul este generat pe baza unei chei folosind stări ale generatorului (*seeds*). Singurele constrângeri sunt ca energia lui să fie uniform distribuită, mai mult sau mai puţin, şi să nu fie corelat cu conţinutul imaginii gazdă. Pentru a crea imaginea marcată $I_w(x,y)$, modelul pseudo-aleator W(x,y) este multiplicat cu un mic factor de câştig *k* şi adunat la imaginea gazdă I(x,y):

$$I_W(x,y) = I(x,y) + k \cdot W(x,y). \tag{2.13}$$

Pentru a detecta un marcaj într-o imagine $I_w'(x,y)$, posibil marcată, se calculează corelaţia dintre imaginea $I_w'(x,y)$ şi zgomotul pseudo-aleator W(x,y). În general, W(x,y) este normalizat înainte de corelaţie, la o medie nulă. Modelele pseudo-aleatoare, generate folosind diferite chei, au o corelaţie foarte redusă între ele. De aceea, pe durata procesului de detecţie, valoarea corelaţiei va fi foarte mare pentru un model pseudo-aleator generat cu cheia corectă, şi va fi foarte mică în caz contrar.

Pe durata procesului de detecţie, se alege de obicei un prag T, pentru a decide dacă marcajul este detectat sau nu. Când corelaţia depăşeşte pragul T, detectorul de marcaj stabileşte că imaginea $I_w'(x,y)$ conţine marcajul W(x,y):

$$\begin{matrix} R_{I_W'(x,y)W(x,y)} > T \rightarrow W(x,y) \text{ detectat} \\ < T \rightarrow \text{nu este detectat } W(x,y) \end{matrix}. \tag{2.14}$$

Dacă W(x,y) este alcătuit doar din numerele întregi {-1,1}, şi dacă numărul de „-1" este egal cu numărul de „1", corelaţia se poate estima ca fiind [LSL00]:

$$\begin{aligned} R_{I_W'(x,y)W(x,y)} &= \frac{1}{N}\sum_{i=1}^{N} I'_{W_i}(x,y)W_i(x,y) = \frac{1}{N}\sum_{i=1}^{N/2} I'_{W_i}W_i^{+} + \frac{1}{N}\sum_{i=1}^{N/2} I'_{W_i}W_i^{-} \\ &= \frac{1}{2}\left\{\mu\left[I_W'^{+}(x,y)\right] - \mu\left[I_W'^{-}(x,y)\right]\right\} \end{aligned} \tag{2.15}$$

Aici N este numărul punctelor de imagine din imaginea I_W', iar +,- indică setul de puncte unde zgomotul corespunzător este pozitiv sau negativ, şi $\mu[I_W'^{+}(x,y)]$ reprezintă valoarea medie a setului de puncte în $I_W'^{+}(x,y)$. Din relaţia (2.15) rezultă că problema detecţiei marcajului corespunde cu testarea ipotezei că două seturi de puncte de imagine, alese aleator dintr-o imagine marcată, au aceeaşi medie.

Pe durata procesului de detecţie, detectorul de marcaj poate comite două tipuri de erori (vezi cap. 1). Poate detecta existenţa marcajului, deşi acesta nu există (*fals pozitiv*), sau respinge existenţa marcajului, deşi marcajul este prezent (*fals negativ*). Funcţia densităţii de probabilitate pentru procesul de detecţie este prezentată în figura 2.14.

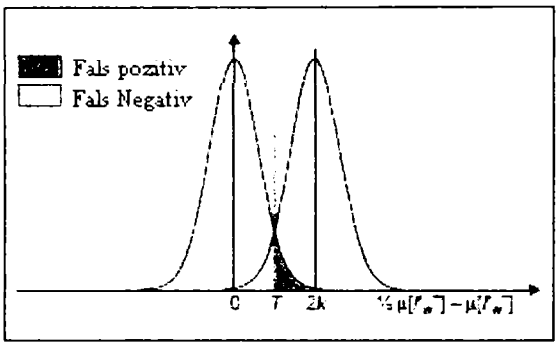


Fig. 2.14: Procedura de detecţie a marcajului

Probabilităţile acestor două tipuri de erori rezultă pe baza modelului autoregresiv de ordin întâi a imaginii [LSL00]:

$$P_{fp} = \frac{1}{2}\operatorname{erfc}\left(\frac{T\sqrt{N}}{\sigma_W \sigma_1 \sqrt{2}}\right) \text{ şi}$$
$$P_{fn} = \frac{1}{2} erfc\left(\frac{\left(\sigma_W^2 - T\right)\sqrt{N}}{\sigma_W \sigma_1 \sqrt{2}}\right) \qquad (2.16)$$

unde

$$\operatorname{erfc}(c) = \frac{1}{\sqrt{2\pi}} \cdot \int_x^\infty e^{-t^2/2} dt$$

Aici P_{fp} reprezintă probabilitatea de fals pozitiv, iar P_{fn} reprezintă probabilitatea de fals negativ (P_{fp} a fost notată în capitolul 1 cu P_{fa}, iar P_{fn} a fost notată în capitolul 1 cu P_{rej}), σ_W^2 reprezintă dispersia pixelilor marcajului şi σ_I^2 reprezintă dispersia pixelilor din imagine. Dacă marcajul W(x,y) constă doar din numerele întregi {-1,1}, şi numărul de „-1" este egal cu numărul de „1", dispersia marcajului, σ_W^2 , este egală cu k^2. Erorile P_{fp} şi P_{fn} pot fi minimizate crescând factorul de câştig k. Totuşi, folosind valori mai mari pentru factorul de câştig, scade calitatea vizuală a imaginii marcate.

Întrucât conţinutul imaginii poate interfera cu marcajul, în special în componentele de joasă frecvenţă, fiabilitatea detectorului poate fi îmbunătăţită prin aplicarea unei filtrări adecvate înainte de corelaţie [DKL98, STO94]. Acest lucru scade contribuţia imaginii originale la corelaţie. De exemplu, poate fi folosit, un filtru simplu, cu răspuns finit la impuls (FIR), de intensificare a marginilor, F_{edge}:

$$F_{edge} = \frac{1}{2} \cdot \begin{bmatrix} -1 & -1 & -1 \\ -1 & 10 & -1 \\ -1 & -1 & -1 \end{bmatrix}.$$

Rezultatele experimentale arată că filtrarea înainte de corelaţie reduce semnificativ probabilitatea de eroare, chiar dacă a fost serios afectată calitatea vizuală a imaginii marcate, înainte de corelaţie [HLR00], [LLL97]. În [LR00] pentru creşterea robusteţii marcajului este propusă egalizarea spectrală înaintea plasării marcajului.

Cele mai multe tehnici bazate pe SS folosesc corelaţia pentru detecţia marcajului. Acest tip de detector presupune implicit că interferenţa este gaussiană. Cu toate acestea, imaginile nu au o distribuţie gaussiană şi mulţi autori sugerează prefiltrarea imaginii înainte de detecţie, pentru a îmbunătăţi performanţa detectorului, din cauză că cea mai mare energie se află în frecvenţele joase ale acesteia. Filtrarea trece-sus face ca imaginea să aibă o distribuţie mai apropiată de cea gaussiană. În schemele private de marcare transparentă, extragerea imaginii originale din cea marcată, este tot o formă de prefiltrare.

În abordările bazate pe SS, se presupune că există o sincronizare perfectă între transmiţător şi receptor. Dacă imaginea este decupată, scalată sau transformată geometric, apare desincronizarea. Unele lucrări propun marcaje invariante la astfel de atacuri geometrice, RST, bazate pe transformarea Fourier-Mellin [RP98].

In [CM03] se propune *detecţia secvenţială a marcajului*, care duce la o creştere în viteză faţă de detectoarele cu mărime fixă. Sunt discutate optimizarea codării asociată cu detecţia marcajului şi autorii constată creşterea în viteză cu 70%. Metoda poate avea succes în multe aplicaţii practice. Detecţia secvenţială permite controlarea simultană a probalititătilor de alarmă falsă şi de eroare (*miss*). Se fixează aceste probabilităţi şi apoi se variază numărul eşantioanelor încât să se obţină aceste probabilităţi. Lungimea marcajului este aleasă ad-hoc, dar autorii propun o cale de calculare a lungimii pentru o metodă dată.

2.2 Tehnici de marcare transparentă

Tehnicile de marcare transparentă din literatură pot fi grupate în trei mari clase:

-Prima include metodele din *domeniul transformatelor*, care înserează informaţia de marcaj prin modularea coeficienţilor transformatei imaginii originale.

-A doua clasă include tehnicile din *domeniul spaţial*, care înserează marcajul modificând direct valorile pixelilor imaginii originale. Tehnicile care înserează marcajul în domeniul unei transformate se dovedesc a fi mai robuste la prelucrări obişnuite de semnal.

-A treia clasă sunt tehnicile care folosesc *domenii cu caracteristici speciale* (*feature domain*). Aceste tehnici ţin cont de regiuni, graniţe şi caracteristicile unui obiect. Astfel de tehnici pot prezenta avantaje în plus faţă de celelalte abordări, în detecţia şi recuperarea marcajului după atacuri geometrice.

Se face o trecere în revistă a principalelor tehnici de marcare conform cu domeniul de înserare. Sunt de asemenea considerate şi exemple de tehnici din domeniul spaţial şi domeniul fractal.

Dintre numeroasele tehnici existente, ne vom axa în principal asupra tehnicilor ce folosesc domeniul wavelet. Deşi acesta pare să fie cel mai eficient până acum, vom considera în cele ce urmează şi celelalte tehnici existente, pentru a avea o imagine de ansamblu asupra principalilor algoritmi.

2.2.1 Algoritmi în domeniul spaţial

Multe tehnici din domeniul spaţial sunt bazate pe adunarea la o imagine, a unei secvenţe de zgomot pseudo-aleator. Operatorii din capitolul 1, $\mathcal{E}$ şi D sunt adunarea şi scăderea. De obicei, marcajul modifică direct valorile pixelilor din imaginea originală, şi anume biţii cei mai puţin semnificativi, LSB, ai imaginii gazdă. Avantajele tehnicilor de marcare bazate pe LSB includ capacitatea mare şi complexitatea de calcul redusă. De aceea, este de aşteptat ca ele să fie puse în practică mai uşor atunci când este vorba de marcarea în timp real. Principalul lor dezavantaj este lipsa de robusteţe la falsificare, atacuri geometrice, filtrare şi compresie.

Tanaka ş. a. [TNM90] au introdus ideea etichetării (tagging) imaginilor pentru ascunderea informaţiei secrete şi asigurarea drepturilor de autor. Pentru înserarea marcajului algoritmul foloseşte o schemă de codare cu predicţie. Marcajul este înserat prin dither-area imaginii, bazată pe proprietăţile statistice ale imaginii.

Caronni [Car95] descrie un sistem de urmărire a distribuţiei neautorizate a imaginilor. El propune marcarea imaginilor fososind modularea spaţială şi numeşte acest proces etichetare. Eticheta este un pătrat de mărime NxN cu valoarea constantă, proporţională cu luminanţa locală maximă a imaginii.. In primul pas, sunt identificate toate locaţiile posibile din imagine unde ar putea fi înserată o etichetă, prin calcularea dispersiei locale şi compararea ei cu nişte limite inferioare şi superioare, determinate empiric. Pentru înserare sunt folosiţi numai pixelii cu dispersia minimă. Aria selectată este marcată prin adunarea/scăderea etichetei şi a unei structuri aleatoare, de medie nulă. Locaţia etichetei şi secvenţa de zgomot sunt generate cu o cheie. Pentru a recupera bitul înserat, se calculează diferenţa dintre imaginea etichetată şi cea originală. Media locaţiei, presupusă marcată, este comparată cu media locaţiei vecine, pentru a determina valoarea bitului. Ca măsură a degradării imaginii etichetate, Caronni propune coeficientul de corelaţie dintre imaginea originală şi cea etichetată. Coeficientul de corelaţie 1 arată că cele două sunt identice, dar pentru imaginile puternic afectate de procesul de marcare, acesta va fi apropiat de zero.

Primele tehnici de marcare fragilă, ca cele descrise de Walton [Wal95] şi Van Schyndel [STO94], înserau marcajul direct în domeniul spaţial al unei imagini. În tehnica de marcare fragilă de semnare a lui Walton, se calculează o sumă de control pentru cei mai semnificativi 7 biţi din planul de biţi ai imaginii, ascunsă apoi în biţi LSB aleşi aleator.

Alte tehnici [STO94], [SO93], [WD96] înserează în planul de biţi LSB, secvenţe-*m*, pentru că prezintă corelaţii foarte bune, şi se poate folosi un detector corelativ. O astfel de schemă a fost propusă în [STO94] şi extinsă la 2D în [SO93].

Tirkel ş.a. [TRSH93] recunosc importanţa marcării transparente şi propun ca aplicaţii etichetarea, protejarea drepturilor de autor, protejarea împotriva falsificării şi accesul controlat la imagini. Pentru imaginile alb-negru sunt propuse două metode. În prima, marcajul, sub forma unui cod PN generat dintr-o secvenţă-*m*, este înserat în planul biţilor LSB, a imaginii originale. Pentru acces nelimitat la planul de biţi LSB, fără introducerea unor distorsiuni vizibile, imaginea este mai întâi comprimată la 7 biţi, prin manipulări adaptive a histogramei. Metoda este o extensie a metodei simple de codare LSB, prin care biţii LSB sunt înlocuiţi cu o informaţie codată. Decodarea este directă, deoarece planul LSB conţine marcajul fără distorsiuni. În a doua, marcajul, generat la fel, este adunat la planul de biţi LSB. Decodarea se face folosind proprietatea de autocorelaţie unică şi optimală a secvenţelor *m*.

Prima lucrare care menţionează explicit şi defineşte noţiunea de marcare transparentă digitală (watermarking) este lucrarea lui *Schyndel* ş.a. [STO94]. Sunt descrise două tehnici: în prima se înlocuiesc biţii LSB ai imaginii, iar în a doua se adună o secvenţă PN la planul de biţi LSB al imaginii originale, folosind pentru detecţie autocorelaţia. Aceasta este de fapt şi ideea folosirii secvenţelor-*m*; adunarea LSB este extinsă, îmbunătăţită şi conduce la o schemă mai robustă, folosind secvenţe-*m* bidimensionale, 2D [TSO93].

Wolfgang şi Delp [WD96] au continuat munca lui van Schyndel pentru a îmbunătăţi robusteţea şi localizarea marcajelor, cu tehnica VW2D. Marcajul este înserat prin adăugarea unei secvenţe-*m* bipolare, în domeniul spaţial. Detecţia se face printr-un detector corelator modificat. O secvenţă aleatoare este transformată din {0,1} în {1,-1}, aranjată într-un bloc şi adunată la imagine. Pentru a localiza falsificarea în domeniul spaţial, algoritmul suprapune imaginea cu blocul de marcaj, calculează produsul scalar şi îl compară cu valoarea ideală. Fie funcţia de intercorelaţie $R_{XY}(\alpha,\beta)$ a două blocuri X şi Y:

$$R_{XY}(\alpha,\beta)=\sum_i\sum_j X(i,j)Y(i-\alpha,j-\beta). \tag{2.17}$$

Fiind dată imaginea originală X, blocul de marcaj W, imaginea marcată Y şi imaginea probabil falsificată Z, atunci statistica test δ pentru un bloc, e definită ca:

$$\delta = R_{YW}(0,0)-R_{ZW}(0,0). \tag{2.18}$$

Dacă marcajul este neschimbat, $\delta=0$, iar dacă δ depăşeşte un anumit prag, imaginea se consideră falsificată. Metoda detectează orice tip de filtrare şi autorii susţin că o variantă îmbunătăţită a acesteia detectează şi compresia JPEG.

Matsui şi Tanaka [MT94] propun mai multe tehnici de marcare a imaginilor. Prima metodă este bazată pe o schemă de codare cu predicţie, pentru imagini cu nivele de gri, care foloseşte corelaţia dintre pixelii vecini, prin codarea erorii de predicţie, în loc să codeze valorile pixelilor individuali. Imaginea digitală este scanată într-o ordine predefinită, parcurgându-se toţi pixelii. Setul de pixeli este apoi codat, folosind o schemă de codare cu predicţie, păstrând prima valoare şi înlocuind valorile următoare cu diferenţa între pixelii vecini:

$$e_i = x_i - x_{i-1}. \tag{2.19}$$

Tab. 2.1 Tabela de cifrare (sample cipher key)

Δ_i	...	-4	-3	-2	-1	0	1	2	3	4	...
c_i	...	0	0	1	1	0	1	0	0	1	...

Pentru a însera un marcaj sub forma unui şir binar, Matsui şi Tanaka introduc o tabelă de cifrare cu cheie, care asignează un bit c_i fiecărei diferenţe Δ_i posibile (în tabelul 2.1 este dat un exemplu). Corespondenţa dintre valorile biţilor şi

diferenţe este ţinută secretă. Pentru a însera un bit b, se selectează un pixel x_i, cu diferenţa corespunzătoare e_i. Se verifică în tabel dacă valoarea bitului c_i, corespunzând lui $\Delta_i = e_i$, are aceeaşi valoare ca şi bitul b. Dacă da, se trece la înserarea următorului bit. Dacă nu, se selectează cea mai apropiată valoare de e_i în tabela de cifrare care are bitul corespunzător. Marcajul poate fi recuperat prin căutarea bitului în tabela de cifrare.

În a doua metodă se modifică schema ordonată de corecţie (dither), pentru imagini binare. O schemă de corecţie este formată prin compararea nivelelor monotone ale pixelilor dintr-un bloc, cu un prag dependent de poziţie, şi punerea pe 1 a pixelilor care depăşesc pragul. Pragurile dependente de poziţie sunt date într-o matrice pătrată, N*N, matricea de corecţie, cu elementele $d_{pq}^{(n)}$, unde n indică numărul de ordine, între zero şi N^2-1, iar p şi q sunt linia şi coloana (vezi Fig. 2.15).

6	7	8	9
5	0	1	10
4	3	2	11
15	14	13	12

Fig. 2.15 Matrice dither concentrată pe un punct

Fiind dată o matrice de corecţie, valorile de prag corespunzătoare sunt:

$$T = \left(d_{pq}^{(n)} + \frac{1}{2} \right) \times \frac{R}{N^2}. \qquad (2.20)$$

unde R este gama luminanţei dinamice a imaginii. Pentru a corecta o imagine, ea este împărţită în blocuri adiacente, de aceeaşi mărime cu matricea de corecţie. Fiecare valoare dintr-o matrice este apoi comparată cu valoarea de prag corespunzătoare şi modificată în consecinţă. Fie mulţimea perechilor de praguri:

$$S_k = \left\{ \left(x_i, x_j \right)_k \middle| x_i - x_j = k; i, j = 0,1,...,N; i \neq j \right\}. \qquad (2.21)$$

unde x_i, x_j sunt pragurile din matricea dither. Fie $\left(y_i, y_j \right)_k$ semnalul de ieşire al lui x_i, x_j şi presupunem că valorile sunt $(0,0)_k$, $(0,1)_k$, $(1,0)_k$ şi $(1,1)_k$; doar două perechi (0,1) şi (1,0) sunt considerate pentru înserarea datelor. Pentru a însera un bit b este selectată o pereche de ieşire $\left(y_i, y_j \right)_k$ şi y_i este comparat cu valoarea bitului b. La valori egale perechea rămâne neschimbată, altfel y_i si y_j sunt

schimbate între ele. Pentru a decoda semnătura înserată, procedura descrisă mai sus este inversată. Din nou perechile $(0,0)_k$, $(1,1)_k$ nu sunt luate în considerare.

A treia schemă este propusă pentru marcarea documentelor facsimil. Documentele facsimil sunt scanate, cu o rezoluţie orizontală de aproximativ 8.22 pixeli/mm şi apoi sunt comprimate folosind o codare cu pas variabil (Run Length Encoding), urmată de o codare Huffman modificată. Procesul de înserare modifică pasul variabil dintre două secvenţe, schimbând pixelii. Dacă trebuie înserat un 1, pasul variabil este forţat să fie par, iar dacă trebuie introdus un 0, pasul este forţat să fie impar. Pentru o înserare validă, pasul variabil original trebuie să fie mai mare decât 1. Decodarea unui bit se face inspectând lungimea pasului variabil decodat.
Se constată că marcarea digitală, modulaţia digitală şi mai ales modulaţia cu spectru împrăştiat cu secvenţă directă (DS-SS) au concepte similare. Astfel, s-a propus marcarea trasparentă ca o comunicaţie afectată de zgomot negaussian. Prima abordare teoretică a fost propusă de Smith [SC96]. Hernandez ş.a. [HPGR98] au făcut o analiză mai aprofundată a modulaţiei în amplitudine a impulsurilor multiple 2D.
Bender ş.a. [BGM95, BGML96] propun două tehnici de marcare. Una din acestea, o metodă statistică de marcare, cunoscută şi ca metoda *patchwork* [BGM95], împarte imaginea în 2 subseturi, A şi B, unde luminanţa unui subset este crescută cu o cantitate mică, iar luminozitatea celuilalt subset B este scăzută cu aceeaşi cantitate. Perechea de pixeli (a_i, b_i) este folosită pentru a ascunde un bit 1; se creşte valoarea lui a_i cu 1, şi se descreşte valoarea lui b_i cu 1. Presupunând că imaginea gazdă are anumite proprietăţi statistice, marcajul poate fi regăsit foarte uşor, prin medierea diferenţei dintre valorile celor două subseturi. Se presupune că, dacă nu există marcaj, diferenţa medie este apropiată de zero. Numărul de pixeli din fiecare set fiind n: dacă pixelii din A sunt incrementaţi cu 1, iar cei setul B sunt decrementaţi cu 1, suma diferenţelor între cele două seturi este egală cu $2n$:

$$\sum_n (a_i - b_i) = \begin{cases} 2n, & \text{perechi marcate} \\ 0, & \text{perechi nemarcate} \end{cases} \tag{2.22}$$

A doua metodă, numită codarea blocurilor cu textură, inserează marcajul prin copierea unui bloc de textură, într-o altă zonă a imaginii cu textură similară. Pentru recuperarea marcajului, este folosită autocorelaţia. Proprietatea interesantă a tehnicii este robusteţea la orice fel de distorsiune, deoarece ambele zone din imagine sunt la fel distorsionate, deci recuperarea marcajului prin autocorelaţie încă funcţionează.

Pitas şi Kaskalis [NP96, Pit96, PK95] propun o metodă de înserare a semnăturii, bazată pe ideea algoritmului patchwork, folosit de Bender ş.a. [BGM95]. Marcajul $S = \{s_{m,n}\}$ este format dintr-un model binar, de aceeaşi mărime ca imaginea originală, având acelaşi număr de 1 ca şi de 0 (distribuţie uniformă). Imaginea originală I, împărţită aleator în două subseturi A şi B de aceeaşi mărime este:

$$\begin{aligned} A &= \{x_{mn} \in I, s_{mn} = 1\} \\ B &= \{x_{mn} \in I, s_{mn} = 0\} \end{aligned} . \tag{2.23}$$

Cu $x_{m,n}$ s-au notat valorile luminanţei, iar m şi n indică poziţia pixelului. Marcajul este adăugat la imagine, prin incrementarea subsetului A cu un termen *k* pozitiv, de exemplu $A' = \{x_{mn} + k, x_{mn} \in A\}$. Imaginea marcată este dată de unificarea celor două subseturi, A' şi B. De fapt, se adună un zgomot de frecvenţă înaltă la imaginea originală. Pentru a verifica prezenţa marcajului, este folosită testarea ipotezelor. Statistica test q este definită ca fiind diferenţa normalizată dintre media $\bar{a}'$ a setului A' şi media $\bar{b}$ a setului B:

$$q = \frac{\bar{b} - \bar{a}'}{\sqrt{\sigma_{A'}^2 + \sigma_B^2}}. \qquad (2.24)$$

unde $\sigma_{A'}^2$ şi σ_B^2 sunt variantele setului A' respectiv B. Rezultatul este comparat cu un prag pentru a determina existenţa marcajului. Metoda este imună la subeşantionare urmată de supraeşantionare şi rezistă la compresia JPEG până la o compresie de 1:4.

O variantă îmbunătăţită a acestei tehnici este propusă de Langelaar ş.a. [LLL97]. Imaginea este împărţită în pătrate cu mărimea multiplu de 8. Un singur bit este înserat prin modificarea iterativă a unui bloc selectat pseudoaleator. Fiecare bloc selectat are asignat un model pseudoaleator P, cu distribuţie uniformă de 1 şi 0. Pentru a însera un bit de valoare 1, modelul scalat $k \times P$ este adunat la bloc, unde k este un factor predefinit. Pentru un bit 0, modelul scalat este scăzut din bloc. Fie I_0 media tuturor valorilor pixelilor din bloc pentru care valoarea modelului corespunzator este zero, şi I_1 media celorlalti pixeli. Fie diferenţa între cele două medii, $D_{high} = I_1 - I_0$, iar $D_{low} = \hat{I}_1 - \hat{I}_0$ diferenţa dintre medii, după compresia JPEG cu un factor predefinit Q. Dacă este înserat un 0 (sau 1), modelul P este scăzut iterativ din bloc, până când ambele diferenţe sunt mai mici (sau mai mari) decât un prag predefinit T, sau este atins numărul maxim de iteraţii. Bitul poate fi extras prin calcularea diferenţei D_{high} dintre cele două medii, I_1 şi I_0. Semnul diferenţei este folosit pentru a determina valoarea bitului. Testele efectuate au folosit ca parametri: mărimea blocului 32x32, pragul T=1, factorul de scalare iniţial k=4, şi numărul maxim de iteraţii 6, indicând că metoda este destul de robustă la compresie JPEG, cu eroare de bit de aproximativ 5% pentru calitate JPEG 85%, şi respectiv BER=20% pentru calitate JPEG 60%.

În a doua metodă, autorii propun o metodă bazată pe transformata DCT. Coeficienţii DCT sunt ordonaţi prin scanare, iar cei de la capăt sunt puşi pe zero.

Pentru a creşte performanţa metodelor spaţiale bazate pe împărţirea imaginii în blocuri, Bruyndonckx ş.a. [BQM95] folosesc clasificarea pixelilor. Marcajul este generat modificând luminanţa în blocuri 8x8 ale imaginii, adunând câte un bit de informaţie la fiecare bloc. Codorul alege locaţia secretă a blocului care va fi modificat. Pixelii, din blocuri selectate pseudoaleator, sunt clasificaţi în zone (1 şi 2) cu valori omogene ale luminanţei. Clasificarea se bazează pe trei tipuri de contrast între zone: mare, progresiv şi cu zgomot. Fiecare zonă este şi ea împărţită în două categorii A şi B, bazată pe un model (*grid*) definit de codor. Fiecare pixel este apoi

clasificat într-una din cele patru combinaţii de categorii, 1/A, 1/B, 2/A şi 2/B. Un bit b este înserat prin modificarea mediei categoriei pentru a satisface condiţiile:

$$\begin{aligned} \text{dacă } b=0: \quad & m^*_{1B} - m^*_{1A} = S \\ & m^*_{2B} - m^*_{2A} = S \\ \text{dacă } b=1: \quad & m^*_{1A} - m^*_{1B} = S \\ & m^*_{2A} - m^*_{2B} = S \end{aligned}$$

unde m^*_{1A}, m^*_{1B}, m^*_{2A} si m^*_{2B} sunt mediile categoriei modificate, iar S este intensitatea de marcare. Modificarea valorilor mediilor se face prin uniformizarea dispersiei luminanţei pentru toţi pixelii din aceeaşi zonă. Pentru creşterea robusteţii, autorii folosesc înserarea redundantă a biţilor de marcaj şi coduri corectoare de erori. Autorii raportează o robusteţe bună la compresia JPEG.

În [Hir96] se propune o metodă pentru autentificare şi stabilirea dreptului de copyright. Se construieşte un graf derivat din imagine, care conţine semnătura digitală şi un graf izomorf. Ambele grafuri sunt ascunse în imagine, în planul LSB. Pentru stabilirea izomorfismului grafului la receptor se aplică algoritmul ZKIP (Zero Knowledge Interactive Proof) pentru a afirma dreptul de copyright asupra imaginii. In consecinţă, informaţia secretă nu este dezvăluită în timpul autentificării.

Pentru a creşte performanţa marcării transparente bazată pe comunicaţiile SS, în domeniul spaţial, Kutter ş.a. [KJB97, KJB98] propun o metodă care înserează marcajul exclusiv în canalul pentru culoarea albastră (Blue din RGB), pentru maximizarea intensităţii marcajului, păstrând imperceptibilitatea. Ei propun şi preprocesarea imaginii înainte de detectarea marcajului. Această operaţie îmbunătăţeşte semnificativ robusteţea şi este aplicabilă oricărei tehnici de tip SS în domeniul spaţial. Marcajul este înserat sub forma unui număr binar, printr-o modulaţie de amplitudine în domeniul spaţial. Într-o poziţie (i,j) aleasă aleatoriu, este înserat un singur bit b ; în funcţie de valoarea bitului, se adună sau se scade o cantitate proporţională cu luminanţa din acea locaţie:

$$B_{i,j} \leftarrow B_{i,j} + \alpha(-1)^b L_{i,j} \tag{2.25}$$

unde $B_{i,j}$ este valoarea din poziţia (i,j) a canalului albastru, $L_{i,j}$, luminanţa din acea locaţie, iar α, intensitatea de marcare. Pentru a recupera bitul de marcaj, se calculează un estimat al valorii imaginii nemarcate, folosind o combinaţie liniară a pixelilor adiacenţi, în formă de cruce:

$$\hat{B}_{i,j} = \frac{1}{4c}\left(\sum_{k=-c}^{c} B_{i+k,j} + \sum_{k=-c}^{c} B_{i,j+k} - 2B_{j,k} \right) \tag{2.26}$$

unde c este mărimea ferestrei în formă de cruce. Valoarea bitului este dată de semnul diferenţei $\delta_{i,j}$ dintre pixelul posibil marcat şi cel estimat original. Pentru a

creşte robusteţea, fiecare bit este înserat de mai multe ori, iar la extragere, se foloseşte o logică majoritară. Având cheile potrivite, ambele marcaje originale pot fi recuperate. Extensiile acestei metode au îmbunătăţit robusteţea şi chiar recuperarea marcajului după atacuri geometrice [Kut98] sau atacurile de tip print şi scan.

Macq ş.a. [MQ95] au introdus marcarea transparentă adaptivă funcţie de HVS, folosind mascarea şi modularea. Marcajul, o structură binară, este filtrat trece-jos, modulat în frecvenţă, mascat şi apoi adunat la imaginea gazdă. Este folosită o cheie secretă pentru a determina frecvenţele de modulaţie şi localizarea marcajului. Pentru mascare, este folosit rastrul (grating) o extensie a fenomenului de mascare pentru semnale monocromatice. Pentru a adapta şi mai bine marcajul la imagine, este folosită o masca perceptuala, bazată pe zone morfologice omogene de frecvenţă înaltă. Recuperarea marcajului se face prin demodulare, urmată de o corelaţie.

P. Wong [WPW98] descrie o tehnică de marcare fragilă, care obţine un rezumat al imaginii utilizând o funcţie *hash*. Imaginea, dimensiunile ei şi cheia de marcare sunt modificate de funcţia *hash* în timpul inserţiei şi sunt folosite pentru a schimba bitul LSB al imaginii originale. Astfel că, atunci când informaţia suplimentară corectă şi imaginea marcată nealterată sunt furnizate detectorului, se obţine o imagine binară aleasă de proprietar (de exemplu un *logo* al unei companii). Metoda are proprietăţi de localizare şi poate identifica regiuni de pixeli modificaţi în imaginea marcată.

Tehnica lui Yeung şi Mintzer [YM97] este mai complicată, nu doar de înserare a unei valori binare în cel mai puţin semnificativ bit. Cheia de marcare este folosită pentru a genera secvenţe pseudo-aleatoare (una pentru fiecare canal sau componentă a culorii) care controlează modificările ulterioare ale pixelilor. După inserţie, este folosit un proces de difuzie a erorilor pentru răspândirea efectelor pixelilor alteraţi, făcând ca marcajul să fie mai greu de văzut

Metodele recente [STHW04] aplică marcajul în planul LSB, şi în alte planuri, sau într-o combinaţie a acestora. Cantitatea de date înserată poate fi fixă sau variabilă, depinzând de numărul de pixeli selectaţi, de luminanţă şi de contrast.

Într-o manieră diferită, Voyatzis şi Pitas [VP96a, VP96b] marchează imaginile prin înserarea unui logo, folosind automorfisme toroidale. Un automorfism toroidal poate fi considerat ca o trasformare spaţială a regiunilor plane care aparţin unei arii pătratice 2D, fiind definit în subsetul $U = [0,1) \times [0,1) \in R^2$ prin:

$$\boldsymbol{r}' = \mathbf{A}\boldsymbol{r}, \quad \begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod 1. \tag{2.27}$$

Acţiunile iterative ale lui $\mathbf{A}$ asupra unui punct $\mathbf{r}_0$ formează un sistem dinamic, care poate fi exprimat ca o hartă (map):

$$\mathbf{r}_{n+1} = \mathbf{A}^n \mathbf{r}_0 \pmod 1 \quad \text{sau} \quad \mathbf{r}_{n+1} = \mathbf{A}\mathbf{r}_n \tag{2.28}$$

Un exemplu de automorfism în dinamică este "cat map", definit ca:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod 1.$$

Setul de puncte $\{\mathbf{r}_0, \mathbf{r}_1, \mathbf{r}_2, ...\}$ este numit orbita sistemului. Un astfel de sistem "amestecă" sau mixează haotic punctele. În anumite circumstanţe, automorfismul poate avea orbite periodice, adică după T iteraţii punctul curent este acelaşi cu cel initial, $\mathbf{A}^T\mathbf{r}_0 = \mathbf{r}_0$.

Pentru marcarea unei imagini, un marcaj pătratic, sub forma unei imagini binare mai mică decât imaginea gazdă, este mai întâi mixat cu automorfismul $\mathbf{A}_N$. Marcajul mixat este suprapus peste un bloc selectat din imaginea originală, folosind o funcţie de înserare, ca modificarea LSB. Recuperarea marcajului se face prin extragerea marcajului mixat din imaginea semnată, urmată apoi de reconstrucţia marcajului folosind automorfismul $\mathbf{A}_{N-T}$, unde T este perioda automorfismului în sistemul dat. Robusteţea poate creşte prin proceduri sofisticate de suprapunere/înserare.

Înserarea marcajului nu este bazată numai pe principiul modulării SS. Chen si Wornell [CW01a,b] au propus cuantizarea. Metoda lor numita QIM (Quantized Index Modulation), modulaţia prin cuantizare indexată foloseşte un set de cuantizoare N-dimensionale, care satisfac o condiţie de distorsiune. Sunt construite astfel încât valorile de reconstrucţie dintr-un cuantizor să fie „depărtate" de punctele de reconstrucţie ale altui cuantizor. Mesajul de transmis este folosit ca index pentru selectarea cuantizoarelor. Cuantizorul selectat este folosit apoi pentru înserarea informaţiei, prin cuantizarea pixelilor în domeniul spaţial sau DCT. La decodare este folosită o metrică de evaluare a tuturor cuantizoarelor, iar indexul cuantizorului cu distanţa minimă identifică informaţia înserată. Autorii arată că performanţa schemei propuse este superioară celei standard cu modulaţie SS.

Pe lângă tehnicile care folosesc modulaţia din domeniul spaţial, Maes ş.a. [MO98] propun modificarea proprietăţilor geometrice ale imaginii. Metoda se bazează pe un model de linii dense generat pseudoaleator, care reprezintă marcajul. Se calculează un set de puncte reprezentative, cu un filtru detector de muchii. Punctele detectate sunt apoi deviate, astfel ca multe puncte să fie în vecinătatea liniilor. La detecţie, se verifică dacă un număr semnificativ de puncte sunt în vecinătatea liniilor din model.

In [CB01], marcajul se înserează cu ajutorul a două chei. Prima codează bitul într-un bloc de pixeli, iar a doua generează secvenţa de marcaj. Înserarea marcajului se face prin adunarea sau scăderea modelului pseudo-aleator în domeniul spaţial; intensitatea de înserare este dată de distribuţia densităţii spectrale a coeficienţilor DCT şi tabela de cuantizare JPEG, pentru a creşte robusteţea la compresia JPEG. Modelul este un şir de biţi înseraţi într-un set pătratic de blocuri şi repetat pe toată imaginea. La detecţie, se verifică marcajul cu operaţia XOR. Metoda este rezistentă la filtrare, decupare, zgomot aditiv (marcaj detectat cu BER 3.17% respectiv BER 22.2% pentru 15% respectiv 20% zgomot uniform) şi alte atacuri.

2.2.2 Algoritmi în domeniul unei transformate

Au fost propuse multe tehnici care se folosesc o transformată. Pentru înserarea marcajului, este aplicată semnalului gazdă o transformare şi apoi sunt modificaţi coeficienţii transformatei. Transformatele au fost studiate mai ales în contextul codării şi compresiei imaginii, dar multe rezultate sunt aplicabile şi pentru marcarea transparentă. În cele mai multe imagini culorile pixelilor adiacenţi sunt

corelate. Trecerea imaginii într-un domeniu al unei transformate, ca DCT sau DWT, ar trebui să decoreleze eşantioanele originale şi să concentreze energia semnalului original în câţiva coeficienţi. O imagine codată în frecvenţă are energia concentrată în coeficienţii cu index mic, deci conţine mai ales componente de joasă frecvenţă. Ele reprezintă forma şi caracteristicile globale ale imaginii, luminanţa şi contrastul. Frecvenţele înalte reprezintă muchiile imaginii, dar contribuie puţin la energia din domeniul spaţial-spectral. O imagine ar putea conţine 95% din energia sa în 5% din frecvenţele cele mai joase ale transformatei DCT bidimensionale. Obiectivul creării unei tabele de cuantizare adecvate pentru compresia JPEG este reţinerea acestor coeficienţi DCT, şi componente de frecvenţă înaltă suficiente pentru a avea destule muchii, ca să fie acceptabilă vizual.

Metodele din [RDB96], [RDB96b], [BP96a], [BP96b], [NP96], [PI96], [BRD95], [CKLS95], [CKLS96], [HG96] sunt primele în domeniu şi reprezintă un cadru de cercetare fundamental pentru marcare. In [FKK01], [FKK04] se determină domeniul în care este maximizată capacitatea marcajului. Autorii se concentrează asupra compresiei cu pierderi, care implică cuantizarea într-un anume domeniu. Folosind o cuantizare liniară, se estimează capacitatea de marcare pentru diferite domenii. Se precizează cele mai adecvate transformate pentru marcare la compresia JPEG. Autorii constată că un cod de repetiţie şi marcarea într-alt domeniu decât al compresiei cresc capacitatea de marcare.

2.2.2.a Metode bazate pe transformata DCT

Există o multitudine de metode care folosesc transformata DCT a întregii imagini, sau pe blocuri de 8x8. Dintre cele mai cunoscute sunt metodele propuse de Cox ş.a. [CKLS95], [CKLS96] şi Koch şi Zhao [KZ95].

Matsui si Tanaka [MT94] propun o metodă bazată pe modificarea coeficienţilor DCT, într-o schemă de transmisie progresivă. Biţii de marcaj sunt înseraţi modificând regula de rotunjire a coeficienţilor cuantizaţi, astfel încât coeficienţii rezultati, să fie pari sau impari, în funcţie de biţii marcajului.

Marcarea eficientă în domeniul DCT a fost introdusă de Koch ş.a. [KZ95, BKZ98]. Imaginea este împărţită în blocuri 8x8, ca la compresia JPEG şi apoi se calculează transformata DCT a fiecărui bloc. Dintr-un un bloc selectat pseudoaleator, se alege o pereche de coeficienţi de frecvenţă medie, din 12 perechi predeterminate. Pentru înserarea unui bit, coeficienţii sunt astfel modificaţi (cuantizaţi) încât diferenţa lor să fie ori pozitivă ori negativă, funcţie de valoarea bitului. Pentru a fi rezistentă la compresia JPEG, este luată în considerare matricea de cuantizare JPEG, când se alterează coeficienţii DCT. Metoda are o robusteţe bună la compresii JPEG cu un factor de calitate de până la 50%.

De fapt se modifică diferenţa dintre coeficienţii de frecvenţă medie, selectaţi aleator în blocuri DCT ale imaginii originale, alese tot aleator. Se foloseşte ca marcaj o secvenţă binară, $w \in \{0,1\}$. Din fiecare bloc b_i, sunt selectaţi doi coeficienţi de frecvenţă medie $f_b(m_1,n_1)$ şi $f_b(m_2,n_2)$; apoi fiecare bloc este cuantizat cu un factor de cuantizare Q, conform matricii de cuantizare JPEG. Diferenţa absolută dintre coeficienţii selectaţi este:

$$\Delta_b = \left| f_b(m_1,n_1) \right| - \left| f_b(m_2,n_2) \right|. \qquad (2.29)$$

Un bit de informaţie w_i este înserat într-un bloc b_i, modificând perechea $f_b(m_1,n_1)$ şi $f_b(m_2,n_2)$, astfel încât distanţa dintre cei doi să devină:

$$\Delta_b = \begin{cases} \geq q, & \text{daca } w_i = 1 \\ \leq -q, & \text{daca } w_i = 0 \end{cases}. \tag{2.30}$$

unde q este un parametru ce controlează intensitatea de marcare. Algoritmul nu este foarte robust, din cauză că doi coeficienţi per bloc sunt marcaţi. Algoritmul nu este robust nici la scalare, decupare, fiindcă dimensiunile imaginii sunt folosite pentru a genera o secvenţă de marcaj adecvată. Efectele introduse sunt vizibile, din cauză că marcajul este înserat în domeniul DCT 8x8. Ele pot fi văzute mai uşor în zonele omogene, nu în contururi. Se schimbă coeficienţii de frecvenţă medie, din blocurile cu nivele de cuantizare identice, cu tabela de cuantizare JPEG color; astfel un coeficient $B(u_1,v_1)$ va fi mai mare decât celălalt $B(u_2,v_2)$, dacă bitul este "1", şi mai mic dacă bitul este "0". O altă posibilitate este schimbarea uşoară a unor tripleţi de coeficienţi de frecvenţă medie.

Bors şi Pitas [BP96a, BP96b, BP98] propun modificarea coeficienţilor DCT care satisfac o condiţie de selecţie a poziţiei blocului. Imaginea este împărţită în blocuri 8x8, selectate cu un clasificator gaussian cu reţele. Coeficienţii DCT de frecvenţă medie sunt modificaţi folosind o constrângere DCT liniară sau o regiune DCT de detecţie circulara, pentru a ascunde informaţia de marcaj. În prima abordare, constrângerea liniară este dată de:

$$Y = \mathbf{FQ}. \tag{2.31}$$

unde $\mathbf{F}$ este vectorul de coeficienţi DCT modificat, iar $\mathbf{Q}$ este vectorul ponderilor format de către marcaj. Constrângerea este impusă prin schimbarea coeficienţilor DCT bazată pe criteriul minimizării pătratelor. Al doilea algoritm defineşte regiunile circulare din jurul coeficienţilor DCT selectaţi, coeficienţii care sunt apoi cuantizaţi:

$$\left\|\mathbf{F}-\mathbf{Q}_k\right\|^2 = \min_{i=1}^{H} \left\|\mathbf{F}-\mathbf{Q}_i\right\|^2 \quad \text{atunci} \quad \mathbf{F} = \mathbf{Q}_k \tag{2.32}$$

unde $\mathbf{Q}_i, i = 1,...,H$ este setul vectorilor cu coeficienţi formaţi din marcaj. În recuperarea marcajului, algoritmul verifică mai întâi constrângerea asupra coeficienţilor DCT din toate blocurile, urmată de constrângerea asupra localizării. Algoritmul rezistă la compresia JPEG pentru o rată de compresie de 13:1, respectiv 18:1, folosind constrângerea DCT liniară sau regiunea de detecţie circulară DCT.

Swanson ş.a. [SZT96] propun o metodă de marcare în domeniul DCT, bazată pe mascarea spectrală a blocurilor DCT, similară cu cea propusă de Smith şi Comiskey [SC96]. Imaginea gazdă este împărţită în blocuri pătratice, şi se calculează trasformata DCT pentru fiecare. Pentru fiecare bloc DCT, este calculată o mască spectrală, ştiind că mascarea de tip grilă creşte pragul vizual în jurul frecvenţei de mascare pentru aceste semnale de tip grilaj. Masca perceptuală rezultantă este adăugată la blocul DCT, prin scalare şi înmulţire cu o secvenţă PN de lungime maximă. Procesul de înserare prevede şi post-procesarea de mascare spaţială pentru a face marcajul invizibil şi pentru a controla factorul de scalare. Detecţia necesită imaginea originală şi marcajul original; ea se face prin testarea ipotezelor. Autorii raportează o robusteţe bună la compresia JPEG, zgomot colorat şi decupare.

Tao şi Dickinson [TD97] introduc o tehnică adaptivă de marcare, în domeniul DCT, bazată pe un clasificator perceptual regional, cu indecşi de sensibilitate. Marcajul este înserat în N coeficienţi DCT, tip AC. Aceştia sunt selectaţi să aibă paşii de cuantizare cei mai mici, conform tabelei de cuantizare JPEG. Coeficienţii x_i selectaţi sunt modificaţi după cum urmează:

$$\hat{x}_i = x_i + \max\left[x_i \alpha_m, \operatorname{sign}(x_i) \frac{D_i}{k} \right]. \qquad (2.33)$$

unde α_m defineşte indexul sensibilităţii la zgomot pentru blocul curent, D_i este pasul de cuantizare pentru X_i, iar k satisface conditia $5 \le k \le 6$. Aici, marcajul nu este generat aleator. Există mai multe căi de determinare a sensibilităţii la zgomot, folosind mascarea HVS. Algoritmul foloseşte efectele de mascare a luminanţei, a muchiilor, precum şi a texturilor. Autorii propun un algoritm de clasificare în regiuni, care clasifică blocurile în şase clase perceptuale: muchie, sensibilitate uniformă joasă, moderat ocupată, ocupată, foarte ocupată, în ordinea descrescătoare a sensibilităţii la zgomot. Fiecare clasă perceptuală are asociat un index de sensibilitate la zgomot. Recuperarea marcajului se face cu ajutorul imaginii originale, a marcajului şi a testării ipotezelor. Metoda este robustă la compresia JPEG până la un factor de calitate de 5% şi zgomot aleator cu raportul semnal-pe-zgomot maxim PSNR de 22.1 dB.

Podilchuk [PZ98] propune marcarea perceptuală, folosind diferenţa abia sesizabilă JND (Just Noticeable Difference), pentru a determina masca de modulare a marcajului, dependentă de imagine. Modularea marcajului cu coeficienţii selectaţi se face în domeniul DCT sau wavelet:

$$I^*_{u,v} = \begin{cases} I_{u,v} + JND_{u,v} \times w_{u,v}, & \text{dacă } I_{u,v} > JND_{u,v} \\ I_{u,v}, & \text{altfel} \end{cases}. \qquad (2.34)$$

unde $I_{u,v}$ sunt coeficienţii transformatei imaginii originale, $w_{u,v}$ sunt biţii marcajului, iar $JND_{u,v}$ sunt valorile JND calculate cu modele vizuale. Pentru transformata DCT, autorii folosesc modelul perceptual al lui Watson, care foloseşte sensibilitatea în frecvenţă şi luminozitate, precum şi mascarea de contrast locală. Acest model calculează pragurile de mascare dependente de imagine, pentru fiecare bloc în parte. Detecţia se face prin corelaţia dintre diferenţa imaginii originale şi marcate şi secvenţa de marcaj. Corelaţia maximă este comparată cu un prag, pentru a determina existenţa marcajului. Metoda este foarte robustă la compresia JPEG, decupare, scalare, zgomot aditiv, corecţia de gamă şi atacuri de tip imprimare-copiere-scanare. Pentru atacuri care implică transformări geometrice, înainte de detecţie trebuie aplicate operaţiile inverse.

In [PBBC97] şi [BBCP98a] se descrie o metodă bazată pe trasformata DCT, care foloseşte caracteristicile HVS. Marcajul este o secvenţă pseudoaleatoare de M numere reale, cu distribuţie normală $\mathbf{X} = \{x_1, x_2, ..., x_M\}$. Coeficienţii transformatei DCT, a imaginii originale de dimensiune NxN, sunt reordonaţi într-un vector, prin

scanare în zig-zag (la fel ca la JPEG). Din vector, se aleg coeficienţii cu indexul (L+1) până la (L+M), M fiind lungimea aleasă a marcajului (16000 aici) şi L poziţia de unde începe înserarea, pentru a genera vectorul $\mathbf{T} = \{t_{L+1}, t_{L+2}, ..., t_{L+M}\}$. Detecţia se face fără imaginea originală. Pentru reducerea probabilităţii de eroare, înserarea se face folosind valoarea absolută a coeficienţilor:

$$t'_{L+i} = t_{L+i} + \alpha |t_{L+i}| x_i \tag{2.35}$$

unde α este intensitatea de înserare. Coeficienţii modificaţi înlocuiesc pe cei originali înainte de reconstrucţia imaginii marcate I'.

Deşi formula de înserare a marcajului este construită să ţină cont de HVS, marcajul este vizibil în unele regiuni ale imaginii. De aceea, după înserare, sunt folosite caracteristicile de mascare spaţială ale HVS; imaginea originală I şi cea marcată I' sunt adunate pixel cu pixel, conform unui factor local adaptiv $\beta_{i,j}$, rezultând o nouă imagine marcată I'':

$$y''_{i,j} = y_{i,j}\left(1 - \beta_{i,j}\right) + \beta_{i,j} y'_{i,j}. \tag{2.36}$$

Parametrul $\beta_{i,j}$ este dispersia, calculată pe un bloc 9x9, centrat pe pixelul $y_{i,j}$, şi normalizată la maximul dispersiilor tuturor blocurilor.

Detecţia se face astfel neinformat, folosind corelaţia dintre marcajul original şi coeficienţii posibil marcaţi:

$$z = \frac{\mathbf{Y} \cdot \mathbf{T}^*}{M} = \frac{1}{M} \sum_{i=1}^{M} y_i t^*_{L+i} \tag{2.37}$$

Pragul de decizie este estimat, cu metode statistice, folosind imaginea recepţionată:

$$T'_z = \frac{\alpha}{3M} \sum_{i=1}^{M} |t_i^*| \tag{2.38}$$

Rezultatele experimentale sunt foarte bune, metoda fiind robustă la mai multe tipuri de atacuri, compresie JPEG, filtrare mediană, marcare multiplă, dar şi distorsiuni geometrice (după aplicarea transformării geometrice inverse).

Tehnicile de marcare în domeniul spectral au fost introduse prima oară de Boland ş.a. [BRD95] şi Cox ş.a. [CKLS95], care au dezvoltat independent metode perceptuale adaptive bazate pe modulare. Cox ş.a. propun o metodă bazată pe SS [CKLS95]. Autorii susţin că marcajul trebuie plasat în componentele perceptuale cele mai semnificative, rezistente la compresie şi la prelucrările obişnuite. Marcajul este o secvenţă $X = x_1, ..., x_n$ de 1000 de numere reale aleatoare, alese dintr-o distribuţie gaussiană $\mathcal{N}(0,1)$, care creşte invizibilitatea şi robusteţea. Marcajul X este înserat în imaginea V pentru a produce secvenţa de coeficienţi V' modificaţi.

Când se înserează X în V, pentru a obţine V', se specifică un parametru de scalare α , care determină măsura în care X modifică pe V. Pentru calcularea lui V' se poate folosi una din cele trei formule:

$$v_i' = v_i + \alpha x_i . \tag{2.39}$$

$$v_i' = v_i \left(1 + \alpha x_i\right). \tag{2.40}$$

$$v_i' = v_i e^{\alpha x_i} . \tag{2.41}$$

unde x_i este bitul de marcaj, α este intensitatea de marcare, iar v_i sunt coeficientii perceptual semnificativi. Fiind dat V^*, se poate calcula funcţia inversă pentru a obţine X^* din V^* şi V. Ecuaţia (2.39) este totdeauna inversabilă, iar ecuaţiile (2.40) şi (2.41) sunt inversabile dacă $v_i \neq 0$.

Ecuaţia (2.39) nu e potrivită dacă valorile lui v_i variază mult. Dacă $v_i = 10^6$, adăugând 100 s-ar putea să fie insuficient pentru recuperarea marcajului, dar dacă $v_i = 10$ adăugând 100 va distorsiona această valoare într-o măsură inacceptabilă. Inserţia bazată pe ecuaţia (2.40) sau (2.41) este mai rezistentă împotriva acestor variaţii mari. Este de menţionat că (2.40) şi (2.41) dau rezultate similare dacă αx_i este mic. De asemenea dacă v_i este pozitiv, atunci (2.41) este echivalent cu $\log(v_i') = \log(v_I) + \alpha x_I$, şi poate fi privit ca o aplicaţie a lui (2.39) pentru cazul în care sunt folosiţi logaritmii valorilor originale.

Autorii [CKLS97] sugerează că nu este suficient un singur parametru de scalare α, pentru perturbarea tuturor valorilor lui v_i, deoarece diferitele componente spectrale ar putea avea toleranţa la modificări diferită. În relaţia $v_i' = v_i (1+\alpha_i x_i)$, se pot folosi parametri de scalare multipli $\alpha_1, \alpha_2, \ldots \alpha_n$. Un α_i mare înseamnă că v_i se modifică cu un factor mare, fără să se modifice calitatea perceptuală a documentului. Parametrul α_i poate fi privit ca măsura relativă a modificării lui v_i.

Detecţia se face pe baza similarităţii dintre marcajul original X şi marcajul X^* extras din imaginea marcată şi atacată:

$$\mathrm{sim}\left(X, X^*\right) = \frac{X^* \cdot X}{\sqrt{X^* \cdot X^*}} . \tag{2.42}$$

Algoritmul este robust la manipulări de tip compresie JPEG (calitate 5%), dithering, transmisie fax, imprimare-copiere-scanare, marcare multiplă, atacul de coliziune. În experimente, marcajul a avut o lungime de 1000 de numere cu distribuţia N(0,1), α = 0.1, iar coeficienţii selectaţi sunt cei maximi, cu excepţia componentei continue. Robusteţea se datorează selecţiei coeficienţilor importanţi din punct de vedere perceptual. Algoritmul nu este robust la atacul de inversiune propus de Craver ş.a. [CMYY97], iar efectuarea transformatei DCT pe toată imaginea face ca algoritmul să fie lent. Boland ş.a. propun o tehnică similară bazată pe modulaţia de amplitudine şi modulaţia de frecvenţă de tip FSK (Frequency Shift Keying); ei sugerează folosirea unor transformate cum ar fi: DCT, wavelet, Walsh-Hadamard, şi transformata Fourier rapidă, FFT.

Cuantizarea pară-impară este o tehnică simplă care înserează un bit "0" sau "1" folosind operatorii de cuantizare pară sau impară [WL02a], [WL02b]. Marcarea diferenţiată alterează energia a două grupuri de blocuri DCT, A şi B, încât $E_A < E_B$ dacă bitul de marcaj este "1". Înainte de a schimba energia acestor blocuri, blocurile DCT sunt schimbate aleator astfel încât aceste perechi de blocuri A-B să fie selectate tot aleator în imagine, crescând astfel securitatea metodei de marcare [LL01].

In [BTS05] se consideră mai adecvată modelarea coeficientilor DCT cu "cozi lungi" (familia alpha-stable), decât funcţiile exponenţiale precum modelul gaussian generalizat [HPGA98]. Pentru detecţia oarbă, se foloseşte distribuţia Cauchy din familia alfa-stabilă. Distribuţia este singura cu formă compactă, din familia alfa-stabilă simetrică negaussiană, şi conduce la un detector aproape optimal.

2.2.2.b Metode bazate pe transformata DFT

Ruanaidh ş.a. [RDB96, RDB96b] propun marcarea folosind faza DFT. Pentru a însera un bit, este modificată faza unui coeficient selectat $F(k_1,k_2)$ prin adunarea unei valori mici δ :

$$\angle F(k_1,k_2) \leftarrow F(k_1,k_2)+\delta \tag{2.43}$$

Pentru ca imaginea marcată să fie reală, faza trebuie să satisfacă simetria impară, ceea ce conduce la o modificare suplimentară:

$$\angle F(N_1-k_1,N_2-k_2) \leftarrow \angle F(N_1-k_1,N_2-k_2)+\delta \tag{2.44}$$

unde $0 \le k_1 < N_1$ şi $0 \le k_2 < N_2$. Coeficienţii sunt modificaţi numai dacă puterea lor relativă este mai mare decât un prag dat. Dacă imaginea originală este cunoscută, marcajul poate fi recuperat cu uşurinţă comparând faza. Atunci când aceasta nu este cunoscută la detector, Ruanaidh sugerează folosirea cuantizării fazei originale înainte de modificarea ei. Deviaţiile dintre stările cuantizate sunt apoi folosite pentru a ascunde marcajul.

2.2.2.c Metode bazate pe transformata Fourier-Mellin

Ruanaidh ş.a. [HPRP98] propun o metodă care plasează marcajul într-un domeniu invariant la rotire, scalare şi translaţie, folosind o combinaţie dintre transformata Fourier discretă, DFT, şi reprezentarea polară logaritmică, LPM (log polar map). Figura 2.16 prezintă o schemă a acestei metode de marcare transparentă.

În primul pas, este calculată transformata DFT a imaginii originale. Una din proprietăţile transformatei DFT este că o translaţie în domeniul spaţial este echivalentă cu o deplasare de fază în domeniul DFT. Astfel, dacă se păstrează numai amplitudinea coeficienţilor DFT, se obţine un domeniu invariant la translaţii. În pasul următor, pentru fiecare coordonată carteziană (u,v) a amplitudinilor DFT este determinat un punct corespunzător (μ,θ) în LPM:

$$u = e^{\mu}\cos(\theta) \qquad v = e^{\mu}\sin(\theta) \tag{2.45}$$

unde $\mu \in R$ şi $0 < \theta 2\pi$.

Sistemul de coordonate polar logaritmic transformă rotirea şi scalarea din domeniul cartezian, în translaţii de-a lungul axei orizontale şi verticale. În continuare, prin folosirea amplitudinii DFT a coordonatelor LPM, se obţine un domeniu invariant la rotire, scalare şi translaţie. Transformata Fourier pentru LPM este echivalentă cu transformarea Fourier-Mellin. Combinând cei doi paşi se obţine o

transformare invariantă la rotire, scalare şi translaţie. Marcajul ia forma unui semnal SS bidimensional. În teste, marcajul are 104 biţi, imaginea marcată este rotită cu 143^0 şi scalată la 75% pe fiecare axă. Marcajul este recuperat cu succes din imaginea astfel atacată. Metoda este rezistentă la compresie JPEG până la calitatea de 75% şi decupare la 50% din imaginea originală. Această metodă a fost prima construită special pentru a rezista atacurilor RST.

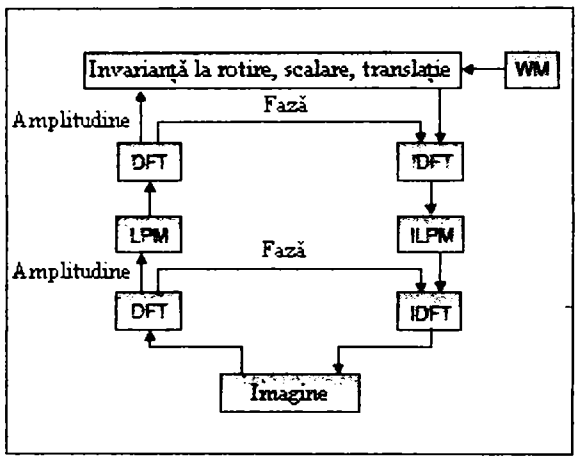


Fig. 2.16: Schemă de marcaj transparent invariantă la rotire, scalare, şi translaţie

În Figura 2.17 se pot vedea proprietăţile LPM. Partea (b) arată LPM al imaginii Lena (a). Partea (c) ne arată o versiune rotită şi scalată a imaginii Lena, şi (d) ne arată LPM corespunzătoare lui (c). Se poate vedea clar că rotirea şi scalarea în domeniul spaţial, original sunt convertite în translaţii în domeniul LPM.

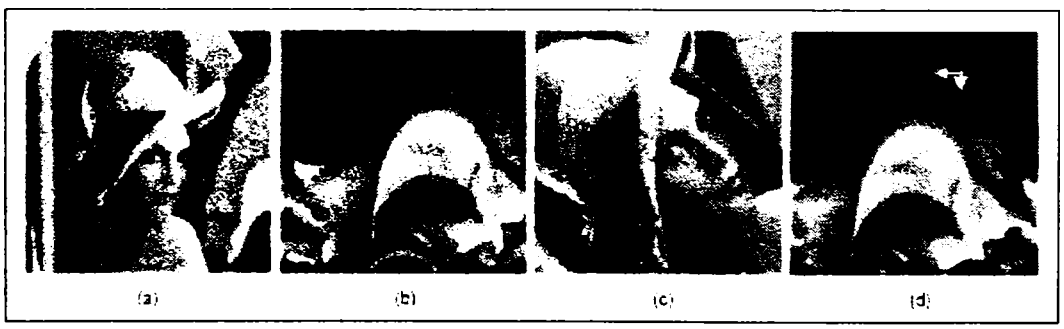


Fig. 2.17: Exemplu al proprietăţilor LPM. (a) Imaginea originală, (b) LPM lui (a), (c) Scalat şi rotit, şi (d) LPM lui (c)

Implementarea practică a schemei anterioare s-a dovedit a fi dificilă. De aceea autorii au propus o abordare diferită, unde un marcaj transparent CDMA este plasat în domeniul amplitudinii DFT invariante la translaţii. Pentru a face marcajul transparent invariant la scalare şi rotire, se plasează un al doilea marcaj transparent ca şablon, în acest domeniu [HRPP98], [RPHP99]. Pentru a extrage marcajul transparent, mai întâi se determină scara şi orientarea imaginii marcate, folosind şablonul, astfel:

-se calculează transformata DFT a imaginii marcate,

- se calculează coordonatele LPM ale amplitudinilor coeficienţilor DFT şi ale modelului şablonului
- se calculează diferenţele (offset) orizontale şi verticale dintre cele două LPM, cu tehnici de căutare şi intercorelaţie, rezultând un factor de scalare şi rotire.

În final, imaginea este transformată înapoi la mărimea şi orientarea originală, şi este extras marcajul purtător de informaţie. O variantă a acestei metode a fost propusă de Lin ş.a. [LWBC01], folosind transformata Radon.

2.2.2.d Metode bazate pe domeniul wavelet

Boland ş.a. [BRD95] au propus prima dată înserarea marcajului folosind o descompunere multirezoluţie. Marcajul este un model pseudoaleator bidimensional. Imaginea şi marcajul sunt descompuse folosind transformata wavelet discretă 2D, şi marcajul este adăugat în fiecare subbandă a imaginii prin ponderare. Decodarea se face prin corelaţie normalizată între estimarea marcajului şi marcajul original. Au fost propuse mai multe scheme folosind transformata wavelet [IMK99, Kun99, XBA97, ZXZ98], diferenţa fiind modul de ponderare pentru a diminua efectele vizibile. Majoritatea înserează marcajul în subbenzi de detaliu, cu mici excepţii [JSSK02].

O tehnica perceptuală [WQF98] înserează marcajul astfel încât zgomotul să nu depăşească diferenţa abia sesizabilă, JND, pentru fiecare coeficient. Ordinea de înserare este ca cea a semnificaţiei vizuale. Este garantată invizibilitatea şi robusteţea, dar nu şi securitatea, ceea ce este un dezavantaj major.

Zhu ş.a. [ZXZ98] implementează o tehnică de marcare în domeniul wavelet, cu 4 nivele de descompunere, folosind ca marcaj o secvenţă gaussiană de numere pseudo-aleatoare. Sunt marcate numai benzile de detaliu. Dacă W_j este secvenţa de marcaj w_j de la nivelul de rezoluţie j, este satisfăcută relaţia:

$$\ldots \subset W_3 \subset W_2 \subset W_1$$

Lungimea marcajului W_j pentru o imagine de marimea $M \times M$ este dată de:

$$N_j = 3\frac{M^2}{2^{2j}} \tag{2.46}$$

Acest algoritm poate fi uşor adaptat pentru tehnici de marcare video, bazat pe transformata wavelet 3D, datorat tocmai simplităţii. Natura ierarhică a dezvoltării wavelet permite detecţia multirezoluţie a marcajului, care este un vector gaussian aleator adunat la toţi coeficienţii din benzile de frecvenţă înaltă, în domeniul wavelet. S-a arătat că atunci când imaginea este comprimată, marcajul poate fi identificat corect la fiecare nivel de rezoluţie. Marcajul nu este sigur deoarece, când se cunoaşte algoritmul, poate fi extras statistic de atacatori.

Podilchuk [PZ98] propune marcarea perceptuală folosind diferenţa abia sesizabilă, JND, pentru a determina masca de modulare a marcajului, dependentă de imagine. Modularea marcajului cu coeficienţii selectaţi se face în domeniul DCT sau wavelet, aşa cum s-a văzut în ecuaţia (2.34). Sunt folosite filtre biortogonale 7/9. Modelul vizual pentru a determina factorii JND în domeniul wavelet este cel al lui Watson ş.a. [WYSV96]. Ei compară robusteţea marcajului înserat în domeniul DCT cu cel în domeniul DWT, respectiv cu algoritmul SS-DCT din [CKLS97]; ambele sunt mai bune decât metoda SS, iar marcajul din domeniul wavelet rezistă mai bine la compresie, decupare, scalare decât cel din domeniul DCT. Dar selecţia coeficienţilor în domeniul wavelet nu include părţile semnificativ vizuale şi deci

există posibilitatea ştergerii marcajului înserat în coeficienţii nesemnificativi. Filtrarea trece-jos va afecta marcajul înserat în coeficienţii de frecvenţă înaltă. Aici autorii propun un detector modificat, la care este calculată media corelaţiei pentru fiecare nivel:

$$\rho_{ww}.(l) = \frac{1}{N_f}\sum_{f=1}^{N_f}\rho_{ww}.(l,f) \qquad (2.47)$$

unde N_f este numărul de orientări, $N_f = 3$. Prin evaluarea corelaţiilor separat pe nivelul de rezoluţie, detectorul este mai robust la operaţii precum decuparea, care afectează componentele spectrale de frecvenţă înaltă, din cauza că marcajul are un suport spaţial mai mic în nivele de rezoluţie joasă (l = 1). De asemenea este mai robust la filtrarea trece-jos. Prin eliminarea nivelelor care au valori de corelaţie mici, detecţia devine mai robustă. De asemenea, se consideră corelaţia medie per orientare în frecvenţă:

$$\rho_{ww}.(f) = \frac{1}{N_l}\sum_{l=1}^{N_l}\rho_{ww}.(l,f), \qquad (2.48)$$

unde N_l este numărul de nivele, care aici este 4. Prin evaluarea corelaţiilor separat pe orientare, se profită de orice structură asociată cu imaginea originală, unde marcajul este mai puternic. Examinând corelaţiile separat per subbandă, se alege valoarea maximă per nivel şi per locaţiile în frecvenţă:

$$\rho_{ww}.(f) = \max_{l,f}\left\{\rho_{ww}.(l), \rho_{ww}.(f)\right\} \qquad (2.49)$$

ceea ce duce la o robusteţe crescută.

Dugad ş.a. [DRA98] folosesc ca marcaj o secvenţă gaussiană de numere reale pseudo-aleatoare. Marcajul este înserat în câţiva coeficienţi selectaţi. Transformata wavelet este pe 3 nivele de rezoluţie, cu filtre Daubechies-8. Algoritmul selectează coeficienţii din toate subbenzile de detaliu cu amplitudinea peste un prag dat T_1 şi îi modifică, folosind relaţia:

$$f'(m,n) = f(m,n) + \alpha\left|f(m,n)\right| w_i \qquad (2.50)$$

La partea de extragere, sunt luaţi în considerare numai coeficienţii peste un prag $T_1 > T_2$. Mascarea vizuală implicită, prin proprietăţile de localizare în timp-frecvenţă ale transformatei DWT. Din cauză că subbenzile de detaliu la care se adaugă marcajul conţin mai mult muchii, energia semnăturii este concentrată în jurul acestora. Aceasta face ca marcajul să fie invizibil, deoarece observatorii umani sunt mai puţin sensibili în zonele cu texturi şi muchii. Dar robusteţea algoritmului este redusă, fiindcă aceste locaţii sunt cel mai uşor de modificat prin compresie sau alte atacuri obişnuite.

Inoue ş.a. [IMK99], propun folosirea unei descompuneri multirezolutie cu filtre simetrice 5/3, sau Daubechies-16. Cu algoritmul EZW coeficienţii sunt clasificaţi ca semnificativi sau nu, folosind arborele-zero [LK92], [PK95], [STO94], [Sha93]. Coeficientul f(m,n) este nesemnificativ dacă $\left|f(m,n)\right| < T$, T fiind pragul. Dacă un coeficient şi toti descendenţii lui sunt nesemnificativi faţă de pragul T, atunci setul format din aceşti coeficienţi este numit arbore-zero pentru pragul T.

Se consideră două grupuri. Unul este cel al coeficienţilor semnificativi unde sunt aleşi toţi arborii zero, Z pentru pragul T. Acest grup nu consideră subbanda de aproximare LL. Toţi coeficienţii din arborele-zero Z_i sunt setaţi dupa cum urmează:

$$f'(m,n)=\begin{cases}-m & \text{dacă} \quad w_i=0\\ +m & \text{dacă} \quad w_i=1\end{cases} \tag{2.51}$$

Al doilea grup manipulează coeficienţii semnificativi de la nivelul cu rezoluţie joasă, adică subbenzile de detaliu LH_3, HL_3 şi HH_3. Selecţia coeficienţilor se face cu relaţia:

$$T_1<\left|f(m,n)\right|<T_2;\ \text{unde}\ T_2>T_1>T \tag{2.52}$$

Marcajul înlocuieşte un coeficient selectat prin cuantizare.

$$f'(m,n)=\begin{cases}T_2 & w_i=1 \ \text{şi} \ f(m,n)>0\\ T_1 & w_i=0 \ \text{şi} \ f(m,n)>0\\ -T_2 & w_i=1 \ \text{şi} \ f(m,n)<0\\ -T_1 & w_i=0 \ \text{şi} \ f(m,n)<0\end{cases} \tag{2.53}$$

Pentru a extrage marcajul din primul grup de coeficienţi, este calculată M valoarea medie a coeficienţilor aparţinând arborelui-zero Z_i cu relaţia:

$$w_i=\begin{cases}0 & \text{dacă} \quad Mi<0\\ 1 & \text{dacă} \quad Mi\geq 0\end{cases} \tag{2.54}$$

Pentru al doilea grup marcajul w_i este detectat dintr-un coeficient semnificativ:

$$w_i=\begin{cases}0 & \text{dacă} \quad \left|f^*(m,n)\right|<(T_1+T_2)/2\\ 1 & \text{dacă} \quad \left|f^*(m,n)\right|\geq(T_1+T_2)/2\end{cases} \tag{2.55}$$

Se folosesc poziţiile rădăcinilor pentru a „ghida" procesul de detecţie. Rezultatele experimentale arată că metoda propusă dă o imagine marcată de o calitate mai bună decât tehnicile existente la momentul respectiv şi că este robustă la compresia JPEG. Pe de altă parte, detectorul este sensibil la atacuri de desincronizare deoarece depinde de coeficienţii nesemnificativi.

În [WSK98], marcajul este adăugat la coeficienţii semnificativi în subbenzi semnificative. Mai întâi este folosită codarea wavelet multiprag MTWC, pentru a selecta coeficienţii semnificativi. Spre deosebire de alte codoare, care folosesc un singur prag iniţial în cuantizarea prin aproximaţii succesive, SAQ (Succesive Approximate Quantization), MTWC are praguri diferite în subbenzi diferite. Formula de înserare este:

$$f'_{s,i}(m,n)=f_s(m,n)+\alpha_s\beta_s T_s w_i \tag{2.56}$$

unde f' este coeficientul marcat, f este coeficientul original, α_s este ponderea pentru subbanda s, β_s este ponderea pentru subbenzi, T_s este pragul curent

pentru subbanda s în planul de biţi j, iar w_i este al *i*-lea element din secvenţa de marcaj de lungime N_w. Selectarea coeficienţilor semnificativi se desfăşoară astfel:

1) Se pune pragul $T = f_{\max,s}/2$, jumătate din maximul valorii absolute a coeficienţilor wavelet din subbanda respectivă; toti coeficienţii sunt neselectaţi.

2) Se selectează subbanda, în afară de termenul DC, cu valoarea maximă $\beta_s T_s$, unde β_s este ponderea pentru subbanda s. Pentru subbanda selectată, se examinează coeficienţii neselectaţi $f_s(m,n)$ şi se aleg ca semnificativi coeficienţii mai mari decât valoarea curentă a pragului T_s. Marcajul este înserat în aceştia.

3) Se actualizează pragul cu noua valoare $T_s^{new} = T_s/2$;

4) Se repetă paşii 2 şi 3 până când tot marcajul este înserat.

Detecţia se face fără a recurge la imaginea originală.

Xie şi Arce [XA98] descompun imaginea folosind transformata wavelet pentru a obţine o reprezentare a imaginii de frecvenţă joasă. Marcajul care este o secvenţă binară, este înserat în imaginea de aproximare (subbanda LL) a imaginii originale. De fiecare dată sunt selectaţi coeficienţii nesuprapuşi dintr-o fereastră alunecătoare, de dimensiune 3x1. Mai întâi, sunt ordonate crescător elementele b_1, b_2, b_3 ale acestei ferestre. Apoi gama între $\min|b_j|$ şi $\max|b_j|$ cu $j = 1,...,3$, este împarţită în intervale de lungime

$$\Delta = \alpha \cdot \frac{\max|b_j| - \min|b_j|}{2} \tag{2.57}$$

Medianul acestor coeficienţi este cuantizat la un multiplu de D. Coeficientul median este modificat pentru a îngloba un bit de marcaj şi înlocuit în subbanda respectivă. Procesul de extragere nu recurge la imaginea originală. Acest algoritm este construit atât pentru aplicaţii de autentificare, cât şi protejarea drepturilor de autor. Numărul nivelelor de rezoluţie determină robusteţea algoritmului. Cu 5 niveluri de rezoluţie se poate obtine o robusteţe bună. Metoda presupune însă un efort mare de calcul.

Xia ş.a. [XBA97], [XBA98] propun un algoritm de marcare cu filtre wavelet Haar, folosind două nivele de descompunere. Sunt adăugate coduri pseudo-aleatoare la coeficienţii mari, în benzile de frecvenţă mare şi medie din DWT. Înserarea se face conform relaţiei:

$$f'(m,n) = f(m,n) + \alpha \cdot f(m,n)^{\beta} w_i$$

în care α este un factor de ponderare sau intensitatea de marcare, iar β este amplificarea pentru coeficienţi mari. În subbanda de aproximare nu este înserat marcaj. De aceea, acest algoritm concentrează cea mai mare energie în muchii şi texturi, care reprezintă cei mai mulţi coeficienţi în subbenzile de detaliu. Aceasta sporeşte invizibilitatea procesului de marcare, deoarece observatorii umani sunt mai puţin sensibili la schimbarea de informaţie în muchii şi texturi, comparativ cu schimbările în componentele spectrale de joasî frecvenţă din subbanda LL. Practic se înserează mai multe marcaje în domeniul DWT în fiecare imagine de detaliu, cu excepţia subbenzii de aproximare, sugerând că detectia poate fi făcută ierarhic, calculând intercorelaţiile marcajului original cu diferenţa dintre cele două imagini pentru fiecare nivel de rezoluţie. Metoda este robustă la o serie de distorsiuni, dar

filtrarea trece-jos şi mediană afectează robusteţea marcajului deoarece coeficienţii marcati sunt în frecvenţele înalte.

Kundur şi Hatzinakos, [KH98], propun aplicarea familiei de filtre ortogonale Daubechies pentru descompunerea imaginii originale cu DWT pe trei nivele de rezoluţie. Algoritmul selectează pseudo-aleator locaţiile în care se înserează marcajul în subbenzile de detaliu. Coeficientul median este cuantizat la cel mai apropiat punct de reconstrucţie care reprezintă informaţia de marcaj. Pasul de cuantizare este controlat de parametrul Δ. Cuantizarea mai grosieră creşte robusteţea, dar astfel creşte şi distorsiunea introdusă de procesul de marcare. Robusteţea algoritmului nu este suficientă. De aceea, autorii sugerează o îmbunătăţire în [KH01], unde se foloseşte un marcaj de referinţă pentru a estima dacă un marcaj a fost înserat sau nu. Tot Kundur si Hatzinakos [KH98b], [KH99] propun o tehnică de marcare fragilă, numită metodă de dovedire a autenticităţii. Marcajul binar se înserează în domeniul wavelet prin cuantizare, cu chei specificate de utilizator. Metoda de cuantizare este aceeaşi din [KH98]. Este introdusă o transformată wavelet, care produce pixeli întregi în domeniul spaţial, pentru a evita erorile de rotunjire în timpul transformării inverse, deoarece acestea pot fi considerate ca falsificare. Algoritmul este o extensie a metodei din [KH98], fiind folosit pentru a dovedi falsificarea.

Ei dezvoltă un algoritm pentru imagini statice în care se folosesc tehnicile de fuziune a imaginilor de detaliu şi incorporează un model al HVS [KH97]. Marcajul este o imagine logo, descompusă cu DWT. Imaginea e descompusă cu L paşi unde $L \le M$. Marcajul este înserat în toate subbenzile de detaliu. Kundur prezintă şi setul de reguli pentru selectarea parametrilor pentru modelul HVS şi a parametrilor de scalare. Simulările arată robusteţea algoritmului la distorsiuni obişnuite, dar algoritmul nu este robust la rotaţie.

Chae ş.a. [CM98] folosesc ca marcaj o imagine cu nivele de gri, care poate fi 25% din imaginea originală, şi transformata DWT cu un nivel de descompunere pentru ambele imagini, cea originală şi cea de marcaj. Coeficienţii sunt "expandaţi" deoarece imaginea de marcaj este un sfert din cea originală. Pentru imaginea logo, A, B, C desemnează cei mai semnificativi biţi MSB, octetul mijlociu şi cei mai putin semnificativi biţi, LSB. Astfel A, B, C dau 24 biţi per coeficient. Sunt obţinute trei numere A', B', C' reprezentate pe 24 biţi, considerând A, B, C ca fiind cel mai semnificativ octet al acestora. Planele de biţi mijlociu şi LSB sunt puse pe zero. Se construieşte un bloc de mărime 2x2. Imaginea logo este adaugată după cum urmează:

$$f'(m,n) = \alpha f(m,n) + w(m,n) \tag{2.58}$$

unde $w(m,n)$ este coeficientul DWT al imaginii originale, iar coeficienţii DWT ai imaginii logo sunt daţi de $w(m,n)$. Acest algoritm este limitat la imagini logo de marcaj de mărime cel mult 25% din imaginea originală. Este dificil de folosit nivele de descompunere mai mari din cauza că marcajul este un logo. Rezultatele experimentale arată că procesul de marcare nu afectează vizibil imaginea, iar calitatea marcajului extras este bună chiar şi după compresia JPEG. Dar atacurile geometrice nu au fost studiate. Apare un compromis între capacitate (cantitatea de date ascunse) şi calitatea imaginii marcate.

Murkherjee [MCM98] şi Chae ş.a. [CMM98] introduc o secvenţă de marcaj w_i de simboluri cu p biţi (structura latice). Este calculată o descompunere de un nivel DWT a imaginii originale şi a imaginii marcate, iar coeficienţii sunt cuantizaţi în

p-nivele. Patru coeficienţi sunt aranjaţi pentru a forma un vector de dimensiune n. Coeficienţii corespunzători din banda de aproximare a imaginii logo de marcaj sunt înseraţi în coeficienţii corespunzători din banda LL a imaginii originale. Aceeaşi metodă este aplicată şi pentru benzile de detaliu. Înserarea se face conform relaţiei:

$$v' = v + \alpha C(w_i) \tag{2.59}$$

unde $C(w_i)$ este cuvântul de cod pentru coeficienţii de marcaj w_i. Pentru a detecta marcajul, este cerută imaginea originală. Vectorul eroare:

$$e = \frac{v^* - v}{\alpha} \tag{2.60}$$

este folosit pentru căutarea vecinului cel mai apropiat din dicţionarul cuvintelor de cod, pentru a recupera informaţia de marcaj:

$$w_i = \min_{w_i} \left\| C(w_i) - e \right\|$$

Robusteţea poate fi controlată cu factorul de intensitate α şi calitatea imaginii de marcaj poate fi reglată prin nivelul de cuantizare p. Căutarea în dicţionar face metoda lentă dacă acesta este mare.

O metodă de marcare pentru decizie multi-index (metoda maximizării deviaţiei) este propusă de Zhihui şi Liang [ZL00]. Tehnica este aplicată în domeniul DCT şi wavelet, folosind modele vizuale umane. Rezultatele experimentale arată că metoda bazată pe transformata DWT se apropie de capacitatea de marcare maximă, comparativ cu alte domenii de marcare.

Tsekeridou şi Pitas [TP00] folosesc marcaje cu autocorelaţie mare într-o reţea carteziană, cvasi-invariante la scalare. Schema este implementata în domeniul wavelet. Este de aşteptat ca aceste marcaje să fie robuste la scalare dar nu şi la alte transformări geometrice.

In [HTC00] se prezintă o arhitectură VLSI, pentru algoritmul EZW, care face o codare a imaginii în timp real. Pentru scanarea coeficienţilor wavelet se face o căutare pe nivel, începând de sus, pentru a localiza relaţiile părinte-copil şi pentru a creşte viteza. Simbolurile generate în procesul de creare a hărţii de semnificaţii (SMAP) şi cuantizarea prin aproximaţii succesive (SAQ) sunt codate independent. Aceasta permite transmisia a mai puţini biti şi uşurează comunicaţia fără sacrificarea PSNR-ului. Împreuna cu codorul EZW este prezentată o schemă progresivă de marcare, pentru protejarea drepturilor de autor.

Loo şi Kingsbury [LK00] propun un algoritm de marcare în domeniul transformării wavelet complexe; ei modelează marcarea ca o comunicaţie. Ei arată că CWT are o capacitate relativ mare de înserare. Se concluzionează că CWT este un domeniu potrivit pentru a însera un marcaj.

Hsu şi Wu [HW00] descompun marcajul şi imaginea gazdă printr-o reprezentare multirezoluţie, marcajul fiind o imagine logo. Imaginea de marcaj este 50% din cea originală care se descompune cu DWT Daubechies-6, iar imaginea de marcaj cu o funcţie de reducere în rezoluţie RR, din standardul de compresie JBIG. Această descompunere este potrivită pentru imagini alb-negru, dar nu e practică pentru imagini normale. Un nivel de diferenţă este obţinut prin scăderea unei versiuni mărite a reziduului din marcajul original. Coloanele pare ale marcajului sunt ascunte în subbenzile HL_i, iar cele impare în subbenzile LH_i. Marcajul nu se inserează în subbanda de aproximare pentru a mentine imperceptibilitatea, şi nici în subbenzile HH_i pentru că marcajul este mai uşor de distrus în frecvenţele înalte.

Masca reziduală este folosită pentru a modifica relaţia dintre coeficienţii vecini din imaginea gazdă. Imaginea originală se presupune cunoscută la detector. Algoritmul este sensibil la orice fel de compresie, din cauză că informaţia de marcaj este înserata în subbenzile de detaliu.

Ejima şi Miyazaki [EM00] folosesc pachetele wavelet pentru marcare de imagini şi video. Este calculată energia fiecărei subbenzi $B_{i,j}$, iar anumite subbenzi sunt selectate pseudo-aleator conform energiei. Media valorii absolute a coeficienţilor pentru fiecare subbandă selectată este cuantizată şi folosită pentru înserarea unui bit de informaţie. Coeficienţii din subbanda respectivă, selectaţi pseudo-aleator, sunt modificaţi pentru a reflecta această medie cuantizată. Algoritmul generează informaţie redundantă, fiindcă pachetele wavelet au subbenzi de detaliu şi aproximare pentru fiecare nivel de rezoluţie, ceeace duce la creşterea complexităţii metodei.

Kim ş.a. [KSLR99] înserează marcajul în coeficienţii mari ai fiecărei subbenzi DWT, cu L=3 nivele de rezoluţie, în afară de primul nivel. Numărul de biţi de marcaj w_i este proporţional cu energia subbenzii respective. Energia este definită ca fiind:

$$e_s = \frac{1}{M \cdot N} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} f^2(m,n) \tag{2.61}$$

unde M, N sunt dimensiunile subbenzii ; marcajul w_i este generat dintr-o secvenţă pseudo-aleatoare de numere reale cu distribuţie gaussiană. În subbenzile de detaliu, sunt modificaţi 4500 de coeficienţi, dar numai 500 în subbanda de aproximare. Înainte de înserare, coeficienţii sunt sortaţi după amplitudine. Metoda este robustă la compresie JPEG, netezire, decupare. Nu se fac referiri la robusteţea împotriva atacurilor geometrice (redimensionare, rotaţie).

În [KM99] sunt selectaţi coeficienţii semnificativi perceptual cu ajutorul pragurilor dependente de nivel. Imaginea este descompusă în trei nivele L=3, cu filtre biortogonale. Marcajul este o secvenţă gaussiană, de 1000 de numere pseudo-aleatoare reale. Detecţia se face folosind pragurile cunoscute din procesul de înserare. Metoda este robustă la diverse atacuri, dar nu şi la cele geometrice. Lucrarea nu se referă la posibilitatea înserarii marcajului cu repetiţie, sau ponderarea marcajului pentru a creşte robusteţea. O metodă similara, propusa în [KKK02], înserează marcajul în coeficienţii semnificativi perceptual pentru fiecare subbandă, folosind proprietăţile statistice ale HVS şi ale imaginii originale.

In [BBP01], autorii înserează marcajul în toţi coeficienţii subbenzilor de detaliu de la nivelul de rezolutie cel mai fin, dar folosind un factor de ponderare care împiedică sesizarea marcajului. Masca perceptuală ţine cont de sensibilitatea la zgomot, textura şi luminanţa tuturor subbenzilor.

$$\tilde{I}_l^{\theta}(i,j) = I_l^{\theta}(i,j) + \alpha w_l^{\theta}(i,j) x_l^{\theta}(i,j) \tag{2.62}$$

unde α este intensitatea de marcare iar $w_l^{\theta}(i,j)$ este o funcţie de ponderare, a cărei valoare este egală cu jumătate din pasul de cuantizare, $q_l^{\theta}(i,j)$. Pasul de cuantizare este calculat ca produsul ponderat a trei factori. Metoda nu se foloseşte de imaginea originală la detecţie şi este extrem de robustă la diverse tipuri de atacuri. O extensie a acestei metode în domeniul transformarii wavelet redundante este propusă în [HF02].

Tehnicile de marcare în domeniul wavelet sunt de asemenea folosite pentru marcarea fragilă, care este o componentă semnificativă în autentificarea conţinutului [PW03, KH99].

2.2.2.e Metode ce folosesc fractalele

Ideea folosirii fractalelor a apărut în [PJ96]. Tehnicile de marcare bazate pe compresia imaginii cu fractale sunt strâns legate de tehnicile de marcare în domeniul spaţial. În compresia cu fractale a imaginii, aceasta este codată folosind principiile sistemelor cu funcţii iterative şi auto-similaritate (self-similarity). Codorul foloseşte auto-similaritatea imaginii la diferite rezoluţii, asociind, printr-o serie de comprimări, blocurile mai mari ale imaginii unor blocuri similare mai mici. Decodorul aplică oricărei imagini transformările inverse pentru a găsi originalul. Modificând dimensiunea blocurilor, pragul de eroare şi distanţa de căutare, se modifică timpul de codare, PSNR şi rata de bit. Comparativ cu codarea JPEG şi JPEG-2000, folosirea fractalelor duce la un timp de codare mult mai mare, dar decodarea este mult mai rapidă.

Imaginea originală este împărţită în blocuri pătrate R_k numite blocuri de gamă (range block). F este setul de funcţiilor de asociere f_k, compuse dintr-o transformare geometrică g_k şi o transformare masică m_k (massic transform). Funcţiile de asociere sunt aplicate pe blocuri de domeniu D_k, mai mari decât blocurile de gamă.

Transformarea geometrică implică mutarea blocului de domeniu D_k la locaţia unui bloc de gamă R_k şi reducerea mărimii acestuia la mărimea blocului de gamă.

Transformarea masică implică ajustarea intensităţii şi orientării pixelilor în blocul de domeniu, după transformarea geometrică, rotaţii cu 90, 180 şi -90^0, reflecţia la jumătatea orizontalei şi a axelor diagonale, precum şi asocierea identităţii.

Pentru a comprima o imagine pentru toate blocurile de gamă R_k, trebuie găsită cea mai bună funcţie de asociere, astfel încât diferenţa dintre blocul de domeniu R_k şi blocul domeniu asociat $F_k(D_k)$ să fie minimă. Deci codarea include o căutare spaţială pe toate blocurile de domeniu posibile. Decodarea se face prin iterarea funcţiilor de asociere codate folosind orice imagine iniţială. Pentru a însera un bit cu această schemă, e selectat pseudoaleator un bloc de gamă. Spaţiul de căutare corespunzător S_k pentru blocurile de gamă este apoi divizat în două subspaţii de căutare, S_K^1 si S_K^2, de dimensiune egală. Fiecare subspaţiu este asignat unui bit, şi blocul de gamă curent e codat printr-o căutare doar în subspaţiul corespunzător valorii bitului curent. Pentru a regăsi bitul înserat, imaginea e comprimată din nou, de data aceasta folosind întregul spaţiu de căutare, a blocurilor de domeniu. Pentru blocul de gamă marcat, locaţia blocului de domeniu corespunzător indică valoarea bitului înserat. Algoritmul a fost testat pentru compresie JPEG şi a indicat o robusteţe bună, până la o compresie cu o calitate de aproximativ 50%. Dezavantajul tehnicii este viteza redusă datorată schemei de compresie cu fractale.

O abordare foarte asemănătoare a fost propusă de Davern şi Scott [DS96]. Singura diferenţă este că ei nu codează întreaga imagine, ci doar o regiune de gamă definită de utilizator, bazată pe regiunea de domeniu definită tot de utilizator. Fiind date două regiuni, codarea marcajului este echivalentă cu sistemul propus de Puate si Jordan [PJ96] în care regiunea e împărţită în două şi, depinzând de valoarea bitului, este folosită una din cele două părţi pentru codarea unui bloc de gamă. Ideea folosirii fractalelor în domeniul spaţial pentru marcare a fost extinsă pentru transformata DCT pe blocuri de către Bas ş.a.[BCD98].

În [FS00] se propune pentru marcarea transparentă o metodă bazată pe transformata DCT în subbenzi, compusă dintr-o transformată wavelet şi apoi una DCT aplicată pe fiecare subbandă. Marcajul este distribuit într-un număr mare de coeficienţi selectaţi din toate patru subbenzile unei descompuneri cu un nivel. Fiecare subbandă dă o altă ieşire a detectorului. Rezultatul este mediat. Rezultatul final este îmbunătăţit faţă de ieşirea per subbandă, iar schema de marcare este foarte robustă. Autorii folosesc acelaşi detector ca cel propus de Piva în [BBCP98a].

In [KAS05] autorii înserează marcajul în domeniul transformatei discrete multiwavelet; pentru a găsi parametri, ca pragurile de detecţie şi intensitatea de înserare, se folosesc algoritmi genetici.

2.2.2.f Marcare transparentă cu transformata SVD.

Există metode care înserează marcajul în domeniul spaţial sau al unei transformate, ca DCT sau DWT, dar numai după ce este aplicată şi transformarea SVD (Singular Value Decomposition), de descompunere în valori singulare, care are proprietatea de a concentra energia în câţiva coeficienţi [LT02], [Cha02], [Cha03], [GZE03], [GE04]. Transformarea SVD este o tehnică liniara în algebră, cu aplicaţii ca: problema celor mai mici pătrate, calcularea matricii pseudo-inverse şi analiza cu variabile multiple. În plus, SVD a fost folosită pentru codarea imaginii, estimarea zgomotului şi mai recent marcarea imaginilor. O imagine X de mărime M×N, cu M ≥ N, poate fi reprezentată cu SVD astfel:

$$X = U \sum V^T = \sum_{i=1}^{N} \sigma_i u_i v_i^T \tag{2.63}$$

unde U şi V sunt matrici ortogonale de mărime MxM, respectiv NxN, iar $\sum$ este o matrice MxN cu elementele diagonale reprezentând valorile singulare, σ_i a lui X. Coloanele matricii ortogonale U sunt vectorii singulari din stânga, iar cele ale matricii V – vectorii singulari din dreapta. Vectorii singulari din stânga lui X sunt vectori proprii a lui XX^T ; vectorii singulari din dreapta sunt vectori proprii pentru $X^T X$. Matricea Σ are structura de forma:

$$\sum = \begin{bmatrix} \sigma_1 & & 0 \\ 0 & \sigma_2 & \\ & & \\ 0 & & \sigma_N \\ \hline & 0 & \end{bmatrix} \tag{2.64}$$

Transformarea SVD este o descompunere matricială care, în sensul celor mai mici pătrate, compactează maximum de energie a semnalului în cât mai puţini coeficienţi posibili. Are posibilitatea de a se adapta la variaţiile statistice locale ale

imaginii; cu toate acestea, tranformarea SVD a imaginii este necesară pentru a recupera marcajul. În [Cha02], atât marcajul cât şi imaginea gazdăa se descompun cu SVD. Marcajul este o imagine mai mică decât imaginea originală.

$$X = U \sum_x V^T \tag{2.65}$$

$$W = U_w \sum_w V_w^T \tag{2.66}$$

Inserarea valorilor singulare ale marcajului se face folosind valorile singulare ale imaginii originale, precum si o intensitate de marcare. Dacă imaginea de marcaj este mai mică, se folosesc numai primele valori singulare:

$$\sigma_{y_i} = \sigma_{x_i} + \alpha_i \sigma_{w_i} \tag{2.67}$$

Imaginea marcată se obţine tot cu transformata SVD, folosind matricile U şi V:

$$Y = U \sum_y V^T \tag{2.68}$$

Estimarea marcajului se face informat, cunoscând imaginea originală, şi marcajul original, mai precis matricile $\sum_x$, U_w si V_w; detecţia presupune următorii paşi:

$$\hat{Y} = \hat{U} \hat{\sum}_y \hat{V}^T \tag{2.69}$$

$$\hat{\Sigma}_w = \frac{\hat{\Sigma}_y - \Sigma_x}{\alpha} \tag{2.70}$$

$$\hat{W} = U_w \hat{\Sigma}_w V_w^T \tag{2.71}$$

Gradul de asemănare este dat de similaritatea dintre W şi $\hat{W}$. Pentru a însera mai multi biţi, imaginea se descompune în blocuri. Rezultatele arată că metoda neadaptivă este mai robustă decât cea adaptivă, pentru ambele abordări, pe toată imaginea, sau pe blocuri.

O metodă similară, bazată pe transformarea SVD pe blocuri 8x8 pentru inserarea unei imagini logo este descrisă în [Cha03]. În [GZE03] se foloseste marcare dublă în domeniul SVD, iar în [GE04] marcajul este inserat domeniul DWT-SVD.

2.2.2.g Marcare transparentă cu transformata Ridgelet. O schema multiplicativă în domeniul Ridgelet este propusă în [CKN04]. Sensibilitatea direcţională şi anizotropia transformatei RT sunt folosite pentru a obţine o reprezentare rară (sparse) a imaginii, în care coeficienţii semnificativi sunt direcţiile cu energie mare asociate muchiilor drepte. Pentru o imagine naturală, imaginea de muchii asociată este obţinută cu un banc de filtre, construite cu funcţii circulare armonice CHF; apoi această imagine de muchii este împărţită în blocuri mai mici pentru a obţine muchii drepte. Transformata RT este aplicată fiecărui bloc, iar marcajul este înserat în anumiţi coeficienţi.

2.2.2.h Marcare transparentă cu cuaternioni. Imaginile color pot fi marcate separat per canal, sau în domeniul transformatei cuaternionice, [BBC03]. Pixelii RGB sunt asociaţi cu un număr unic în domeniul QFT, care are trei părţi imaginare. Transformata QFT depinde de un cuaternion pur μ; valoarea acestuia este selectată pentru o robusteţe şi/sau imperceptibilitate dată, funcţie de valoarea medie a culorii per bloc şi a unei componente perceptuale. Una din schemele implementate este bazată pe QIM. Metoda este robustă la tehnici de filtrare de luminanţă.

2.2.2.i Marcare transparentă cu transformata LOT. In [PRP99] autorii propun o metodă de marcare de tip SS în domeniul transformatei LOT (Lapped

Orthogonal Transforms), folosită în locul transformatei DCT pentru a nu produce artefacte vizibile atunci când puterea marcajului creşte. Se sugerează folosirea unui model în domeniul DFT pentru a compensa dezavantajul că transformata LOT nu este robustă la decupare, rotaţie sau schimbare de scală. O dată detectate aceste transformari, marcajul este detectat în domeniul LOT, fără a folosi imaginea originală. Alte tehnici folosesc segmentarea Voronoi şi apoi o transformată, cum ar fi DCT [SO03].

2.3 Concluzii

Cele mai multe scheme se bazează pe acelaşi principiu simplu, schimbarea redusă a valorii unor coeficienţi aleşi pseudoaleator în domeniul spaţial sau al unei transformate. Aceste schimbări sunt apoi identificate folosind un corelator sau alte tehnici asemănatoare corelaţiei. În mod normal, numărul de coeficienţi modificaţi este mult mai mare decât numărul de biţi de înserat. Aceasta poate fi considerată ca o marcare redundantă şi duce implicit la creşterea robusteţii.

Domeniul de înserare al marcajului poate influenţa semnificativ robusteţea marcajului. Metodele de marcare în domeniul spaţial sunt mai puţin robuste la atacuri de tip adăugare de zgomot, compresie JPEG. Dar marcajul poate fi recuperat uşor dacă imaginea a fost decupată sau translatată. Acest avantaj este mai puţin evident în frecvenţă. Decuparea în domeniul spaţial produce distorsiuni mari în domeniul spectral ceea ce duce de obicei la distrugerea marcajului. Acelaşi lucru este valabil şi pentru transformata DCT aplicată pe toată imaginea. Dacă sunt marcate blocuri DCT, pentru o detecţie cu succes este important să se cunoască poziţia blocurilor în care a fost înserat marcajul. Domeniul wavelet are dezavantaje asemănătoare, deoarece transformarea nu este invariantă la translaţie sau rotaţie. Cele mai multe metode plasează marcajul în domeniul spaţial, dar şi numărul metodelor în domeniul DCT este mare.

3. ATACURI ASUPRA SISTEMELOR DE MARCARE

3.1. Problema marcării transparente

Canalul de distribuţie a documentelor multimedia de la producător la utilizatori, poate fi considerat ca un *canal de atac* asupra marcajului înserat, astfel că abordarea acestei probleme face apel la metodele din teoria transmisiunii informaţiei. Atacurile pot genera distorsiuni întâmplătoare sau intenţionate. Atacurile pot avea loc în timpul transmisiei sau asupra mediului de memorare. Atacurile pot fi clasificate şi în funcţie de obiectivele pe care încearcă să le împiedice.

Obiectivele marcării transparente sunt: *imperceptibilitatea, robusteţea, capacitatea, şi securitatea criptografică.*

Imperceptibilitatea se referă la faptul că marcajul ar trebui să nu poată fi perceput şi în plus să nu interfereze cu datele ce trebuie protejate. Deşi diferenţele abia vizibile se accentuează dacă produsul original este comparat direct cu cel marcat, ele rămân practic neobservate, deoarece produsul original este accesibil doar proprietarului legal.

Robusteţea se referă la posibilitatea de înlăturare a marcajului: cu cât acesta este mai greu de înlăturat, cu atât marcajul este mai robust. Atacurile asupra robusteţii sunt cele care încearcă să elimine sau să estimeze marcajul prin prelucrarea semnalului primit.

Capacitatea se referă la cantitatea de informaţie conţinută de marcajul înglobat. Atacurile asupra capacităţii vizează reducerea capacităţii marcajului. Astfel, într-o aplicaţie de *fingerprinting*, fiecare utilizator primeşte o copie a originalului, în care este înserat un marcaj diferit. Prin formarea unei coaliţii de atacatori, în urma acţiunii lor comune, se reduce capacitatea marcajului.

Securitatea criptografică se referă la integritatea semanticii marcajului şi la identificarea sursei în aplicaţia de autentificare, respectiv la asigurarea confidenţialităţii marcajului în marcarea robustă. Atacurile asupra securităţii criptografice sunt atacuri de falsificare ilegală. Un exemplu grăitor este fotografia lui Bill Clinton alături de soţia sa Hillary, care în varianta falsă pare că este alături de Monica Levinsky [BCHL05, C.-Y. Lin]. Sistemul propus de C.-Y. Lin poate reconstitui imaginea originală; acesta este cunoscut sub denumirea de *Self-Authentication and Recovery Image*, SARI [LYC00].

Ultimele trei obiective – robusteţea, capacitatea, şi securitatea criptografică – reprezintă şi punctele vulnerabile ale sistemului de marcare în faţa unui atacator.

3.2. Constrângeri asupra atacatorului

Obiectivul atacatorului este *reducerea securităţii sistemului de marcare*, adică reducerea probabilităţii de detecţie/extragere a marcajului original, respectiv creşterea probabilităţii de detecţie/extragere a unui marcaj care nu a fost înserat în semnalul marcat (extragere falsă). În atingerea obiectivelor sale, atacatorul este supus şi el unor constrângeri [Kun05].

O primă constrângere este *imperceptibilitatea*. Un atacator trebuie să păstreze valoarea comercială a produsului multimedia în cauză, neputând induce decât *distorsiuni imperceptibile*, distorsiuni care se apreciază prin:

- variaţia energiei imaginii: eroarea medie pătratică MSE, raportul semnal-pe-zgomot, SNR, sau raportul semnal pe zgomot de vârf, PSNR; dar acestea nu sunt cele mai bune măsuri pentru evaluarea degradării calităţii unei imagini.

- factorul JND (*Just Noticeable Difference*), diferenţa abia sesizabilă, când marcajul este considerat încă imperceptibil; se foloseşte în modelele perceptuale. Un JND este acel nivel de distorsiune introdus care poate fi perceput în 50% din cazuri [CMB02]. Modelul propus de Watson în [Wat93] încearcă să estimeze JND comparând imaginea originală şi cea degradată. El defineşte unitatea de măsură a JND cu ajutorul unui zgomot alb, care produce o distorsiune unitară.

A doua condiţionare se referă tot la *consideraţii de ordin perceptual*, cum ar fi tipul de document multimedia care este marcat, agresivitatea codării perceptuale aplicate, respectiv procesări sau atacuri anterioare.

A treia constrângere se referă la *ipoteza marcării transparente* (*marking assumption*), când se presupune că există o schemă de marcare ce satisface în acelaşi timp cerinţele de fidelitate şi robusteţe. Acest principiu este folosit în construirea codurilor rezistente la coliziune pentru amprentarea (*fingerprinting*) datelor [BS95], [BS98]. Amprenta este compusă dintr-un set de mărci, fiecare fiind modelată ca poziţie în semnalul digital şi poate lua un număr finit de stări. O *marcă* este considerată *detectabilă* dacă membrii unei coaliţii de utilizatori nu au mărcile identice pe fiecare poziţie.

Spre exemplu, pentru mai multe copii marcate ale aceluiaşi document original, marcajul poate fi identificat prin localizarea pixelilor de valoare diferită de pe aceleaşi poziţii (umbrite în Figura 3.1). Ipoteza marcării transparente presupune că mărcile nedetectabile nu pot fi schimbate arbitrar fără a face semnalul digital inutilizabil; dar se consideră perfect posibil ca o marcă detectabilă să fie schimbată în orice stare de către coaliţia de atacatori. Conţinutul redistribuit de atacator va include părţi din amprenta originală, permiţând astfel identificarea copiilor ilegale (*traitor tracing*). Astfel, un posibil atac este interschimbarea pixelilor sau coeficienţilor unei transformate a imaginii de valoare diferită în copiile respective.

$$
\begin{array}{rcl}
m_1 & = & \boxed{0}\,1\,\boxed{1}\,1\,0\,\boxed{1} \\
m_2 & = & \boxed{0}\,1\,\boxed{1}\,0\,1\,\boxed{1} \\
m_3 & = & \boxed{0}\,0\,\boxed{1}\,1\,1\,\boxed{1}
\end{array}
$$

Fig. 3.1: Într-o coaliţie de atacatori, aceştia nu cunosc localizarea marcajului, decât prin compararea coeficienţilor de valoare diferită în copii marcate diferite.

Atacatorul este limitat de *informaţia de care dispune pentru a estima/elimina marcajul* şi anume: algoritmii de înserare/extragere a marcajului; modelele perceptuale pentru semnalele multimedia; numărul necesar de copii ale aceleiaşi imagini, marcate cu marcaje diferite, pentru atacul de coliziune tip I cu

succes; numărul necesar de copii ale imaginilor diferite marcate cu acelaşi marcaj, pentru atacul de coliziune tip II cu succes.

În fine, atacatorul este condiţionat de *resursele disponibile*: puterea de calcul, documentul original, decodorul, respectiv codorul.

3.3. Clasificarea atacurilor

Atacurile pot folosi *o singură copie marcată* a unui original (caz în care atacurile pot fi *neintenţionate* sau *intenţionate*), sau *mai multe copii* ale documentului original (caz în care ele sunt intenţionate).

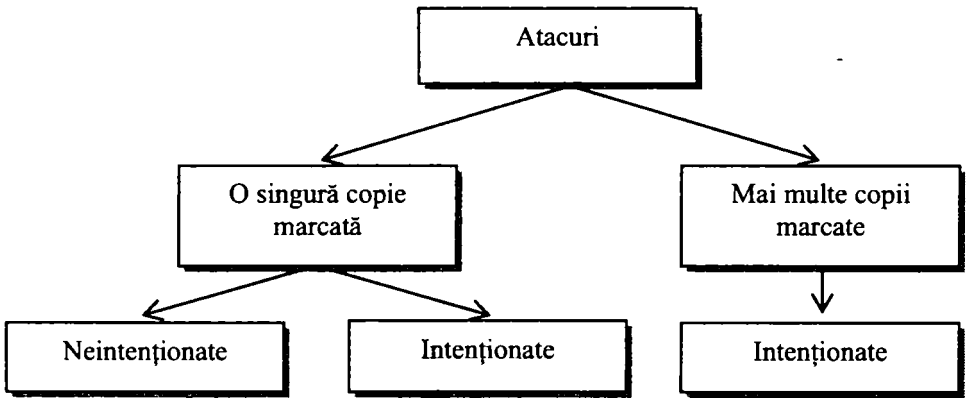


Fig. 3.2: Clasificarea atacurilor, funcţie de numărul de copii marcate.

Atacurile asupra unei copii marcate, pot fi clasificate după cum urmează:

- *neintenţionate*: conversiile în alt format, care rezultă din
  - compresie,
  - modificarea ratei de bit,
  - compensarea raportului de aspect, sau
  - conversia tipului de fişier.

- *intenţionate*, care se pot clasifica în două mari categorii:
  - atacuri asupra unui *singur cadru* (*single-frame*):
    - filtrare,
    - transformări geometrice,
    - atacuri criptografice,
    - de protocol,
    - de estimare a semnalului gazdă sau a marcajului,
    - zgomot aleator;
  - atacuri asupra *mai multor cadre* (*multiple-frames*):
    - medierea mai multor cadre;
    - estimarea mai multor cadre (de exemplu prin mediere ponderată).

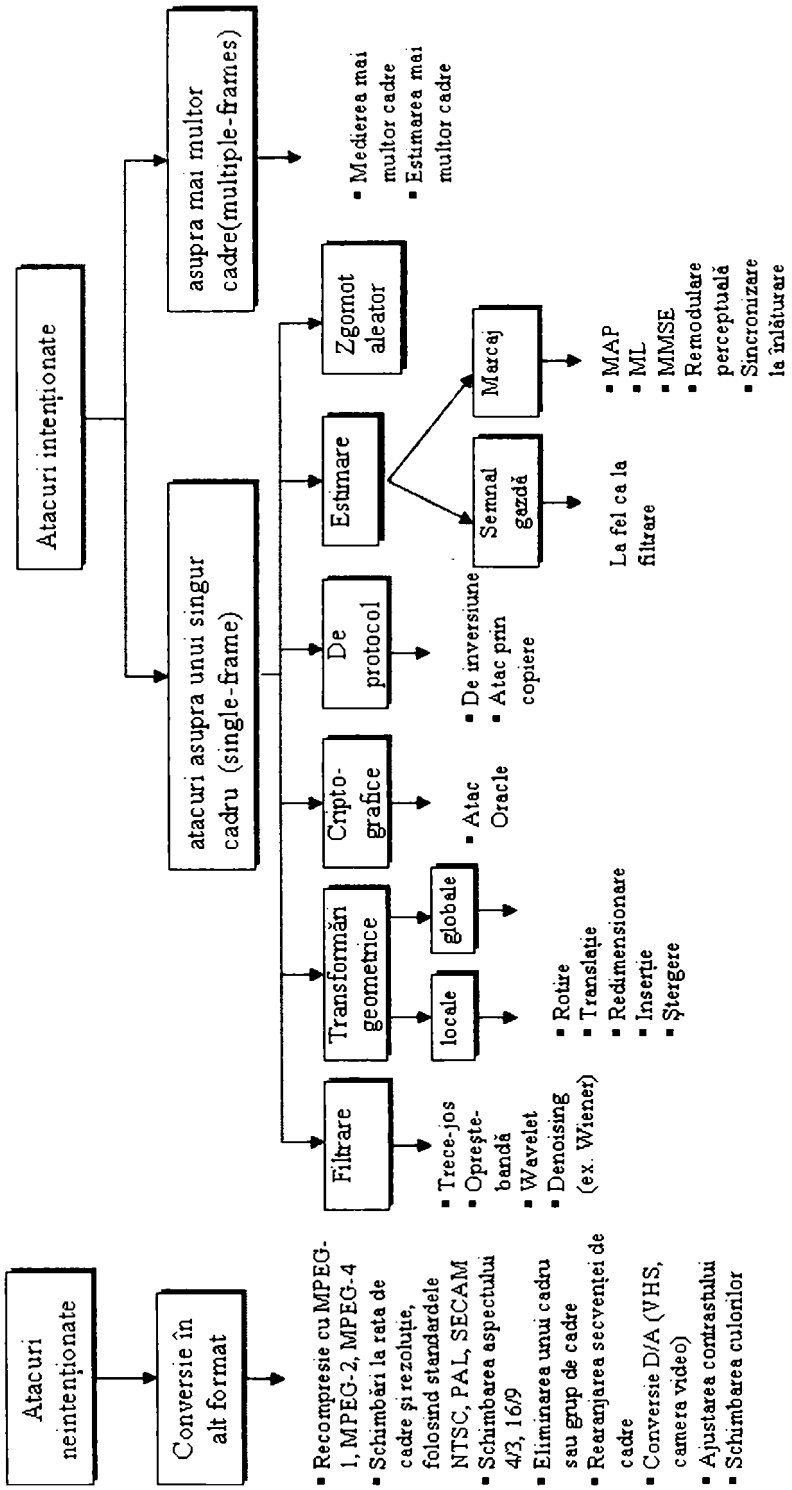


Fig. 3.3: Atacuri ce acționează asupra unei copii marcate.

3.4 Atacuri care folosesc o copie marcată

Aceste atacuri folosesc o singură copie a documentului marcat, putând fi intenţionate sau nu. Atacurile *intenţionate* asupra unui singur cadru exploatează informaţia spaţială şi/sau spectrală a unei imagini, în timp ce atacurile intenţionate ce operează asupra mai multor cadre folosesc informaţia temporală de la cadru la cadru.

3.4.1 Compresia

În categoria atacurilor *neintenţionate*, cel mai întâlnit atac este compresia. Aceasta înlătură părţile nesemnificative din punct de vedere perceptual, dintr-un semnal multimedia. Astfel, prin compresie, semnale perceptual asemănătoare, ajung să fie identice. Pe de altă parte, marcarea înserează mesaje diferite într-un semnal multimedia original, astfel că se ajunge la o mulţime de semnale diferite, dar perceptual asemănătoare. Prin urmare, cele două operaţiuni sunt complementare.

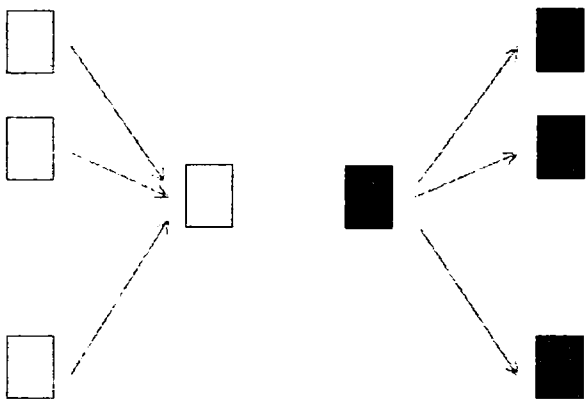


Fig. 3.4: Compresia şi marcarea transparentă, ca operaţii complementare.

Robusteţea la compresia JPEG poate fi îmbunătăţită în mai multe moduri. O metodă constă în comprimarea şi apoi decomprimarea unui model pseudo-aleator W, cu ajutorul algoritmului JPEG [SC96]. Energia modelului rezultat este crescută pentru a compensa pierderea de energie datorită compresiei. În final, acest model este adăugat la imagine pentru generarea imaginii marcate. Aici, ideea este de a folosi algoritmul de compresie pentru a elimina în avans, prin filtrare, toată energia care s-ar pierde mai târziu pe parcursul compresiei. Se presupune că un marcaj alcătuit în acest fel, este invariant la compresii JPEG ulterioare, cu acelaşi factor de calitate, cu excepţia unor mici artefacte numerice. Pot fi aplicate alte distorsiuni preliminare ale modelului de marcaj, precum filtrarea, pentru a preveni alte degradări anticipate ale imaginii marcate.

În [NP96] energia modelului de marcaj este concentrată în componentele spectrale de frecvenţe mai joase, prin calcularea unui factor de câştig individual $k_{x,y}$ pentru fiecare pixel al modelului de marcaj, în locul folosirii aceluiaşi factor de câştig k pentru toţi pixelii. Mai întâi este generat un model pseudo-aleator W(x,y), care constă din numerele *0* şi *k*. Apoi modelul este despărţit în blocuri 8x8, şi este calculată transformata DCT W(u,v) a fiecărui bloc 8x8. Elementele nenule din

blocurile 8x8, sunt acum privite ca factori de câştig $k_{x,y}$, şi adaptate în aşa fel încât energia Φ din coeficienţii DCT de frecvenţă înaltă F_H să fie minimizată (Figura 3.5):

$$\Phi = \sum_{u,v \in F_H} W(u,v)^2 \qquad F_H = \{u,v \mid 5 < u \le 8, 5 < v \le 8\}$$

Energia Φ este minimizată ţinând cont de următoarea condiţie:

$$\sum_{x=1}^{8}\sum_{y=1}^{8} W(x,y)\cdot k = \sum_{x=1}^{8}\sum_{y=1}^{8} W(x,y)\cdot k_{x,y},\ k_{\min} \le k_{x,y} \le k_{\max}$$

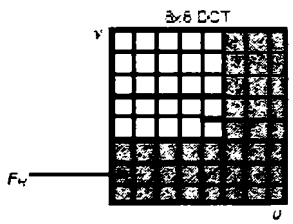


Fig. 3.5: Banda DCT F_H în care energia Φ a marcajului este minimizată

Efectul minimizării energiei de frecvenţe înalte asupra modelului marcajului este ilustrat în Figura 3.6. Figura 3.6 (a) arată modelul marcajului în interiorul unui bloc 8x8, unde este folosit un factor de câştig constant *k=3.* După minimizarea energiei pentru k_{min}=0 şi k_{max}=6, modelul marcajului descreşte spre zero (Fig. 3.6 (b)), deşi suma pixelilor nenuli încă este egală cu suma pixelilor nenuli din marcajul original.

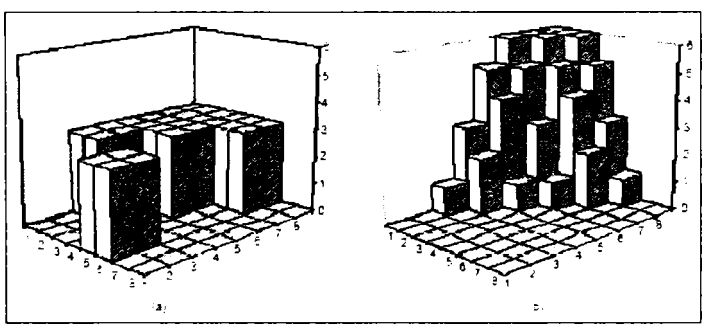


Fig. 3.6: (a) Marcaj original şi (b) Marcaj de frecvenţă joasă

În [HLR00] şi în [LLL97], imunitatea la compresia JPEG se asigură prin obţinerea unui factor de câştig *k* pentru fiecare bloc de 32x32 de pixeli, pe baza unei imagini comprimate JPEG de calitate mai scăzută. La fiecare bloc de imagine de 32x32 pixeli este adăugat un model pseudo-aleator de 32x32 pixeli reprezentând un bit de marcaj. O copie a acestui bloc de imagine marcată, este degradată în conformitate cu standardul JPEG, pentru care se foloseşte un factor de calitate relativ scăzut. Dacă bitul de marcaj nu se poate extrage corect din această copie degradată, modelul de marcaj este adăugat la imagine cu ajutorul unui factor de câştig mai mare, şi este alcătuită o nouă copie degradată pentru a verifica bitul.

Această procedură este repetată iterativ pentru fiecare bit, până toţi biţii pot fi extraşi cu un grad de certitudine mare din copiile degradate. Un marcaj format în acest mod este rezistent la compresia JPEG, folosind un factor de calitate mai mare sau egal cu factorul de calitate folosit pentru degradarea copiilor. În figura 3.7 este dat un exemplu pentru un asemenea marcaj, amplificat pentru a fi vizibil.

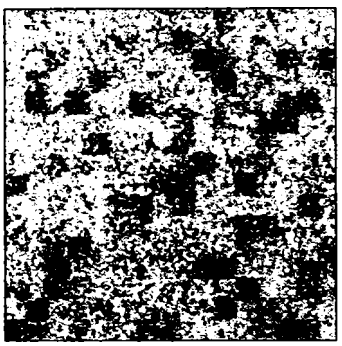


Fig. 3.7: Marcaj unde factorul de câştig local la un bloc este bazat pe o imagine comprimată JPEG cu calitate mai scăzută

3.4.2 Filtrarea

Filtrarea modelează *marcajul ca un zgomot aditiv*, care este o presupunere rezonabilă în cazul marcării transparente de tip *spread spectrum*. Înlăturarea marcajului este echivalentă cu o problemă de eliminare a zgomotului din imagine (*denoising*), rezultatul fiind estimarea imaginii originale.

Pentru *denoising* se pot folosi metode simple de filtrare medie şi mediană în domeniul spaţial, respectiv filtrarea trece-jos, opreşte-bandă, folosirea filtrelor *wavelet* în domeniul unei transformate. O abordare îmbunătăţită este filtrarea trece-bandă a unei anumite game de frecvenţă, în cazul în care marcajul a fost înserat într-o gamă cunoscută de frecvenţă.

Filtrarea de tip trece-jos este un atac eficient dacă marcajul a fost înserat în coeficienţii de înaltă frecvenţă, iar filtrarea opreşte-bandă este eficientă dacă marcarea a fost făcută folosind coeficienţii de frecvenţă medie.

O altă metodă de *denoising* este filtrarea Wiener, care nu necesită informaţie apriori, fiind bazată pe modelarea stohastică a imaginilor cu modelul gaussian staţionar generalizat [VHBP99]. Considerând o secvenţă video cu N_f cadre marcate y_t, din care x_t sunt cadrele originale, respectiv n_t sunt marcajele înserate, se calculează estimatul cadrului original $\hat{x}_t$ după cum urmează:

$$\hat{x}_t(i,j) = \left(\frac{\hat{\sigma}^2_{x_t}(i,j)}{\hat{\sigma}^2_{x_t}(i,j) - \sigma^2_{n_t}} \right) y_t(i,j) \qquad t = 1 \ldots N_f \tag{3.1}$$

unde $\hat{\sigma}^2_{n_t}$ este estimatul dispersiei globale a marcajului şi $\hat{\sigma}^2_{x_t}$ este estimatul dispersiei *locale* a semnalului original. Dispersia globală a marcajului este dată de relaţia:

$$\hat{\sigma}_{n_t}^2 = \left(\frac{\text{med}_{i,j}\left[\left| y_t(i,j) - \hat{\bar{x}}_t(i,j) \right| \right]}{0.6745} \right)^2 \qquad t = 1 \ldots N_f \tag{3.2}$$

unde $\text{med}_{i,j}$ este valoarea mediană globală; valoarea 0.6745 a fost calculată în conformitate cu modelul gaussian staţionar generalizat, iar $\hat{\bar{x}}_t$ este pre-estimatul mediei locale pentru imaginea originală.

Dispersia locală a imaginii originale poate fi aproximată ca fiind:

$$\hat{\sigma}_{x_t}^2(i,j) = \max\left[0, \overline{y_t^2}(i,j) - \hat{\sigma}_{n_t}^2 \right] \tag{3.3}$$

unde pătratul mediei locale a imaginii marcate este dat de un estimat de plauziobilitate maximă, ML (Maximum-Likelihood). Toţi parametrii locali de mai sus pot fi estimaţi folosind o fereastră locală de dimensiuni 5×5.

Această metodă de *denoising* poate fi aplicată asupra cadrelor în domeniul spaţial sau într-un context multirezoluţie, bazat pe transformata *wavelet*. În acest caz, filtrarea Wiener adaptivă se aplică la fiecare subbandă *wavelet* şi imaginea atacată este reconstruită din descompunerea *wavelet*.

Ca o măsură posibilă împotriva atacurilor de filtrare este folosirea eficientă a redundanţei şi a diversităţii. Marcajul poate fi trimis prin mai multe canale de transmisie, iar la detecţie se face o combinare optimală, astfel încât rata erorilor să scadă [KH01], aşa cum se vede în Figura 3.5.

3.4.3 Atacul prin adăugare de zgomot

Zgomotul adăugat introduce distorsiuni imperceptibile, chiar la un raport semnal pe zgomot mic, de 20 dB, iar impactul negativ asupra detecţiei marcajului este nesemnificativ.

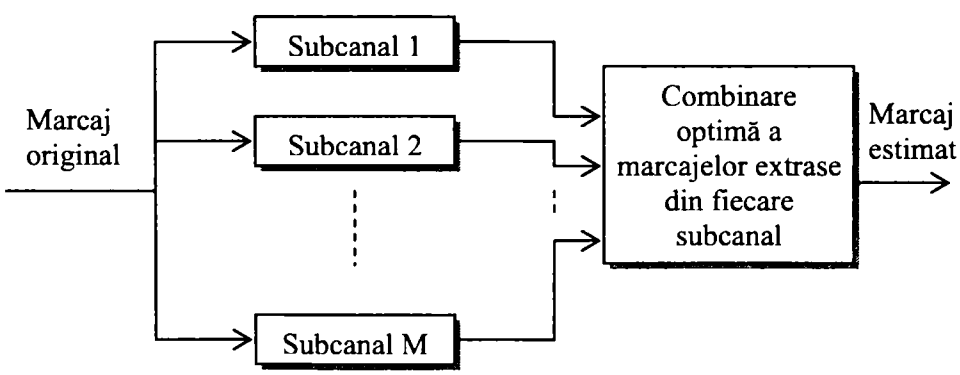


Fig 3.8: Folosirea diversităţii şi a combinării repetiţiilor marcajului în mod optim.

Soluţiile posibile împotriva atacului prin zgomot AWGN sunt codurile corectoare de erori precum şi folosirea diversităţii şi a combinării repetiţiilor marcajului în mod optim.

3.4.4 Atacurile geometrice

Atacurile geometrice au ca obiectiv desincronizarea detectorului, pentru ca acesta să nu găsească marcajul. Atacurile geometrice posibile sunt: translaţia, rotaţia, redimensionare (scaling), respectiv combinaţii ale acestora; curbarea neliniară a imaginii; ştergere şi înserare de cadre (în cazul semnalelor video).

Atacurile geometrice se împart în două categorii: globale sau staţionare, respectiv locale. În cazul atacurilor geometrice *globale* noile valori ale pixelilor se obţin astfel:

$$\hat{Y}_n(i,j) = Y_n\left(T(i,j)\right), \tag{3.4}$$

unde T este transformarea (atacul) respectiv. În continuare se prezintă câteva astfel de atacuri şi transformările care le corespund.

- atac RST,

$$T(i,j) = \begin{bmatrix} k\cos\theta & k\sin\theta & t_x \\ -k\sin\theta & k\cos\theta & t_y \end{bmatrix} \begin{bmatrix} i \\ j \\ 1 \end{bmatrix} \tag{3.5}$$

- atac de tip translaţie ciclică (cyclic shift),

$$\hat{Y}_n(i,j) = Y_n\left(i + \Delta_x \bmod M, j + \Delta_y \bmod N\right) \tag{3.6}$$

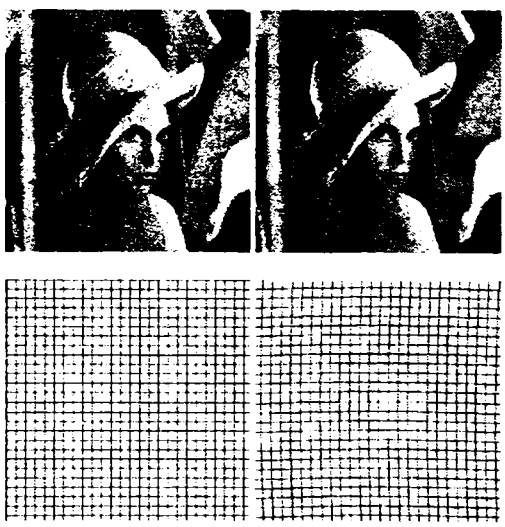


Fig. 3.9: Atac jitter, Stirmark. Stânga: imaginea originală (sus), matricea asociată (jos). Dreapta: imaginea după atac (sus), „matricea" asociată (jos). Efectul atacului este vizibil numai asupra matricii asociate.

Atacurile *locale* (de tip Stirmark [PAK98]) profită de faptul că sistemul vizual uman nu este sensibil la translaţii şi modificări afine locale. Pixelii sunt translataţi şi redimensionaţi local, fără a introduce distorsiuni vizibile.

Robusteţea împotriva transformărilor afine *globale* este asigurată prin folosirea unui domeniu invariant la acestea (cum este transformata Fourier-Mellin), folosirea unui marcaj de referinţă, sau folosirea marcajelor periodice, a căror funcţie de autocovarianţă, ACF, permite estimarea distorsiunilor. Asigurarea robusteţii împotriva atacurilor *locale* introduse de programe ca şi Stirmark este încă nesoluţionată. Un exemplu de atac de acest tip este prezentat în Figura 3.9.

În cazul marcării neinformate, folosirea unor metode eficiente de înregistrare poate asigura robusteţea la atacurile geometrice.

Un marcaj trebuie să fie robust nu numai la tehnicile de compresie cu pierderi, dar şi la transformările geometrice ca scalare, decupare, rotire, etc. Transformările geometrice afectează în mică măsură calitatea imaginii, dar afectează în mare măsură marcajele plasate cu ajutorul metodelor descrise anterior. Deoarece transformările geometrice afectează în mod tipic sincronizarea dintre modelul pseudo-aleator al marcajului şi imaginea marcată, sincronizarea trebuie redobândită înainte ca detectorul să înceapă calculul corelaţiilor.

Cea mai la îndemână metodă de a obţine invarianţa la translaţie (shift), este modulaţia de amplitudine a coeficienţilor DFT. Dacă, dintr-o anumită cauză, este preferat un alt domeniu pentru plasarea marcajului şi este nevoie şi de invarianţă la schimbări de poziţie, se poate adăuga un marcaj (semn) în domeniul spaţial pentru a determina translaţia. Acest semn poate fi un model pseudo-aleator, ca şi marcajul transparent însăşi. Detectorul determină prima oară poziţia spaţială a acestui marcaj, prin mişcarea lui peste toate locaţiile posibile din imagine, şi apoi calculând corelaţia dintre aceasta şi porţiunea de imagine corespunzătoare. Translaţia cu corelaţia cea mai mare defineşte poziţia spaţială a semnului. În final, imaginea este mişcată înapoi în poziţia sa originală, şi aplicată procedura normală de detecţie a marcajului.

O căutare completă a acestui marcaj (semn), este foarte anevoioasă din punct de vedere al calculelor. De aceea, în [KDHM99], este propusă o altă metodă: adăugarea unui model pseudo-aleator în imagine de două ori, dar în diferite locuri. Aici conţinutul marcajului transparent, adică biţii marcajului sunt plasaţi în poziţii relative a două modele de marcaj. Pentru a detecta marcajul transparent, detectorul calculează corelaţia de fază dintre imagine şi modelul de marcaj, folosind transformarea Fourier rapidă (FFT), şi detectează cele două vârfuri de corelaţie a celor două modele. Conţinutul marcajului transparent derivă din poziţiile relative ale vârfurilor. Dacă toată imaginea e deplasată înainte de detecţie, poziţiile absolute ale vârfurilor de corelaţie se schimbă, dar poziţiile relative rămân neschimbate, lăsând biţii marcajului detectabili.

În [FH97], este propusă o metodă în care se adaugă o grilă la o imagine, care poate fi folosită pentru a scala, roti, şi translata înapoi imaginea în poziţia şi mărimea originală. Grila este reprezentată de o sumă de semnale sinusoidale, care apar ca maxime în domeniul de frecvenţă FFT. Aceste vârfuri sunt folosite pentru a determina distorsiunile geometrice.

În [KP99], este propusă o metodă care plasează un model pseudo-aleator de mai multe ori, la diferite locaţii, în domeniul spaţial al unei imagini. Detectorul estimează marcajul W' , prin aplicarea unui filtru trece sus F_{HP} asupra imaginii marcate:

$$W' = I_W \otimes F_{HP}$$

$$F_{HP} = \frac{1}{12} \cdot \begin{bmatrix} 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ -1 & -1 & -1 & 12 & -1 & -1 & -1 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 \end{bmatrix}.$$

În final, este calculată funcţia de autocorelaţie a marcajului estimat W'. Această funcţie va avea valori maxime în centru şi în poziţiile marcajelor înserate de mai multe ori. Dacă imaginea a fost supusă unei transformări geometrice, vârfurile din funcţia de autocorelaţie vor reflecta aceeaşi transformare şi deci, vor furniza o grilă care poate fi folosită pentru a transforma înapoi imaginea, la mărimea şi orientarea originală.

În [HPRP98] şi în [HRPP98], se propune o metodă care plasează marcajul într-un domeniu invariant la rotire, scalare, şi translaţie, folosind o combinaţie dintre transformata Fourier discretă, DFT, şi reprezentarea polară logaritmică, LPM, aşa cum s-a văzut în capitolul 2. Mai întâi este calculată amplitudinea coeficienţilor DFT pentru a obţine un domeniu invariant la translaţii. În pasul următor, pentru fiecare coordonată (u,v) al amplitudinilor DFT este determinat un punct corespunzător (μ,θ) în LPM:

$$u = e^{\mu}\cos(\theta);\ \ v = e^{\mu}\sin(\theta)$$

Acest sistem de coordonate polar logaritmic (LPM) transformă rotirea şi scalarea, în translaţii de-a lungul axei orizontale şi verticale. In continuare, prin folosirea amplitudinii DFT a coordonatelor LPM, se obţine un domeniu invariant la rotire, scalare şi translaţie. În acest domeniu se poate adăuga un marcaj transparent CDMA, de exemplu prin modularea coeficienţilor, folosind relaţia:

$$|I_W(u,v)| = |I(u,v)| \cdot (1 + k \cdot W(u,v)).$$

În practică, implementarea schemei s-a dovedit a fi dificilă. De aceea autorii propun o abordare diferită, unde un marcaj transparent CDMA este plasat în domeniul amplitudinii DFT invariante la translaţii. Pentru a face marcajul transparent invariant la scalare şi rotire, se plasează un al doilea marcaj transparent ca şablon, în acest domeniu. Pentru a extrage marcajul transparent, Mai întâi se determină scara şi orientarea imaginii marcate prin folosirea şablonului după cum urmează:

-Este calculată transformata DFT a imaginii marcate

-Sunt calculate coordonatele LPM ale amplitudinilor coeficienţilor DFT şi ale modelului şablonului

-Sunt calculate „offset"-urile orizontale şi verticale dintre cele două LPM, folosind tehnici de căutare şi intercorelaţie, rezultând un factor de scalare şi rotire.

În final, imaginea este transformată înapoi la mărimea şi orientarea originală, şi este extras marcajul purtător de informaţie.

Pentru a combate efectele atacurilor StirMark, pentru imaginile color, în metoda *canalelor duale*, imaginea este împărţită în două canale, unul pentru sincronizare şi unul pentru înserare [Ker01]. Transformata wavelet complexă a fost propusă ca domeniu de înserare [LK00] pentru a creşte robustetea la transformări geometrice.

3.4.5 Atacurile de tip protocol

Atacurile de tip protocol periclitează întregul concept al sistemului de marcare transparentă. Exemple sunt:

- *atacul de ambiguitate sau inversiune*. Atacatorul extrage un marcaj propriu din semnalul marcat, rezultând un semnal pseudo-gazdă, care atunci când este folosit în detecţia informată, va permite atacatorului detecţia marcajului. Astfel apare incertitudinea cu privire la identitatea deţinătorului drepturilor de autor [CMYY98]. Pentru protejarea copyright-ului, marcajele trebuie să fie neinversabile. Cu alte cuvinte un atacator nu ar trebui să poată extrage o marcă din semnalul multimedia marcat. O soluţie la această problemă este ca marcajul să fie dependent de semnalul original printr-o funcţie *one-way*, neinversabilă.
- *atacul de copiere*, care estimează marcajul dintr-un semnal marcat şi îl inserează într-un alt semnal, numit semnal *ţintă*. Acest tip de atac este aplicabil dacă poate fi produs în semnalul ţintă un marcaj valid fără cunoaşterea sistemului de marcare sau a cheii. Din nou, marcajele dependente de semnalul original pot fi rezistente la atacul de copiere. Atacul este gândit împotriva autentificării.
- *atacul mozaic* împarte semnalul astfel încât el este afişat ca o entitate, dar detecţia marcajului nu este posibilă. Acest atac este de tip Stirmark. În Figura 3.10 se dă un exemplu pentru funcţionarea acestui tip de atac.
- *atacul de re-marcare,* în care o imagine marcată va fi re-marcată cu un alt sistem, creând confuzie asupra primului marcaj înserat. O posibilă contramăsură ar fi ca generarea marcajelor să depindă de momentul de timp (*time-stamping*).

Fig. 3.10: Atacul Mozaic. Imagine originală şi cea segmentată în subimagini cu programul 2Mosaic [PAK98].

Soluţiile posibile împotriva acestor tipuri de atacuri presupun stabilirea unor reguli de construire a sistemului de marcare, pentru a le combate pe cele cunoscute, cum ar fi folosirea marcajelor non-inversabile, în cazul atacului de ambiguitate [CMYY98]. O altă posibilitate este folosirea unui detector flexibil.

3.4.6 Atacurile de tip criptografic

Atacurile de tip criptografic au ca ţintă elemente criptografice din sistemul de marcare transparentă. Ele folosesc metode standarde de criptanaliză pentru atacarea sistemului:

- căutarea prin „forţă brută" a mesajului înserat;

- estimarea cheii;
- atacul Oracle: pentru marcaje rezistente la falsificare, detectorul este disponibil, astfel că se poate deduce modul de înlăturare a marcajului. Oracolul produce un răspuns DA sau NU la întrebarea „este imaginea marcată ?" şi eventual dă şi informaţii suplimentare, ca de exemplu coeficientul de intercorelaţie.

Într-un sistem criptografic, există diferite nivele de securitate:

- *Securitatea necondiţionată* – sistemul nu poate fi spart, chiar şi cu putere de calcul nelimitată, deoarece adversarul nu deţine destule informaţii. Aceasta presupune o măsură teoretică informaţională numită secret perfect,
- *Securitatea cu complexitate teoretică*: modelul atacatorului (puterea de calcul polinomială) este folosit pentru a dovedi ineficienţa atacului; în cel mai rău caz această analiză are o valoare practică aproape nulă,
- *Securitatea practică (demonstrabilă)* se referă la o situaţie în care complexitatea spargerii sistemului poate fi redusă prin rezolvarea unei probleme matematice presupuse dificile,
- *Securitatea computaţională* presupune că un atac asupra sistemului nu este fezabil din cauza puterii de calcul; cel mai bun atac trebuie perceput ca acela care depăşeşte puterea de calcul a atacatorului,
- *Securitatea ad-hoc*: argumentele despre resursele insuficiente ale unui atacator de a sparge mecanismele existente de securitate sunt expuse într-un mod convingător. Aceasta este cea mai răspândită abordare pentru studiul securităţii unui protocol.

O măsură posibilă împotriva acestui tip de atacuri este folosirea unor primitive de criptare bine construite.

3.4.7 Atacurile de estimare

O altă categorie de atacuri sunt cele de estimare. În aceste cazuri, se estimează *marcajul* sau *semnalul gazdă*, fără a cunoaşte cheia secretă, folosind informaţii despre statistica marcajului, respectiv a semnalului gazdă. Aceste atacuri sunt aplicabile când marcajul a fost înserat în mod redundant, sau când avem la dispoziţie mai multe copii marcate. În Figura 3.11 este prezentat atacul prin estimarea marcajului.

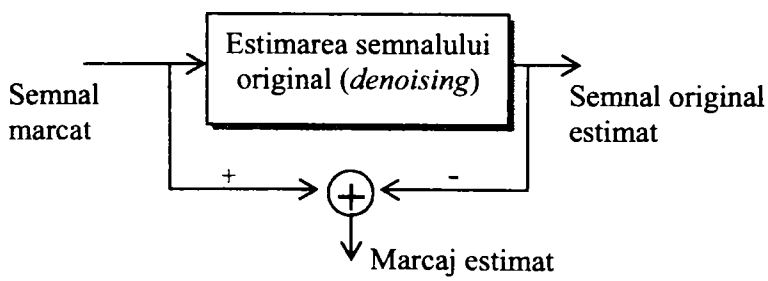


Fig. 3.11: Atac prin estimarea marcajului

Depinzând de scopul final al atacului, atacatorul poate estima marcajul sau semnalul gazdă folosind algoritmii ML (Maximum-Likelihood), MAP (Maximum A Posteriori), sau MMSE (Minimum Mean Square Error). Atacurile de estimare pot fi considerate de eliminare, de protocol, sau de desincronizare, funcţie de scopul în care este folosit semnalul estimat.

La *estimarea semnalului gazdă*, marcajul este considerat ca zgomot în semnalul marcat. Acest atac este echivalent cu proiectarea unei scheme de *denoising* optimal. Dacă se ia în considerare legătura strânsă între *denoising* şi compresie, atunci atacatorul poate folosi un codor bazat pe transformata *wavelet* cu un raport rată-distorsiune optim.

Cu alte cuvinte, estimarea gazdei se face prin *denoising* optimal, sau compresie perfectă. Aceste două operaţii sunt considerate atacuri de eliminare.

Estimarea marcajului se face folosind algoritmii de estimare ML, MAP, MMSE. În urma estimării, se extrage semnalul gazdă estimat din semnalul marcat.

3.4.8 Atacul de remodulare

Cu marcajul estimat, un atacator poate *să remoduleze o imagine*: se extrage marca estimată din imaginea marcată (modulare negativă). Un exemplu de atac de remodulare este prezentat în Figura 3.12. În cazul unui detector cu corelaţie, prin aceste acţiuni se anulează corelaţia pozitivă, cu condiţia ca marcajul estimat să fie asemănător cu cel original. Pe de altă parte, prin extragerea unei versiuni amplificate a marcajului estimat, detectorul prin corelaţie nu va reuşi să găsească marcajul în imaginea atacată. Pentru acest motiv, se introduce un câştig $\gamma \geq 1$ care reprezintă compromisul între distorsiunea structurii de date atacată, respectiv succesul atacului [VPPE01].

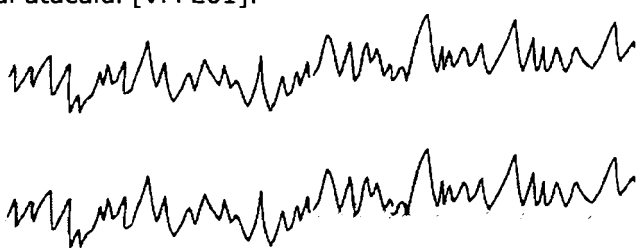


Fig. 3.12: Atac prin remodulare.

Există patru variante ale atacului de remodulare. Pentru câştigul $\gamma = 1$ se obţine un estimat MMSE/MAP şi atacul se reduce la *denoising*. Pentru câştigul $\gamma > 1$ deşi calitatea documentului atacat este redusă, performanţa detecţiei prin corelaţie scade sensibil. Detectorul poate decide chiar că imaginea nu a fost marcată dacă corelaţia ajunge la 0. A treia variantă este folosirea unei măşti perceptuale în loc de un câştig fix, pentru a controla vizibilitatea distorsiunilor introduse.

Ultima variantă a atacului de remodulare este ca atacatorul să scadă estimatul marcajului ponderat de masca perceptuală, dar şi să adauge puncte dispersate (*outliers*), pentru a obţine distribuţia unui zgomot non-gaussian, fapt care, din nou, scade performanţa detecţiei prin corelaţie [VPPE01]. În plus, folosind proprietăţile sistemului vizual uman, acest zgomot poate fi introdus în părţi mai puţin semnificative perceptual. Această tehnică se numeşte *remodulare perceptuală* [VSA00]. Ea este exemplificată în Figura 3.13.

Atacul de estimare poate fi folosit pentru implementarea atacului de copiere, menţionat mai sus. Desigur, marcajul copiat trebuie să fie adaptat la semnalul ţintă pentru a păstra calitatea semnalului marcat în mod fals. Pentru imagini, se poate exploata sensibilitatea la contrast şi fenomenul de mascare a texturilor specifice

sistemului vizual uman. Atacul de copiere bazat pe estimare are succes dacă este folosit acelaşi model perceptual ca pentru algoritmul original de marcare. Atacul descris este potrivit unei scheme de marcare aditivă. În cazul sistemelor bazate pe cuantizare, chiar şi un estimat perfect al marcajului nu poate fi copiat, deoarece este foarte puţin probabil ca semnalul copiat w să fie un marcaj valid pentru semnalul ţintă. În Figura 3.14. este prezentat un sistem de implementare a atacului prin copiere.

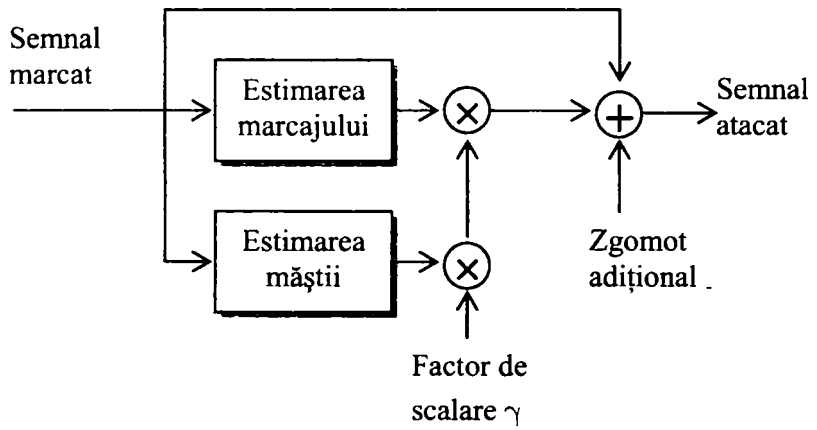


Fig. 3.13: Atac prin estimarea marcajului, remodulare perceptuală.

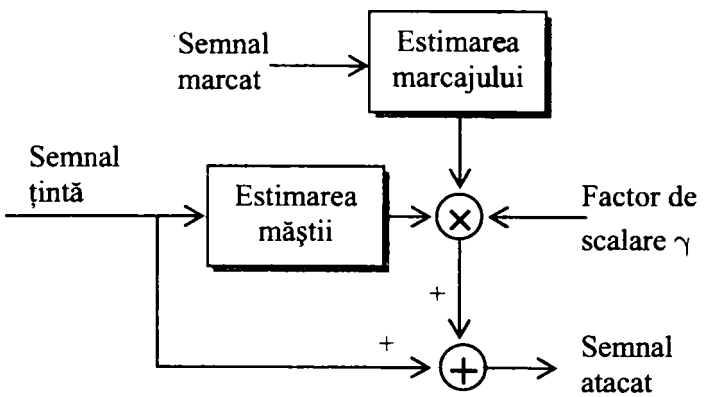


Fig. 3.14: Atac prin copiere

3.4.9 Atacul de estimare în desincronizare

Atacul prin estimarea marcajului poate fi eficient şi în desincronizare. Ideea de bază este căutarea marcajelor care asigură sincronizarea, eliminarea acestora, şi apoi aplicarea unor tehnici de desincronizare, cum sunt transformările globale afine, pentru imagini.

Ne referim în continuare la atacul metodelor de sincronizare prin înserarea unui marcaj de referinţă în spectrul de amplitudini al imaginii, sau prin generarea unor marcaje periodice, care pot fi detectate prin autocovarianţă. În ambele cazuri, maximele sunt generate în domeniul transformatei Fourier [VSA00, VSA01], după

cum se vede în Figura 3.15. Aceste vârfuri pot fi detectate, următorul pas fiind interpolarea spectrului imaginii marcate.

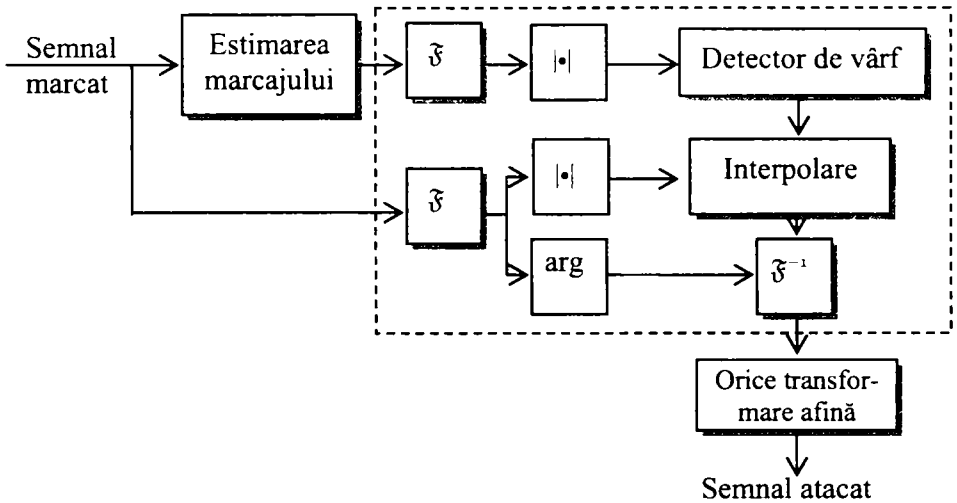


Fig. 3.15: Estimarea marcajului folosită în atacul de desincronizare.

3.4.10 Măsuri împotriva atacurilor prin estimare

Pentru a fi robust în faţa acestor atacuri, marcajul trebuie să fie dificil de estimat. Există două abordări.

În prima abordare [SG99], marcajul trebuie să îndeplinească *condiţia densităţii spectrale de putere* PSD (Power spectral Density). Se are în vedere situaţia ideală din punct de vedere teoretic, când semnalul original şi marcajul sunt tratate ca procese aleatoare, gaussiene colorate, staţionare, independente, de medie nulă. Deoarece semnalul original este dat, se presupune că are o PSD fixă, în timp ce PSD a marcajului poate fi variabilă. Întrebarea este ce formă trebuie să aibă aceasta din urmă pentru ca marcajul să fie rezistent la atacurile prin estimare? În acest prim caz, estimatul optimal este obţinut prin filtrare Wiener.

Eroarea medie pătratică E, între marcajul original şi cel estimat, este o măsură bună pentru rezistenţa marcajului la atacul de estimare. Se poate arăta că E este maximă dacă şi numai dacă densitatea spectrală de putere a marcajului este direct proporţională cu cea a semnalului.

Această cerinţă se numeşte *condiţia densităţii spectrale de putere*. Pentru orice ieşire a filtrului adaptat, un marcaj care îndeplineşte această condiţie face ca atacul de estimare să inducă cea mai mare distorsiune.

Pentru ca valoarea corelaţiei să ajungă la zero, atacul ar trebui să introducă distorsiuni cu puterea egală cu a semnalului original; prin urmare semnalul atacat nu va avea valoare comercială.

A doua abordare foloseşte *funcţia de vizibilitate a zgomotului*. În marcarea imaginii, eliminarea zgomotului (*denoising*) este o cale naturală de a dezvolta atacuri bazate pe estimare, optimizate pentru modelul statistic al imaginilor [SVA99]. Imaginea marcată este văzută ca o versiune zgomotoasă a imaginii originale, iar marcajul reprezintă zgomotul care ar trebui estimat. Astfel, marcajul estimat este acelaşi cu zgomotul estimat. După eliminarea zgomotului, se consideră un anumit model statistic pentru imaginea originală. Rezultă o *funcţie de mascare a*

texturilor, TMF (Texture Masking Function), dependentă de imagine, cu valori între 0 şi 1. Pentru a însera un marcaj dificil de estimat, procesul de înglobare ar trebui să folosească funcţia inversă acesteia, numită funcţia de vizibilitate a zgomotului: NVF = 1 - TMF. Valorile de 1 ale funcţiei NVF indică regiuni plate, unde marcajul ar trebui atenuat, iar valorile de 0 ale NVF indică texturi şi muchii, unde marcajul trebuie amplificat.

Prima abordare poate da rezultate mai slabe, deoarece modelul statistic folosit nu este potrivit imaginilor. Cu toate acestea, rezultatele obţinute cu prima abordare sunt asemănătoare cu cele obţinute cu a doua abordare. Aceasta este în concordanţă cu argumentarea euristică a lui Cox ş.a. [CKLS97], care susţine că marcajul trebuie plasat în "componentele perceptual semnificative" ale unei imagini.

Robusteţea marcajului poate fi îmbunătăţită prin creşterea energiei marcajului. Totuşi, creşterea energiei conduce la degradarea calităţii imaginii. Prin exploatarea proprietăţilor HVS, energia poate fi crescută local în locurile unde marcajul nu este remarcat de ochiul uman. Deci, prin exploatarea HVS, se pot plasa marcaje invizibile perceptual, care au energie mai mare ca în cazul distribuţiei uniforme a acestei energii asupra imaginii.

Aprecierea calităţii imaginilor, pentru compresia măsurată relativ la imaginea originală necomprimată, conţine aspecte subiective [BA99]:

1 Vizibilitatea erorilor în imaginea comprimată depinde foarte mult de localizare, de exemplu dacă sunt în arii foarte netede sau foarte texturate.

2 Importanţa vizuală a erorilor depinde de localizarea în imaginea originală, de exemplu, erorile pe contururile sau pe faţa unui portret vor afecta recunoaşterea, mai mult decât erorile în fundal.

Aceste aspecte pot fi exploatate şi în procesul de marcare transparentă.

Pentru ca un semnal vizual să fie perceput, trebuie să aibă o cantitate minimă de contrast, care depinde de luminozitatea şi frecvenţa medie. Pe deasupra, un semnal de anumită frecvenţă poate masca un semnal perturbator de frecvenţă similară [Wan95], [BBCP98a]. Efectul de mascare este deja folosit în marcajul DCT dependent de imagine, descris în capitolul 2, unde coeficienţii DCT sunt modulaţi cu ajutorul formulei (2.4). Aici, la fiecare sinusoidă din imagine (semnal de mascare), este adăugată o altă sinusoidă (marcajul), având amplitudinea proporţională cu semnalul de mascare. Dacă factorul de câştig *k* este ales corespunzător, se produce mascarea de frecvenţă.

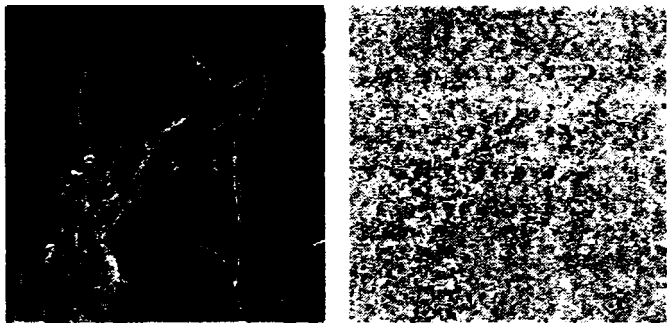
Sistemul vizual uman este mai puţin sensibil la schimbări în regiunile cu luminozitate mare. Acest lucru poate fi exploatat prin alegerea factorului de câştig a marcajului dependent de luminozitate. Deoarece ochiul uman este cel mai puţin sensibil la culoarea albastră, un marcaj perceptual invizibil, plasat în canalul albastru, poate conţine mai multă energie ca un marcaj perceptual invizibil plasat în canalul de luminozitate a unei imagini color [KJB97].

În jurul marginilor şi porţiunilor cu texturi a unei imagini, sistemul vizual uman este mai puţin sensibil la distorsiuni, decât în porţiunile netede. Acest efect se numeşte mascare spaţială, şi poate fi folosit pentru marcare, prin creşterea locală a energiei marcajului în aceste porţiuni mascate ale imaginii [MQ95]. Tehnicile de bază pentru marcarea spaţială descrise anterior, pot fi extinse prin mascare spaţială, de exemplu, folosind următoarea funcţie de modulaţie:

$$I_W(x,y) = I(x,y) + Msk(x,y) \cdot k \cdot W(x,y)$$

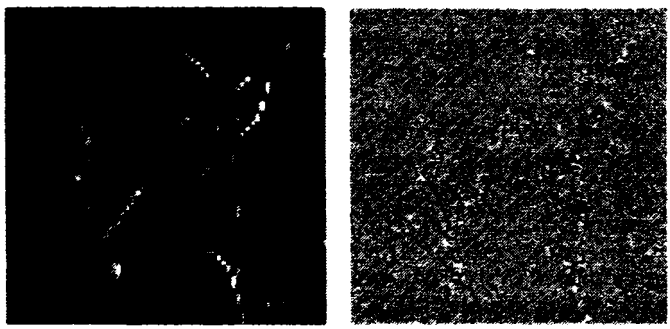
Aici, W(x,y) reprezintă marcajul pseudo-aleator bidimensional, *k* reprezintă factorul de câştig fix, şi Msk(x,y) reprezintă imaginea mască. Valorile măştii se întind de la 0 la k'_{max} şi dau o măsură a insensibilităţii la distorsiuni pentru fiecare punct

corespunzător în imaginea originală I(x,y). O metodă de a genera imaginea mască Msk, este filtrarea imaginii originale cu un filtru Laplace trece-sus şi reţinerea valorilor absolute a imaginii filtrate rezultate [KDHM99]. În figura 3.16(a) este arătată o mască pentru imaginea Lena, care este generată de un simplu detector de margini Prewitt. Figura 3.16(b) arată marcajul puternic amplificat modulat cu această mască.



(a) (b)

Fig. 3.16: Marcare folosind masca bazată pe operatori Prewitt. (a) Mască, şi (b) Diferenţa $W(x,y)=I(x,y)-I_W(x,y)$



(a) (b)

Fig. 3.17: Marcare folosind o imagine mască pe baza energiei DCT-AC. (a) Imaginea mască, şi (b) Diferenţa $W(x,y)=I(x,y)-I_W(x,y)$

O altă metodă pentru generarea imaginii mască este folosirea sumei pătratelor coeficienţilor DCT-AC de 8x8 [NCH99]. Figura 3.17 (a) arată o mască generată folosind această energie DCT-AC, pentru imaginea Lena. Figura 3.17(b) prezintă marcajul puternic amplificat modulat cu această mască. Experimentele arată că un marcaj invizibil, modulat cu un factor de câştig adaptat local la o asemenea mască, poate conţine de două ori mai multă energie ca un marcaj invizibil, modulat cu un factor de câştig fix.

Mascarea spaţială poate fi aplicată şi atunci când marcajul e plasat în alt domeniu, cum ar fi DFT, DCT [BBCP98b], sau DWT. În acest caz, mai întâi este plasat marcajul nespaţial într-o imagine I, rezultatul fiind o imagine temporară notată cu I_{Wt}. Imaginea marcată I_W este acum construită prin mixarea imaginii originale I şi a acestei imagini temporare I_{Wt}, cu ajutorul unei imagini mască Msk:

$$I_W(x,y) = (1 - Msk(x,y)) \cdot I(x,y) + Msk(x,y) \cdot I_{Wt}(x,y)$$

Aici imaginea mască trebuie scalată la valori în domeniul 0 la 1.

3.4.11 Atacurile dependente de statistica locală a semnalului

Mai multe atacuri de estimare pot fi combinate cu succes în funcţie de statistica locală a semnalului. Atacatorul poate estima marcajul folosind proprietăţi ale sistemului vizual uman şi diferite modele statistice ale imaginilor.

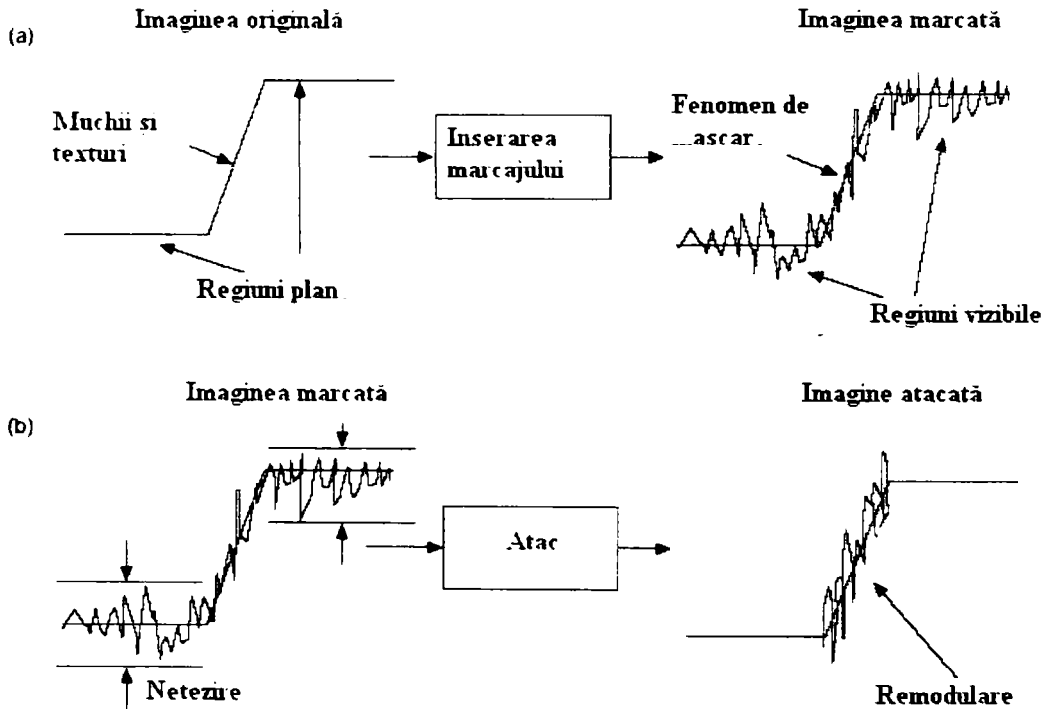


Fig. 3.18: a) Strategia folosită la marcare, prin exploatarea funcţiei de mascare a sistemului vizual uman; b) Strategia atacatorului folosind denoising şi remodulare perceptuală.

Marcajul poate fi estimat şi eliminat cu uşurinţă din regiunile plate ale imaginii, mai degrabă decât din texturi şi muchii. Modelul stochastic pentru texturi şi muchii este nestaţionar şi deci relativ complicat de folosit în cazul în care se doreşte o estimare precisă. De aceea, atacatorul va încerca să folosească pe cât posibil avantajele *denoising*-ului, eliminând marcajul din regiunile plate fără a introduce distorsiuni vizibile, şi chiar îmbunătăţind raportul PSNR. Pe de altă parte, atacatorul va folosi remodularea cu putere crescută în regiunile de texturi şi de muchii, care sunt mascate de sistemul vizual uman. În acelaşi timp, atacatorul poate folosi funcţia de vizibilitate a zgomotului NVF (Noise Visibility Function), pentru a determina automat aceste regiuni [VSA00, VSA01]. Atacul este prezentat în Figura 3.18.

3.4.12 Atacurile optimizate

Până acum, am enumerat atacurile bazate pe estimare, şi soluţiile posibile pentru a le combate. Cu toate acestea, mai există moduri în care sistemul de marcare poate să reacţioneze la atacurile bazate pe estimare, în special la remodulare.

Detectorul poate estima marcajul remodulat şi să încerce să inverseze remodularea, obţinând astfel o detecţie sigură a marcajului. De exemplu, când estimarea marcajului se face prin filtrare Wiener, detectorul poate aplica o filtrare Wiener inversă. Evident, acest lucru nu este dorit de atacator. De aceea, el trebuie să adauge zgomot la semnalul atacat, care ar fi amplificat de filtrarea Wiener inversă, şi astfel performanţa detectorului scade.

Atacatorul trebuie să găsească o combinaţie bună între folosirea marcajului estimat şi a zgomotului care trebuie adăugat. Sistemul de marcare nu numai că trebuie să facă estimarea marcajului dificilă, dar şi puterea marcajului să fie mai mare decât cea a zgomotului aditiv pe care un atacator l-ar putea introduce.

Problema poate fi formulată într-un mod şi mai general: atacatorul încearcă să minimizeze capacitatea marcajului sub constrângerea distorsiunilor introduse de atac, în timp ce sistemul de marcare încearcă să maximizeze capacitatea marcajului, sub constrângerea distorsiunilor introduse de marcare. Această situaţie poate fi privită ca un "joc" între atacator şi sistemul de marcare. Pentru a rezolva această problemă, se foloseşte o abordare din teoria informaţiei, care presupune că adversarii îşi cunosc comportarea [SEG01, MOS03].

Din punctul de vedere al teoriei informaţiei, marcarea este un joc dintre atacator şi marcator. Funcţia de cost este informaţia mutuală între intrarea şi ieşirea canalului de atac, atacatorul încearcă să o minimizeze în timp ce marcatorul încearcă să o maximizeze. Limita superioară a acestei informaţii mutuale este capacitatea marcajului. Cu alte cuvinte, cel mai bun atac este echivalent cu cea mai eficientă compresie posibilă, cu constrângerea dată de distorsiunile introduse, iar strategia optimă de marcare este codarea optimă a canalului când atacatorul cunoaşte caracteristica canalului.

Considerând cazul în care semnalul original şi marcajul sunt procese aleatoare gaussiene colorate, staţionare, independente şi de medie nulă, densitatea spectrală de putere a marcajului este independentă de câtă distorsiune poate fi introdusă de atacator. La nivele scăzute de distorsiune, marcajele de tip zgomot alb se comportă aproape optimal, în timp ce la distorsiuni mari, marcajele care îndeplinesc condiţia densităţii spectrale de putere sunt mai potrivite. Marcajele înserate în componente ale semnalului cu dispersie mare sunt eliminate mai eficient de zgomotul aditiv. Pentru a aplica aceste rezultate în marcarea transparentă, ar trebui folosite descompuneri bune ale semnalului, care-l separă în componente cu statistică diferită. În cazul imaginilor, descompunerea *wavelet* ar putea fi o alegere bună.

3.4.13 Atacurile ce folosesc mai multe cadre din secvenţa video (multiple-frames)

Aceste atacuri sunt specifice secvenţelor video, şi exploatează informaţia temporală disponibilă de la cadru la cadru într-o secvenţă video. Cele mai multe cadre sunt puternic corelate între ele, în special în scene statice sau cvasi-statice. Această corelare se manifestă şi între marcajele înserate în cadrele respective, ceea ce rezultă într-o redundanţă temporală a secvenţei video, precum şi a secvenţei marcajelor. Ideea care stă la baza atacurilor statistice este exploatarea acestei redundanţe pentru a elimina marcajul. În comparaţie cu atacurile asupra imaginilor marcate, atacurile asupra secvenţele video au nevoie de multe cadre pentru a fi eficiente. Aceste atacuri se pot face prin medierea mai multor cadre pentru a estima semnalul gazdă sau marcajul. Există două cazuri posibile:

1. marca înserată este diferită la fiecare cadru (atac de *mediere*), sau dimpotrivă,
2. marca înserată este aceeaşi pentru fiecare cadru (atac de *coliziune*).

Prin urmare, medierea va amplifica una dintre componente, semnalul gazdă original în primul caz, sau marcajul original în al doilea caz, şi va atenua cealaltă componentă [Kun05, DCP00].

- **Atacul de mediere**

Acesta este un atac foarte simplu, bazat pe faptul că nişte cadre consecutive din secvenţa video sunt asemănătoare, mai ales pentru scenele statice. Se presupune că marcajele în cadre diferite sunt *necorelate*. Medierea poate fi văzută ca o filtrare temporală trece-jos a semnalului video marcat, folosind o fereastră alunecătoare de L cadre, care calculează estimatul semnalului video original:

$$\hat{x}_t = \frac{1}{L}\sum_{k=t}^{t+L-1} y_k = \frac{1}{L}\sum_{k=t}^{t+L-1} x_k + \frac{1}{L}\sum_{k=t}^{t+L-1} n_k \qquad t = 1...N_f \tag{3.7}$$

unde $\hat{x}_t$ este cadrul estimat t din semnalul video original, iar y_k este cadrul k din semnalul video marcat. Dacă L nu este prea mare, cadrele sunt asemănătoare şi $\sum x_k$ tinde către un cadru mediu, în timp ce $\sum n_k$ scade spre 0 dacă marcajele sunt independente de la un cadru la altul. În Figura 3.14 este prezentat un atac de mediere. Aceste atacuri păstrează calitatea în scenele statice. Distorsiuni vizibile apar în scenele în mişcare, unde ar trebui folosit un L mai mic.

- **Atacul de coliziune (estimare)**

Problema care apare la medierea printr-o fereastră alunecătoare a cadrelor este că nu funcţionează bine când marcajele sunt corelate în cadre consecutive. Cel mai defavorabil caz apare când acelaşi marcaj este înserat în toate cadrele. În acest caz, un atac mai potrivit este cel de coliziune, care foloseşte redundanţa marcajului în loc de cea a semnalului video. Presupunând că toate cadrele sunt independente, dar au înserate aceeaşi marcă în ele, se estimează marcajul din aceste cadre diferite din *toată* secvenţa video, cu scopul de a-l elimina.

Totuşi, energia cadrelor este mult mai mare decât energia marcajului, şi o simplă mediere nu va da un estimat bun al marcajului. Soluţia este estimare marcajului din fiecare cadru, ca $\hat{n}_t$, de exemplu, dintr-un cadru $\hat{x}_t$ din care zgomotul a fost eliminat, folosind un filtru Wiener, calculând diferenţa $\hat{n}_t = y_t - \hat{x}_t$. Aceste estimări sunt apoi mediate pentru a obţine o aproximare mai bună a marcajului original:

$$\hat{n} = \frac{1}{N_f}\sum_{t=1}^{N_f} \frac{1}{\sigma_{\hat{n}_t}} \hat{n}_t \tag{3.8}$$

unde $\sigma_{\hat{n}_t}$ este deviaţia standard a lui $\hat{n}_t$. Estimatul final al marcajului, $\hat{n}$ poate fi eliminat printr-o scădere din fiecare cadru:

$$\hat{x}'_t = y_t - s \cdot p_t \cdot \hat{\sigma}_{n_t} \cdot \hat{n} \qquad t = 1...N_f \tag{3.9}$$

unde $\hat{\sigma}_{n_i}$ este deviaţia standard globală a zgomotului, estimată din fiecare cadru, iar *s* este un coeficient ales experimental. Scopul acestor factori este de a adapta semnalul, care va fi extras, la energia marcajului care trebuie eliminat, ţinând cont de adaptabilitatea conţinutului. p_i este o variabilă aleatoare cu valori posibile 1 sau 0, cu probabilităţile respective p şi 1-p. Aceasta provine din faptul că un zgomot va fi similar cu un marcaj ales pentru jumătate din pixelii consideraţi. De aceea, extrăgând toţi biţii marcajului estimat din cadrul marcat va creşte probabilitatea ca marcajul original înserat să fie doar inversat, deci încă detectabil. Cea mai bună metodă de eliminare a marcajului este scăderea a jumătate din pixelii acestuia, punând p = 0.5 care duce la anularea autocorelaţiei folosite în general pentru detecţia marcajului.

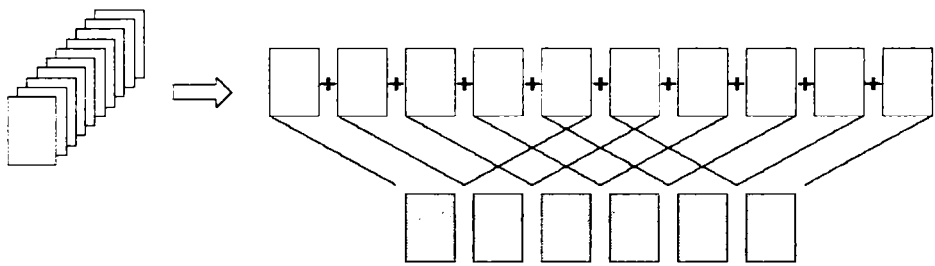


Fig 3.19: Atac de mediere într-o secvenţă video [Kun05].

O soluţie la acest atac a fost propusă în [KMY04]: un sistem de distribuţie multimedia în care toate copiile sunt marcate cu acelaşi marcaj, dar fiecare utilizator are o cheie secretă distinctă, ce diferă de cea de înserare. Un atacator cu acces la o cheie de detecţie poate „păcăli" detectorul corespondent, dar nu şi celelalte detectoare.

3.5 Atacurile ce folosesc mai multe copii marcate (multiple-copy)

Aceste atacuri intervin când semnalul gazdă este acelaşi, iar marcajul este diferit. În esenţă, aceste atacuri sunt de coliziune. Există două mari abordări ale acestui caz: prin prisma prelucrării semnalelor, respectiv prin prisma codării informaţiei. Tipurile de coliziune pot fi clasificate după cum urmează [Kun05, EKK99, SEG00, ZWL03, WTWL04]:

- de estimare: liniară (prin mediere, ponderată sau nu; prin filtrare; zgomot alb) respectiv neliniară,
- de tip statistic: min, max, median, minmax, negativ modificat, negativ aleator.
- ipoteza marcării transparente (*marking assumption*): coliziune prin copiere-şi-lipire, aleatoare, vot majoritar, atacuri binare (and, or, xor).

Într-un atac de coliziune, o coaliţie de piraţi care au versiuni diferite ale aceluiaşi produs multimedia, examinează copiile diferite în speranţa creării unui nou semnal care să nu fie legat de nici unul dintre ei. Există mai multe tipuri de coliziune. O metodă de coliziune liniară este sincronizarea copiilor marcate diferit şi medierea lor. Un alt atac de coliziune, numit „copiere-şi-lipire", constă în asamblarea de către atacatori a unor porţiuni tăiate din propriile copii, rezultând un

semnal nou. Alte atacuri folosesc operaţii neliniare, cum ar fi luarea valorii maxime sau mediane a componentelor din semnale. Trebuie menţionat că acest atac diferă de coliziunea asupra mai multor cadre dintr-o singură secvenţă video, aşa cum s-a specificat în subparagraful 3.4.13.

3.5.1 Coliziunea liniară

Este unul dintre cele mai fezabile atacuri de coliziune împotriva *fingerprinting*-ului. Dacă sunt K utilizatori, fiecare deţinând o copie marcată diferit, şi se coalizează, ei pot să combine liniar aceste K semnale pentru a produce o versiune fără marcaj. Fiindcă, în mod normal, nici unul dintre atacatori nu este dispus să rişte mai mult decât celălalt, semnalele ce conţin amprente diferite se mediază cu ponderi egale, ca în Figura 3.17. Medierea reduce puterea marcajelor. Cu cât numărul de atacatori este mai mare, cu atât fiecare marcaj este mai greu de detectat. Semnalul obţinut poate avea o calitate perceptuală chiar mai bună, în sensul că e mai asemănător cu semnalul original, decât cele marcate. Atacul descris în [EKK99] completează schema din Figura 3.17 prin adăugarea unui zgomot de putere mică, semnalul original fiind afectat de procesul de marcare cu o distorsiune limitată. S-a arătat că $O\left(\sqrt{N/\log N}\right)$ este ordinul de mărime al numărului de adversari suficienţi pentru a învinge sistemul de marcare-amprentare, unde N este lungimea totală a marcajului.

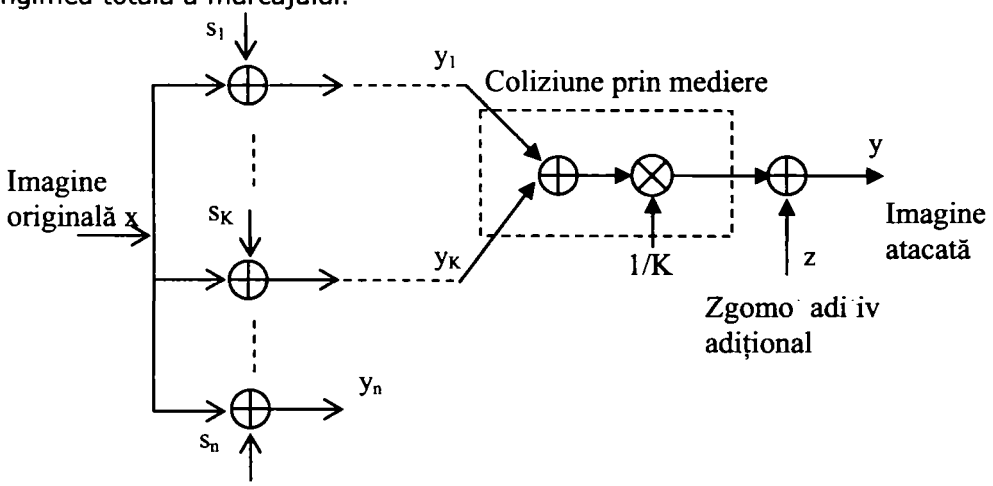


Fig.3.20: Coliziune liniară.

În [SEG00], este expus un atac mai general, în care atacatorii folosesc filtre invariante la translaţia liniară (LSI) plus zgomot alb pentru a elimina marcaje (amprente) bazate pe coduri ortogonale. Presupunând că toate amprentele sunt independente şi au caracteristici statistice identice, s-a arătat că atacul LSI optim este cel pentru care ponderile sunt egale înaintea adăugării zgomotului aditiv. Atunci când marcajul este împrăştiat în tot semnalul gazdă si detecţia se face printr-o corelaţie, atacul de coliziune „copiere-şi-lipire" are un efect similar cu cel de mediere. În ambele cazuri, energia fiecărei amprente este redusă cu un factor corespunzând la numărul de copii care se utilizează.

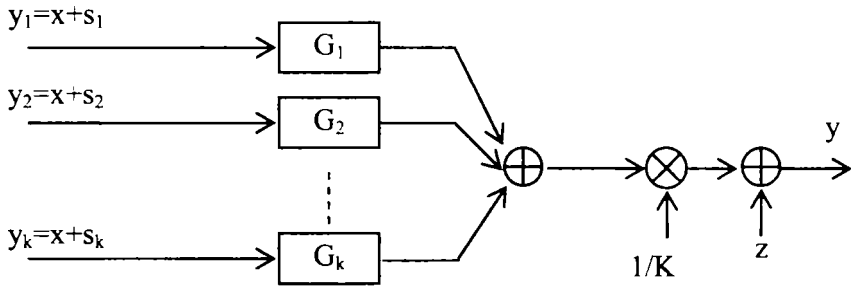


Fig.3.21: Coliziune liniară cu filtre LSI.

3.5.2 Coliziunea neliniară

Pentru fiecare componentă a semnalului multimedia, atacatorii pot alege orice valoare dintre cele observate, cuprinsă între cea minimă şi cea maximă, cu grad mare de încredere că produsul obţinut va avea o calitate perceptuală nealterată (valorile obţinute fiind în gama JND). O clasă importantă de atacuri prin coliziune neliniară sunt cele bazate pe operaţii cum ar fi luarea valorii maxime, minime, sau mediane a componentelor corespondente din cele K copii marcate diferit [ZWL03]. Se poate presupune pentru simplitate, ca aceste atacuri au loc în acelaşi domeniu ca şi cel al marcării. Diferenţa abia vizibilă (JND) din modelul vizual uman este folosită pentru a controla energia marcajelor inserate, pentru garantarea imperceptibilităţii. Câteva atacuri posibile sunt următoarele, [WTWL04]:
- *Minim, maxim, sau median*, semnalul are valoarea minimă, maximă, respectiv mediană a componentelor corespunzătoare a celor K semnale marcate;
- *Atacul minmax*: fiecare componentă din semnalul atacat este media între minimul şi maximul componentelor corespunzătoare;
- *Atacul negativ modificat*: fiecare componentă din semnalul atacat este diferenţa dintre mediană si suma dintre maxim şi minim a componentelor corespunzătoare;
- *Atacul negativ aleator*: fiecare componentă din semnalul atacat ia cu probabilitatea *p*, valoarea maximă a celor K componente ale semnalelor marcate, şi valoarea minimă cu probabilitatea (1 - *p*).

Atacurile de coliziune mediană sau minmax sunt similare ca performanţă cu coliziunea liniară. Pe de altă parte, eficienţa atacului se îmbunătăţeşte prin coliziune minim, maxim sau negativ modificat. Atacul de coliziune negativ modificat are cea mai bună performanţă, dar distorsiunile introduse sunt mult mai vizibile. După combinarea neliniară, atacatorii pot introduce zgomot aditiv [WTWL04].

Măsuri posibile împotriva atacurilor folosind copii multiple, sunt codurile anti-coliziune si construirea marcajelor astfel încât coliziunea să ducă la distorsiuni perceptuale pentru atacator (Joint Source Fingerprinting) [LK05].

3.6 Concluzii

În analiza performanţelor tehnicilor de marcare transparentă, sunt folositoare benchmark-urile (Stirmark, UnZign, Certimark, etc). În paralel cu dezvoltarea tehnicilor de marcare transparentă, are loc şi dezvoltarea unor noi atacuri. Este probabilă o cooperare a criptografiei cu tehnici moderne de prelucrarea semnalelor, domenii legate de obstrucţionarea marcării transparente. Poate fi întrevăzută apariţia unor atacuri noi care să îmbine tehnici de steganaliză cu atacuri din marcare.

4. APLICAREA TRANSFORMĂRII WAVELET ÎN MARCAREA INFORMATĂ A IMAGINILOR

4.1 Introducere

În acest capitol, se prezintă algoritmi de marcare transparentă a semnalelor multimedia, în care s-a dorit ca marcajul să fie nu numai detectabil, ci să poată fi şi extras [NI03, NBK04, Naf04b, NB05, Naf05b, Naf05a, NIB05]. De aceea, pentru simplitate, s-a folosit un marcaj binar. Ne concentrăm asupra marcării imaginilor statice, având în vedere faptul că se poate face o generalizare a metodei şi pentru alte tipuri de semnale multimedia.

În cele ce urmează, vom aborda o metodă de marcare care lucrează în domeniul transformării wavelet. Cercetările făcute asupra ochiului uman indică faptul că retina împarte o imagine în mai multe componente, care se transmit de la ochi înspre cortex pe benzi diferite de frecvenţă. Aceste canale pot fi excitate doar de componente ale unor semnale cu caracteristici asemănătoare. Prelucrarea semnalelor din diferitele benzi de frecvenţă este independentă. Studiile au arătat că fiecare dintre aceste canale are o bandă de lăţime de aproximativ o octavă. În mod asemănător, într-o descompunere multirezoluţie, imaginea este separată în benzi de frecvenţă cu lăţimi aproximativ egale pe o scară logaritmică. De aceea, este de aşteptat ca folosirea transformării wavelet discrete să permită prelucrarea independentă a componentelor rezultate, fără o interacţiune perceptibilă/vizibilă între ele.

În plus, metodele prezentate [NI03, NBK04, Naf04b, NB05, Naf05b, Naf05a, NIB05] plasează marca atât în spaţiu, cât şi în frecvenţă; acest lucru permite în principiu detecţia schimbărilor imaginii, localizate spaţial şi spectral.

Pentru a nu schimba imaginea în mod vizibil, nu înglobăm marcajul în componentele de frecvenţă joasă (subimaginea LL a transformatei). Procesul de înglobare are loc selectiv, în funcţie de o cheie de marcare, în subimaginile de detaliu ale transformatei imaginii. Schimbarea coeficienţilor selectaţi trebuie făcută în aşa fel încât imaginea gazdă să nu fie perceptibil afectată.

4.2 Înglobarea şi extragerea marcajului

4.2.1 Înglobarea marcajului

Presupunem, pentru simplitate, că marcajul binar are lungimea N_w şi este compus din elementele $\{-1,1\}$. Imaginea originală f, în care înglobăm marca, este imaginea gazdă. Marcajul este înglobat în coeficienţii wavelet de detaliu ai imaginii gazdă, cu ajutorul unei chei de marcare. Această cheie este generată în funcţie de imaginea originală şi este folosită pentru a selecta poziţiile exacte în domeniul wavelet în care se înglobează marca. Pentru fiecare coeficient din domeniul wavelet, cheia are valoarea 1 sau 0, indicând dacă coeficientul este sau nu marcat. Numărul valorilor de „1" din cheie trebuie să fie mai mare sau egal cu lungimea marcajului.

Valorile marcajului sunt înglobate repetat în coeficienţi diferiţi selectaţi de cheie, dacă lungimea marcajului este mai mică decât numărul valorilor de „1" din cheie. Tehnica constă în trei etape descrise mai jos:

Etapa 1. Se calculează transformata wavelet discretă la nivelul de rezoluţie *L* a imaginii gazdă, pentru a produce o secvenţă de 3*L* sub-imagini de detaliu, corespunzătoare detaliilor pe orizontală, verticală, respectiv pe diagonală pentru fiecare nivel de rezoluţie şi o aproximaţie grosieră a imaginii la cel mai mic nivel de rezoluţie. Notăm cel de-al *s*-lea coeficient de detaliu din componenta imaginii la nivelul de rezoluţie *l* a imaginii gazdă cu $f_{s,l}(m,n)$, unde $s \in \{h,v,d\}$ (coeficienţii de detaliu pe orizontală, verticală, respectiv diagonală) şi $l = 1,...,L$. Aproximarea imaginii este reprezentată de $f_{a,L}(m,n)$. Indicele *a* provine de la aproximare. În Figura 4.1 se prezintă un exemplu de calcul al transformării wavelet.

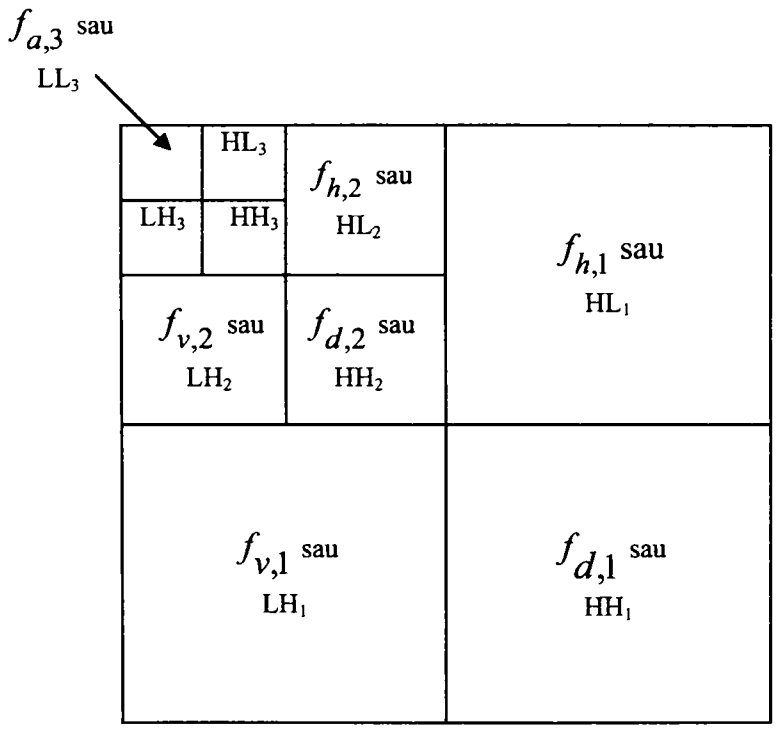


Fig. 4.1: Reprezentare ierarhică a coeficienţilor wavelet pe trei nivele de rezoluţie. Imaginea de aproximare LL şi imaginile de detaliu LH, HL şi HH conţin informaţia necesară pentru refacerea imaginii de aproximare pentru următorul nivel de rezoluţie.

În funcţie de imaginile de detaliu, se generează cheia de marcare *k*, conform relaţiei [NI03, NBK04, Naf04b, NB05]:

$$k_{s,l}(m,n) = \begin{cases} 1, & \text{dacă } f_{s,l}(m,n) > T_{s,l} \\ 0, & \text{altfel} \end{cases} \qquad (4.1a)$$

sau conform relaţiei [NIB05]:

$$k_{s,l}(m,n)=\begin{cases}1, & \text{dacă } \left|f_{s,l}(m,n)\right|>T_{s,l}\\ 0, & \text{altfel}\end{cases} \tag{4.1b}$$

unde $k_{s,l}$ reprezintă cheia asociată fiecărei imagini de detaliu iar $T_{s,l}$ reprezintă un prag dependent de subbandă. Cheia se calculează pentru $l=1,...,L$ şi pentru $s\in\{h,v,d\}$.

Dacă lungimea cheii N_k, o considerăm ca fiind numărul de cifre de „1" din cheie, atunci generarea cheii se va face astfel încât marca originală să fie înserată de un număr impar de ori, adică $\frac{N_k}{N_w}=M=2p+1$ (aici M specifică numărul de repetiţii). De aceea, pentru fiecare nivel, dacă lungimea cheii $k_{s,l}$ este $N_{s,l}$, atunci generarea cheii respective se face astfel încât să se îndeplinească condiţia din relaţia:

$$\frac{N_{s,l}}{N_w}=2p+1 \tag{4.2}$$

unde lungimea cheii *k* se poate defini astfel [NBK04]:

$$N_k=\sum_{\substack{l=1..L\\ s=h,v,d}} N_{s,l} \tag{4.3}$$

Etapa 2. Considerăm fiecare nivel de rezoluţie *l* şi localizarea coeficienţilor (*m, n*). Dacă valoarea asociată cheii *k* este unu se procedează după cum urmează, altfel nu se înglobează marcajul:

$$f_{s,l}^{w}(m,n)=f_{s,l}(m,n)\oplus w(m,n) \tag{4.4}$$

unde $s\in\{h,v,d\}$, $f_{s,l}^{w}$ este coeficientul wavelet de detaliu al imaginii marcate, iar $f_{s,l}$ este coeficientul wavelet de detaliu al imaginii originale, pentru imaginea de

detaliu *k*, şi respectiv pentru nivelul de rezoluţie *l*. Operatorul $\oplus$ reprezintă operaţia de înglobare a bitului marcajului în coeficientul wavelet de detaliu corespunzător.

Etapa 3. Se aplică transformata wavelet inversă imaginilor de detaliu şi de aproximare obţinute, pentru a forma imaginea marcată. Procesul de înglobare a marcajului este prezentat în Figura 4.2.

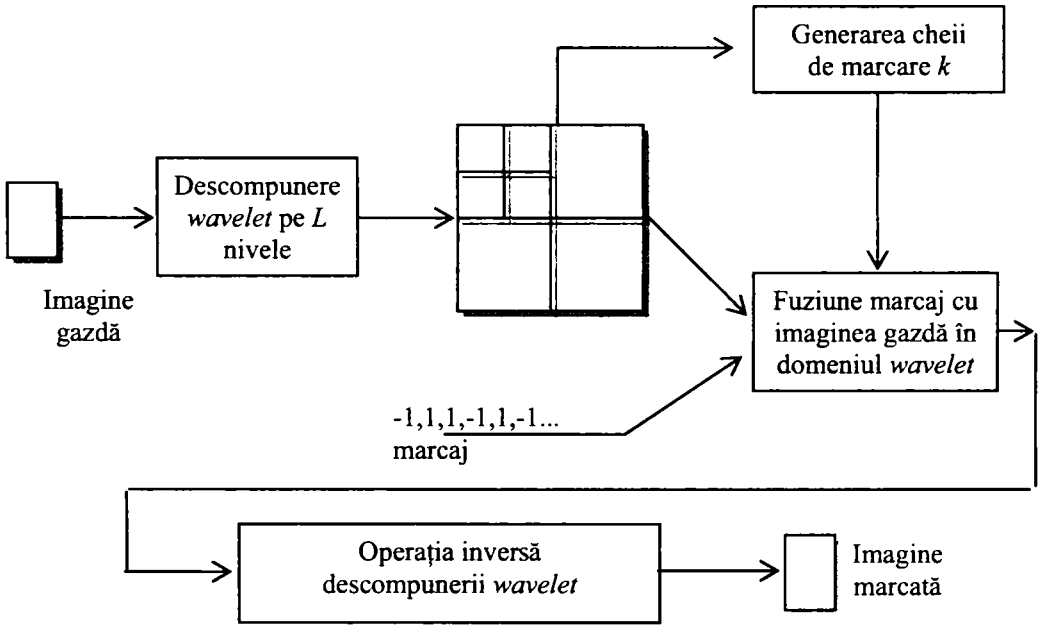


Fig. 4.2: Metodele de marcare propuse [NI03, NBK04, Naf04b, NB05, NIB05] . Se prezintă paşii care trebuie efectuaţi în general pentru a obţine imaginea marcată.

4.2.2 Detecţia şi extragerea marcajului

Pentru a detecta şi extrage marca, imaginea originală trebuie să fie cunoscută. Prin urmare, sistemul de marcare prezentat este *privat*. Imaginea recepţionată este o versiune posibil distorsionată a imaginii marcate. Scopul procesului de extragere este obţinerea unei estimări de încredere a marcajului original. Procesul de detecţie cere cunoştinţe şi despre marcaj $w(m,n)$.

Reprezentăm imaginea căreia vrem să-i aplicăm procesul de extracţie prin $r(m,n)$. Imaginea originală este $f(m,n)$. Pentru detecţia şi extragerea marcajului, se parcurg următoarele etape:

Etapa 1. Primul pas implică aplicarea unei descompuneri wavelet cu *L* nivele asupra imaginii $r(m,n)$, precum şi asupra imaginii originale $f(m,n)$. Fie $r_{s,l}(m,n)$ a *s*-a imagine de detaliu din nivelul de rezoluţie *l* a imaginii $r(m,n)$.

Etapa 2. Cheia *k* se generează folosind imaginea originală, aşa cum s-a văzut în faza înglobării marcajului. Această cheie furnizează locaţiile unde a fost

înglobat un bit al marcajului binar. Extragem marcajul din aceşti coeficienţi după cum urmează:

$$\hat{w}(m,n) = r_{s,l}(m,n)\Theta f_{x,l}(m,n) \tag{4.5}$$

unde $\hat{w}(m,n)$ reprezintă bitul recuperat, iar operatorul Θ reprezintă operaţia inversă celei efectuate în procesul de înglobare.

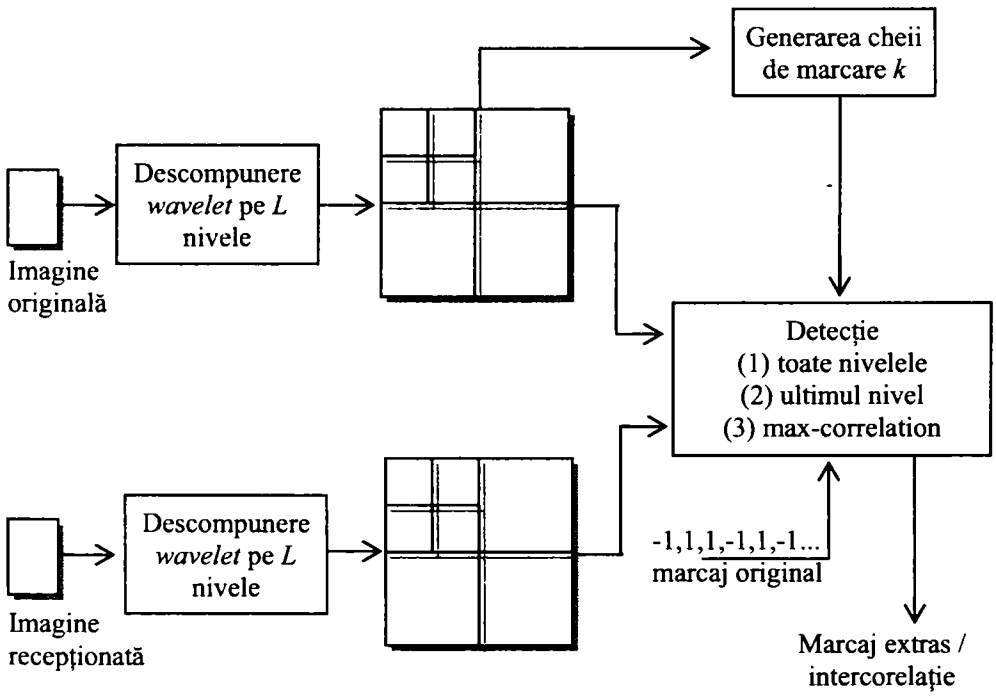


Fig. 4.3: Detecţia şi extragerea marcajului pentru metodele propuse [NBK04, Naf04b, NB05, NIB05]. În [NI03] detecţia se face din (a) subbanda de detalii diagonale a primului nivel de rezoluţie, (b)toate subbenzile de detalii ale acestui nivel

Etapa 3. Dacă marcajul a fost înglobat în locaţii diferite de mai multe ori, atunci este ataşată marcajului estimat valoarea bitului extras cea mai des întâlnită. Dacă au fost extraşi un număr egal de „1", respectiv de „-1", atunci se face o alegere aleatoare pentru valoarea bitului de marcaj. În [NI03], înserarea dar şi detectarea marcajului se face respectiv în/din: **(a)** subbanda de detalii diagonale a primului nivel de rezoluţie, **(b)** toate subbenzile de detalii ale acestui nivel. În afară de [NI03], în restul capitolului ne vom referi la trei tipuri de detectoare: **(1)** din toate nivelele, **(2)** din ultimul nivel, care este cel mai puţin afectat de operaţii precum compresia [NBK04, Naf04b, NB05], **(3)** detecţie cu corelaţie maximă cu marcajul original (*max-correlation*) [Naf05b].

Un marcaj dat este detectat, dacă intercorelaţia dintre marcajul extras şi marcajul dat este mai mare decât un prag cunoscut dinainte. Mai precis, condiţia de detecţie a marcajului este dată de:

$$\rho(w,\hat{w}) = \frac{\sum w(n)\cdot \hat{w}(n)}{\sqrt{\sum w^2(n)}\ \sqrt{\sum \hat{w}^2(n)}} \geq T, \tag{4.6}$$

unde *w* este marcajul dat, $\hat{w}$ este marcajul extras, iar *T* este pragul cunoscut dinainte. $\rho(w,\hat{w})$ este cunoscut ca şi coeficientul de intercorelaţie dintre marcajul dat şi marcajul extras. Dacă nu se menţionează alte condiţii, toate sumele din ecuaţia (4.6) şi din următoarea secţiune au indexul *n* şi domeniul de la 1 la N_W. Dacă coeficientul de intercorelaţie este mai mare sau egal cu *T*, marcajul dat este detectat în imaginea recepţionată. Dacă imaginea de la recepţie este aceeaşi cu imaginea marcată, atunci coeficientul de intercorelaţie ar trebui să fie 1. Dacă imaginea recepţionată este o versiune modificată a imaginii marcate, fără schimbări vizibile, atunci coeficientul de intercorelaţie ar trebui să aibă o valoare mare (subunitară, dar apropiată de 1). Detecţia şi extragerea este prezentată în Figura 4.3.

Cele trei variante ale metodei propuse în [NI03, NBK04, Naf04b, NB05, Naf05b, Naf05a, NIB05], diferă prin modul de înglobare al bitului marcajului, aşa cum s-a definit în ecuaţia (4.4), precum şi în modul de generare a cheii de marcare (diferă valorile $T_{s,l}$). Pentru a treia variantă, alegerea acestor praguri se face pe baza unei *analize statistice* a coeficienţilor wavelet [NIB05].

4.3 Prima metodă de marcare informată

În [NI03], am experimentat înserarea marcajului în **primul nivel de rezoluţie**. Detecţia a fost făcută din toate subbenzile, sau numai din subbanda de detalii diagonale. Imaginea originală se descompune într-o imagine de aproximaţie şi trei imagini de detaliu, cu alte cuvinte *L* este 1. Prin urmare, generarea cheii se face doar pentru primul nivel, folosindu-se un singur parametru q_1. Operaţia definită de operatorul $\oplus$ din relaţia (4.4) este în acest caz:

$$f_{s,1}^{w}(m,n) = f_{s,1}(m,n) + \alpha w(m,n) \tag{4.7}$$

unde $s \in \{h,v,d\}$, iar α este o variabilă pozitivă, definită de utilizator. Este uşor de dedus că operaţia definită de Θ din relaţia (4.5) este în acest caz:

$$\hat{w}(m,n) = \frac{r_{s,1}(m,n) - f_{s,1}(m,n)}{\alpha} \tag{4.8}$$

Dacă $r_{s,1}(m,n) = f_{s,1}(m,n)$, se face o alegere aleatoare pentru bitul de marcaj binar.

Pentru simulări, am folosit următoarele valori pentru parametri: $q_1 = 0.06$, iar $\alpha = 10$, transformata wavelet cu funcţie mother wavelet Daubechies 5. Am înglobat marcajul în două moduri:

- numai în coeficienţii wavelet de **detaliu pe diagonală** ai primului nivel de rezoluţie, respectiv,
- în **toate imaginile de detaliu ai primului nivel** de rezoluţie.

Imaginea originală, precum şi cele două imagini marcate sunt prezentate în Fig. 4.4.

(a) (b) (c)

Fig.4.4(a) Imaginea originală "Lena", (b) Versiunea marcată în subimaginea de detalii diagonale la primul nivel, PSNR=43.76 dB, (c) Versiunea marcată "Lena", în toate imaginile de detaliu ai primului nivel de rezoluţie, PSNR=39.14 dB.

Cele două imagini marcate au $PSNR = 43.76\,\mathrm{dB}$, respectiv $PSNR = 39.14\,\mathrm{dB}$. Se poate observa că a doua imagine este perceptual mai afectată decât prima. Marcajul extras din a doua imagine este mai robust împotriva atacurilor decât cel extras din prima imagine.

Am studiat efectul distorsiunilor obişnuite ale semnalului (compresie JPEG, filtrare mediană, zgomot aditiv alb gaussian) asupra coeficientului de intercorelaţie între marcajul cunoscut şi cel extras din imaginea atacată. Comparăm performanţele acestei prime variante a metodei propuse cu o metodă propusă de Kundur şi Hatzinakos în [KH98]. Cheia de marcare folosită pentru a îngloba marcajul este $k_{d,1}(m,n)$. Parametrul definit de utilizator este $Q = 4$, aşa cum au indicat autorii în [KH98]. În acest caz, imaginea marcată are $PSNR = 57.33\,\mathrm{dB}$.

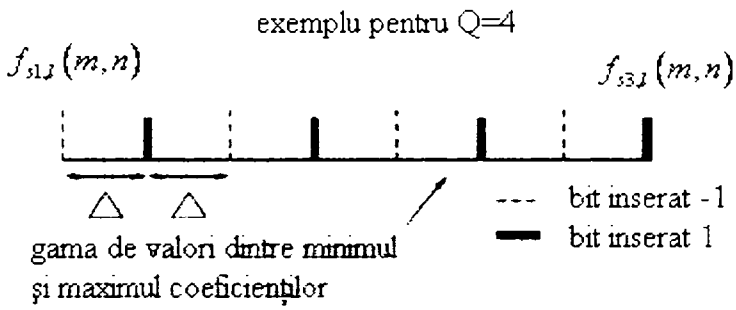
În [KH98], marcajul se inserează după cum urmează:

a. se sortează coeficienţii în ordine crescătoare astfel încât $f_{s1,l}(m,n)$, $f_{s2,l}(m,n)$ şi $f_{s3,l}(m,n)$ sunt coeficienţi $f_{s1,l}(m,n) \le f_{s2,l}(m,n) \le f_{s3,l}(m,n)$, unde $s1, s2, s3 \in \{h, v, d\}$ şi $s1, s2, s3$ sunt diferite.

b. Se cuantizează $f_{s2,l}(m,n)$ ca in figura de mai jos. Gama de valori între $f_{s1,l}(m,n)$ şi $f_{s3,l}(m,n)$ este împărţită în cuante de lăţimea

$$\Delta = \frac{f_{s3,l}(m,n) - f_{s1,l}(m,n)}{2Q-1},$$

unde Q este o variabilă definită de utilizator. Pentru a insera un bit 1, $f_{s2,l}(m,n)$ este cuantizat la cea mai apropiată valoare cu linie continuă din figură, respectiv pentru -1, la cea mai apropiată valoare punctată.



Procedeul de inserare a marcajului în [KH98]

Detecţia se face într-o manieră similară, prin ordonarea coeficienţilor wavelet, şi estimarea bitului care a fost inserat, din poziţia coeficientului de mijloc.

În Fig. 4.5, se prezintă coeficientul de intercorelaţie $\rho(w,\hat{w})$ în funcţie de dimensiunea filtrului $M \times M$, pentru filtrarea mediană, în funcţie de rata de compresie, pentru compresia JPEG, respectiv în funcţie de raportul semnal/zgomot (SNR), pentru zgomot aditiv alb gaussian. Graficele marcate cu simbolul „o" sunt rezultatele pentru prima abordare (a fost marcată numai imaginea de detalii pe diagonală).

Graficele marcate cu simbolul „x" sunt rezultatele pentru a doua abordare (au fost marcate toate imaginile de detalii). Celelate grafice sunt rezultatele pentru metoda propusă în [KH98].

Coeficientul de intercorelaţie pentru metoda propusă în această secţiune este, în mod evident, mai mare decât pentru metoda propusă în [KH98], în cazul compresiei JPEG şi zgomot alb gaussian aditiv.

Metoda propusă nu arată robusteţe împotriva filtrării mediane, comparativ cu metoda din [KH98].

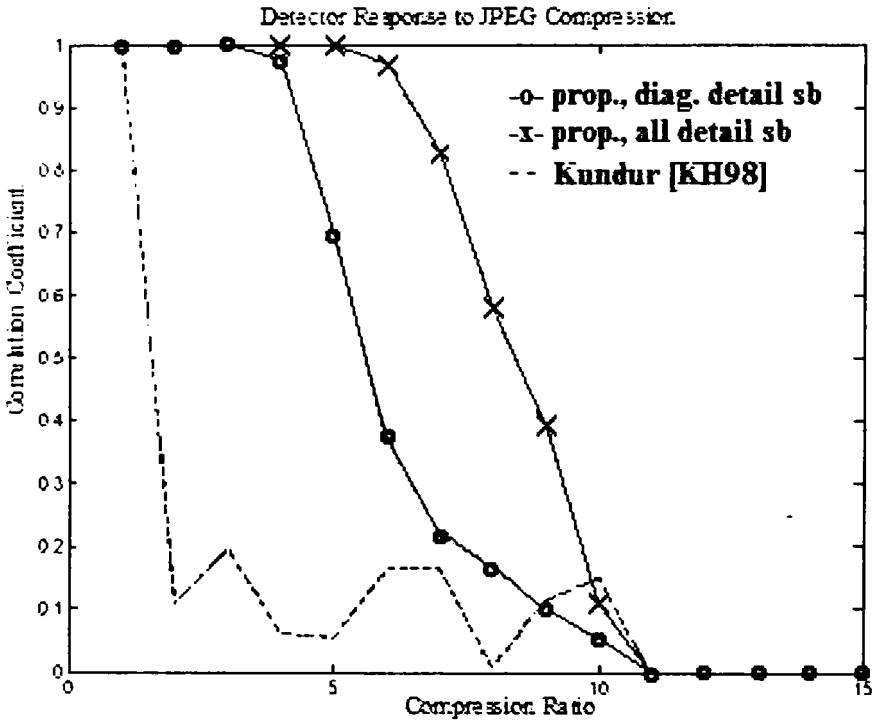


Fig. 4.5 (a) Răspunsul detectorului la compresia JPEG.

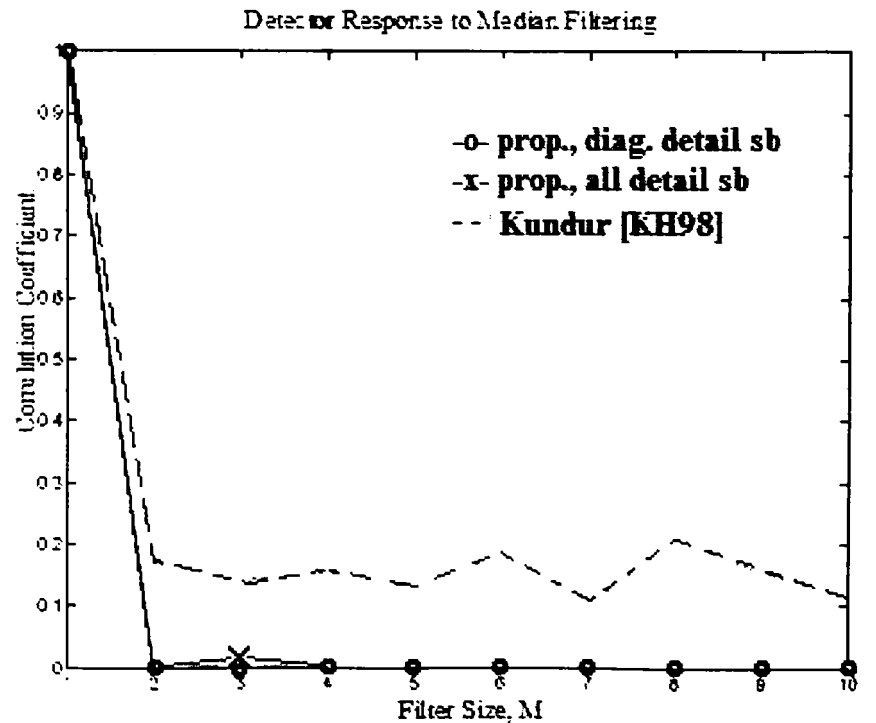


Fig. 4.5 (b) Răspunsul detectorului la filtrarea mediană.

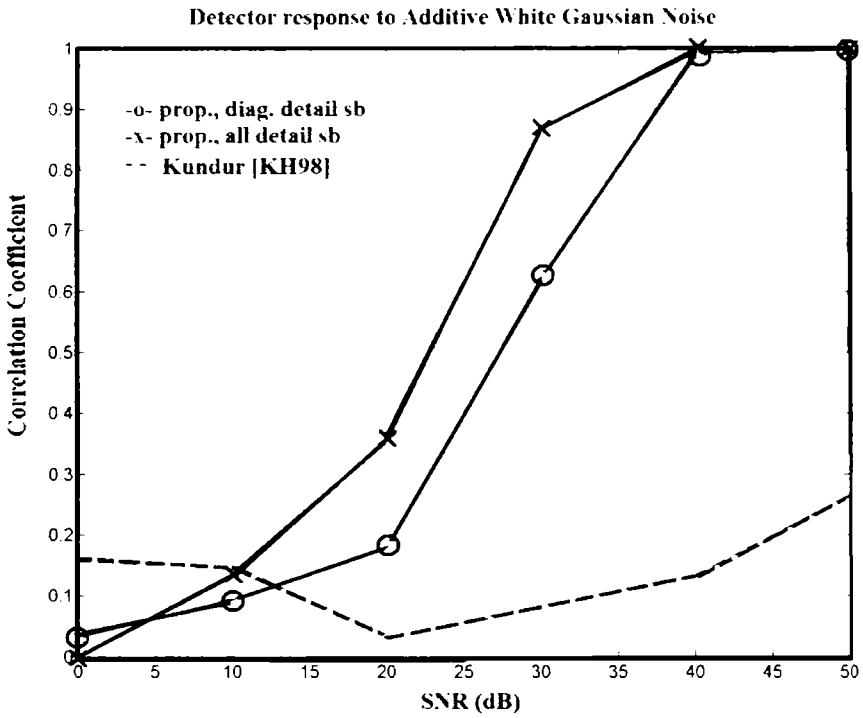


Fig. 4.5 (c) Răspunsul detectorului la zgomot alb gaussian aditiv. Graficele marcate cu simbolul „o" sunt rezultatele pentru prima abordare, cele marcate cu „x" sunt rezultatele pentru a doua abordare. Restul graficelor sunt rezultatele pentru metoda din [KH98].

4.4 A doua metodă de marcare informată

Imaginea originală se descompune pe trei nivele de rezoluţie, adică într-o imagine de aproximaţie $f_{a,3}$ şi câte trei imagini de detaliu pentru fiecare nivel de rezoluţie.

Generarea cheii se face pentru trei nivele de rezoluţie, cu ajutorul parametrilor q_1, q_2, q_3, folosind relaţia (4.1a). Aceştia sunt pozitivi şi pot fi definiţi de utilizator:

$$T_{s,l} = q_l \max_{m,n} \left\{ f_{s,l}(m,n) \right\} \tag{4.9}$$

În acest caz operaţia $\oplus$ din relaţia (4.4) este:

$$f_{s,l}^{w}(m,n) = f_{s,l}(m,n) + \alpha \cdot f_{s,l}(m,n) w(m,n) \tag{4.10}$$

unde $s \in \{h,v,d\}$, $l = 1,...,L$ iar $\alpha \in (0,1)$ este o variabilă definită de utilizator, respectiv operaţia Θ din relaţia (4.5) este:

$$\hat{w}(m,n)=\frac{r_{s,l}(m,n)-f_{s,l}(m,n)}{\alpha\cdot f_{s,l}(m,n)} \tag{4.11}$$

Dacă $r_{s,l}(m,n)=f_{s,l}(m,n)$ şi/sau dacă $f_{s,l}(m,n)=0$, se face o alegere aleatoare pentru $w(m,n)$.

Un set preliminar de experimente [Naf04a] a fost efectuat pe imaginea Lena. Ca parametri s-au folosit, marcajul binar de lungime N_w = 256, transformata wavelet cu funcţia mother wavelet Daubechies 5 ca domeniu de marcare, numărul de nivele de rezoluţie L = 3, intensitatea de marcare α = 0.1 precum şi variabilele dependente de nivel q_1 = 0.06, q_2 = 0.04, q_3 = 0.02.

Imaginea originală, imaginea marcată cu metoda propusă, precum şi imaginea marcată cu metoda descrisă în [KH98] sunt prezentate în Fig. 4.6. Pentru a îngloba marcajul folosind metoda din [KH98], cheile de marcare folosite pentru fiecare nivel de rezoluţie sunt $k_{d,1}$, $k_{d,2}$, respectiv $k_{d,3}$ (care indică selectarea poziţiilor în care se inserează marcajul). Aici înglobarea marcajului se face în mai multe nivele de rezoluţie, faţă de experimentul anterior.

(a) (b) (c)

Fig. 4.6: (a) Imaginea originală "Lena", (b) Versiunea marcată "Lena", folosind a doua variantă a metodei propuse, PSNR=45.39 dB, (c) Versiunea marcată "Lena", folosind metoda din [KH98], PSNR=45 dB

Cele două imagini marcate au *PSNR* foarte apropiat: 45.39 dB, respectiv 45 dB. Nici una nu este afectată în mod vizibil de procesul de marcare.

În Fig. 4.7, se prezintă coeficientul de intercorelaţie $\rho(w,\hat{w})$ în funcţie de dimensiunea filtrului, $M\times M$, pentru filtrarea mediană, în funcţie de rata de compresie, pentru compresia JPEG, respectiv în funcţie de raportul semnal/zgomot (SNR). Graficele marcate cu simbolul „+" sunt rezultatele pentru metoda propusă, cele cu linii întrerupte fiind graficele pentru extragerea marcajului din ultimul nivel de rezoluţie. Graficele nemarcate sunt rezultatele pentru metoda propusă în [KH98], iar cele cu linii întrerupte reprezintă graficele pentru care marcajul a fost extras din ultimul nivel de rezoluţie.

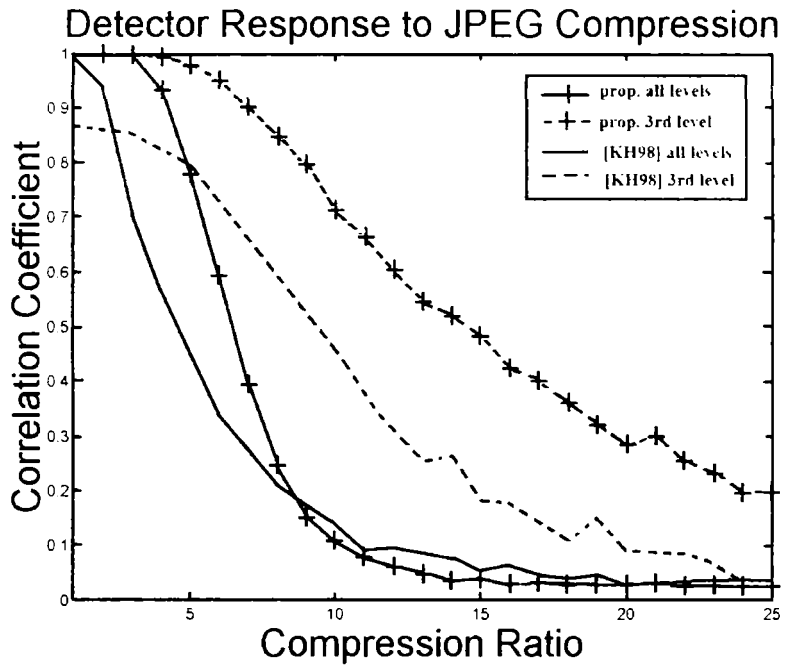


Fig. 4.7(a): Răspunsul detectorului la compresie JPEG

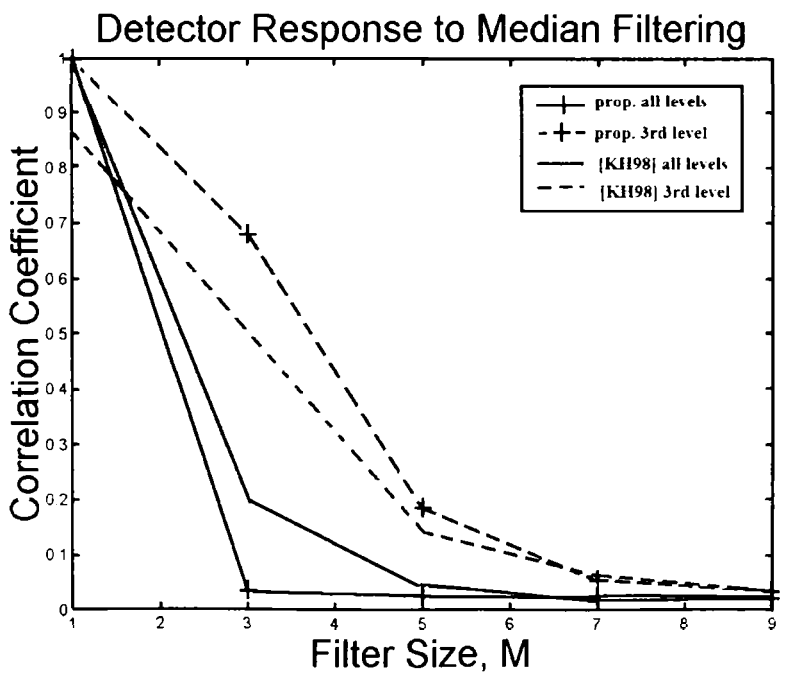


Fig. 4.7(b): Răspunsul detectorului la filtrare mediană

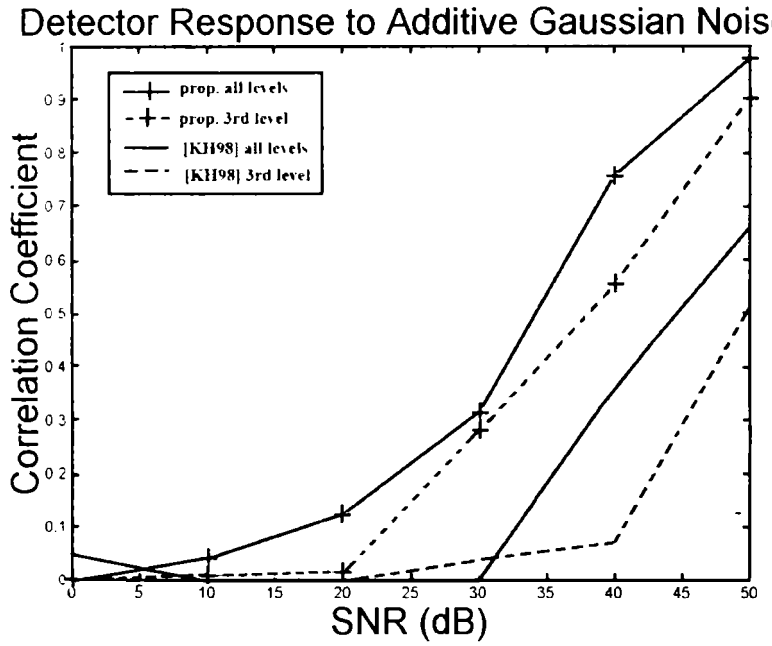


Fig. 4.7(a): Răspunsul detectorului la zgomot AWGN.

Fig. 4.7: Răspunsul detectorului la distorsiuni obişnuite. Graficele marcate cu "+" sunt pentru metoda propusă, cele nemarcate sunt pentru metoda din [KH98]. Graficele cu linie întreruptă sunt obţinute pentru extragerea marcajului din ultimul nivel de rezoluţie.

Rezultate. Se observă că performanţele metodei propuse în [Naf04a] sunt superioare metodei din [KH98]. De asemenea, coeficientul de intercorelaţie este mai mare dacă extragerea marcajului se face numai din ultimul nivel de rezoluţie. Acest lucru se datorează faptului că distorsiunile obişnuite ale semnalului sunt mai semnificative pentru componentele spectrale mai înalte ale imaginii.

Un al doilea set de experimente [Naf04b] a fost efectuat folosind patru imagini de mărime 256x256, şi anume Lenna, Boat, Barbara şi Peppers, prezentate în Figura 4.8. Ca parametri s-au folosit, marcajul binar de lungime N_w = 256, transformata wavelet cu funcţia mother wavelet Daubechies 5 ca domeniu de marcare, numărul de nivele de rezoluţie L = 3, intensitatea de marcare α = 0.1 precum şi variabilele dependente de nivel q_1 = 0.06, q_2 = 0.04, q_3 = 0.02.

Performanţele metodei propuse în [Naf04b] sunt comparate cu tehnica spread-spectrum în domeniul DCT propusă de Cox ş.a. [CKLS97]. Aceştia înglobează o secvenţă pseudo-aleatoare în cei mai mari coeficienţi DCT, fără a afecta coeficientul DC, astfel împrăştiind marca în mai multe componente spectrale:

$$v'(i) = v(i)\left(1 + \beta w(i)\right)$$

unde v(i) reprezintă coeficientul DCT de marcat, w(i) este bitul de marcaj, β este puterea de marcare, iar v'(i) este coeficientul marcat. In lucrarea originală [CKLS97], marcajul era o secvenţă pseudo-aleatoare de tip $\mathcal{N}(0,1)$ cu lungimea 1000 şi puterea de marcare era de valoarea β = 0.1.

Pentru o mai bună comparaţie, marcajul folosit este bipolar, cu aceeaşi lungime, ca la metodele mele, 256 biţi. De asemenea, numărul de repetiţii a fost acelaşi în ambele cazuri (spre exemplu 33 repetiţii pentru Peppers).

Fig. 4.8: Imagini originale folosite în primul set de experimente: Lenna, Boat, Barbara şi Peppers. Coloana din mijloc reprezintă imaginile marcate cu metoda propusă [Naf04b]. Coloana din dreapta reprezintă imaginile marcate cu metoda din [CKLS97]

Diferenţa între imaginea marcată şi cea originală este evaluată în două moduri, folosind PSNR precum şi observatori umani. Imaginile marcate cu metoda propusă nu au fost distorsionate semnificativ faţă de originale, în timp ce cele marcate cu metoda lui Cox ş.a. au distorsiuni vizibile, chiar supărătoare. Imaginile originale şi cele marcate cu ambele metode sunt prezentate în Fig. 4.8. Tabelul 4.1 conţine valorile PSNR pentru fiecare imagine.

Tab. 4.1: Valori PSNR [dB] ca măsură a zgomotului introdus de procesul de marcare

Imagine / Metoda	Lenna	Boat	Barbara	Peppers
Metoda propusă	45.39 dB	44.35 dB	44.18 dB	45.55 dB
Metoda lui Cox şi alţii	27.19 dB	25.35 dB	26.44 dB	25.75 dB

În metoda propusă, diferenţa între imagini este prezentată în Fig. 4.9. Este evident că marcajul este înserat în texturi şi contururi. De exemplu, la imaginea Lenna, marcajul afectează detalii precum penele de la pălărie.

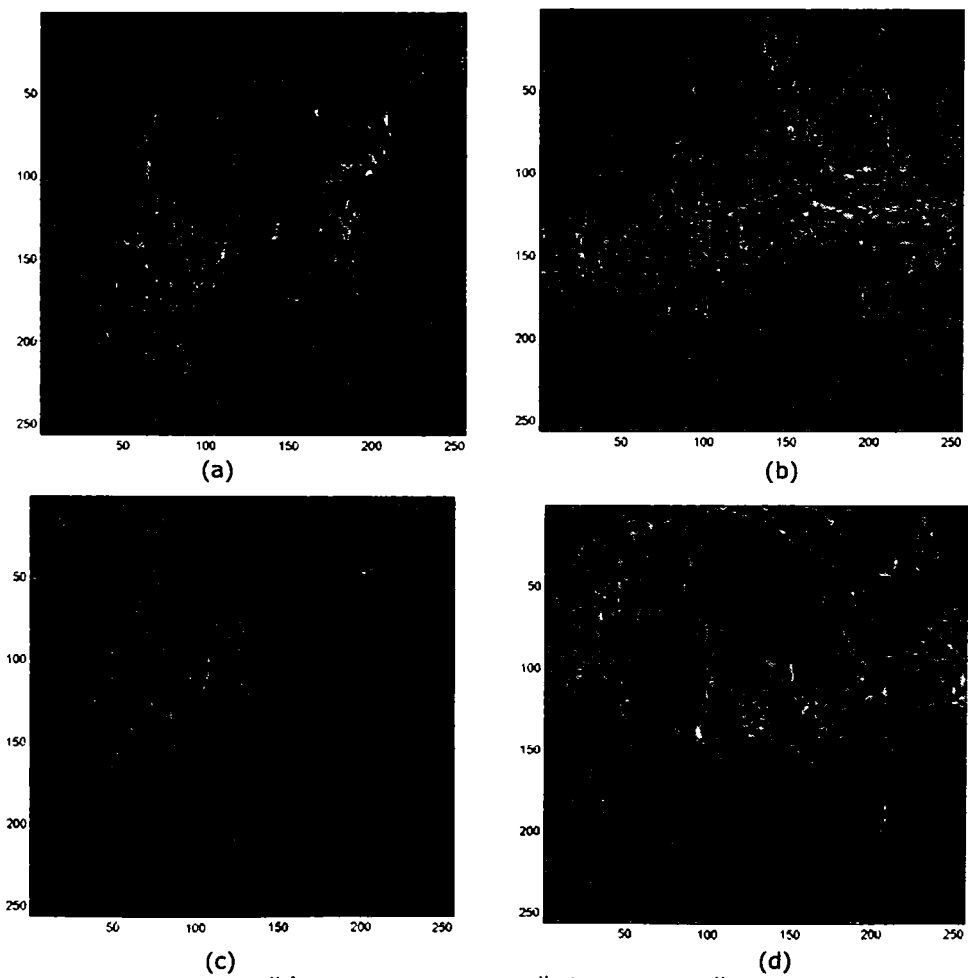


Fig. 4.9: Imagini diferenţă între imaginea marcată şi cea originală pentru cele patru cazuri, Lenna (a), Boat (b), Barbara (c),şi respectiv, Peppers (d).

Rezultate. Am arătat că cele patru imagini nu au fost afectate de procesul de marcare. Se analizează robusteţea sistemului propus cu parametrii prezentaţi. Extragerea marcajului se face în două feluri, folosind regula majoritară (detector tip 1, notat NC1 în următoarele figuri), şi din ultimul nivel, aici l=3, cel cu rezoluţie brută (detector tip 2 notat aici NC2).

Efectul prelucrărilor semnalelor obişnuite (filtrare mediană, zgomot AWGN, compresie JPEG) este prezentat prin coeficientul de corelaţie între original şi marcajul recuperat. Performanţele pentru [Naf04b] sunt comparate cu rezultatele metodei din [CKLS97]. Pentru fiecare imagine, răspunsul detectorului este prezentat ca funcţie de lungimea ferestrei filtrului M, rata de compresie CR şi raportul semnal-pe-zgomot SNR pentru cazul filtrării mediane, compresiei JPEG şi respectiv zgomot AWGN (Fig. 4.10 - 4.21). Răspunsul detectorului a fost calculat ca o medie de 32 răspunsuri pentru 32 marcaje necorelate. Graficele marcate cu simbolurile "o" şi "+" sunt rezultatele pentru metoda propusă [Naf04b], detector 1 şi 2 (sau NC1 şi NC2) respectiv, în timp ce graficele nemarcate reprezintă rezultatele pentru metoda propusă în [CKLS97].

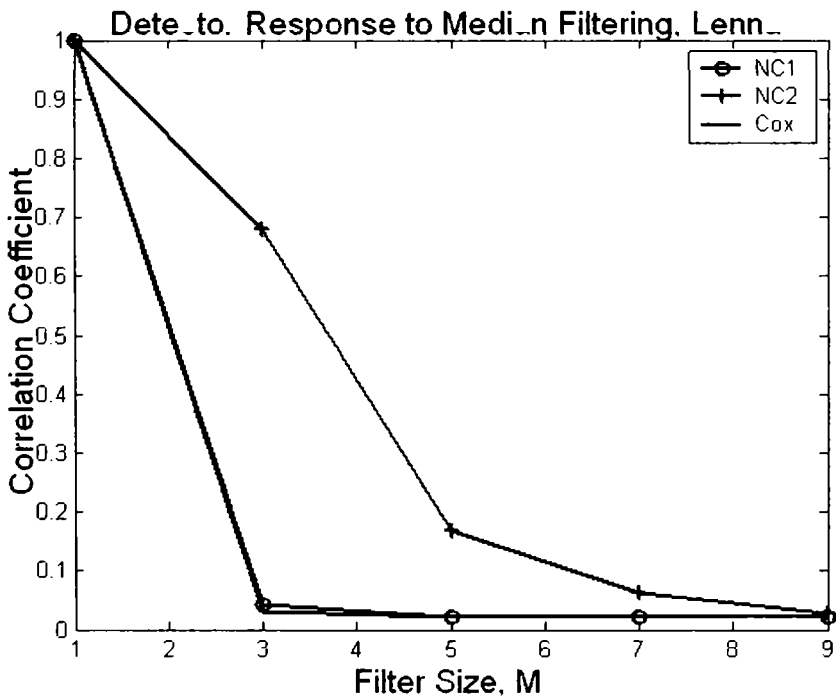


Fig. 4.10: Răspunsul detectorului la filtrarea mediană, imagine test " Lenna" pentru metoda din [CKLS97] (linie continuă), metoda propusă, detectorul 1 ("o"), detectorul 2 ("+").

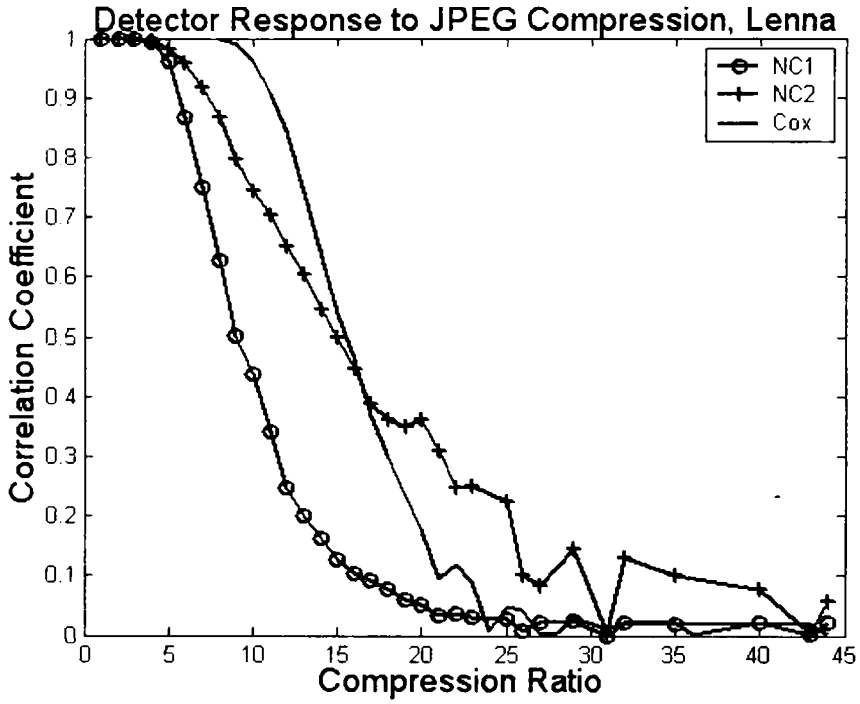


Fig. 4.11: Răspunsul detectorului la compresie JPEG, imagine test "Lenna" pentru metoda din [CKLS97] (linie continuă), metoda propusă, detectorul 1 ("o"), detectorul 2 ("+").

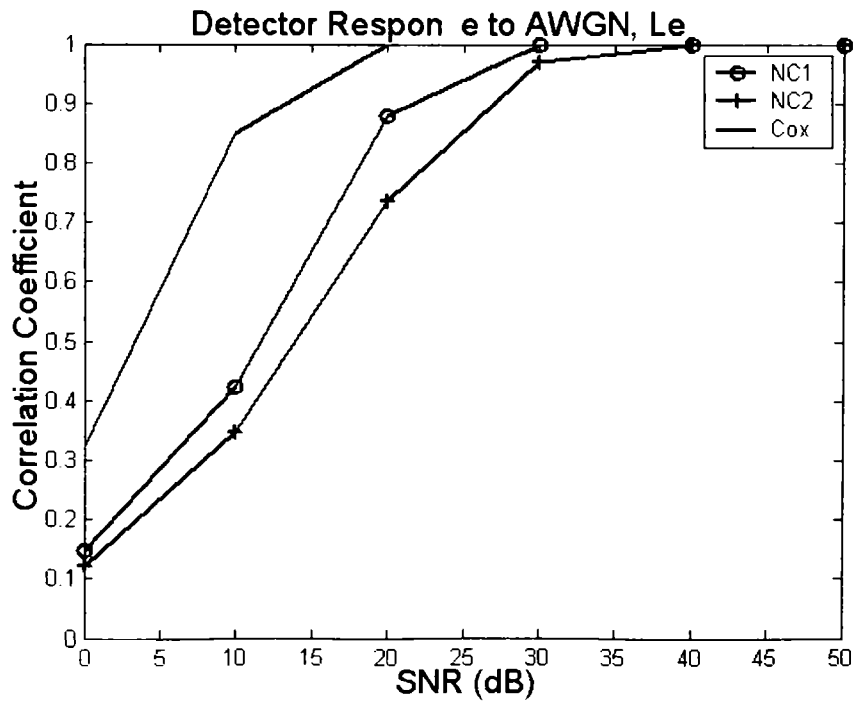


Fig. 4.12: Răspunsul detectorului la AWGN, imagine test "Lenna" pentru metoda din [CKLS97] (linie continuă), metoda propusă, detectorul 1 ("o"), detectorul 2 ("+").

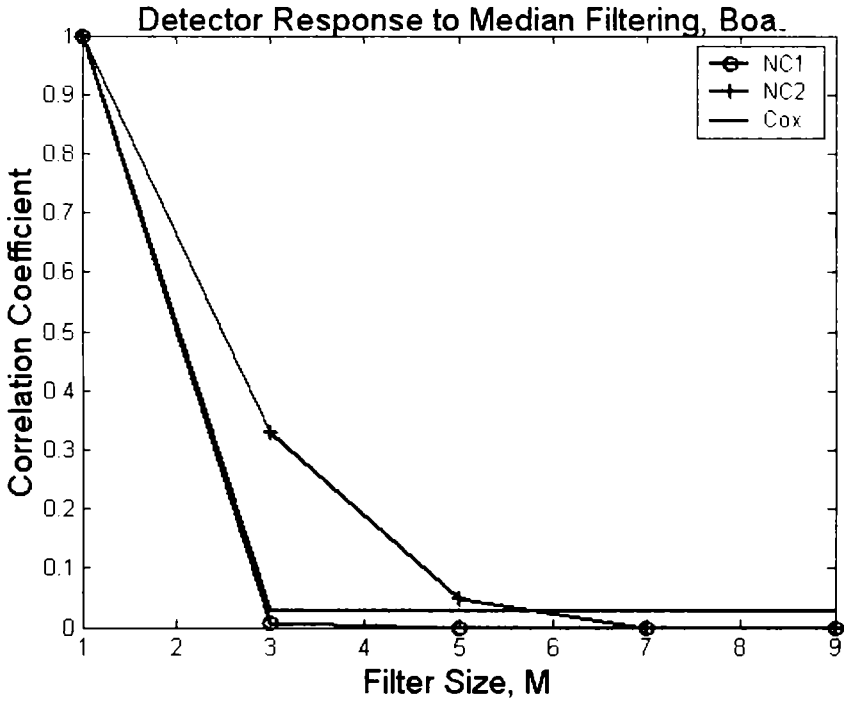


Fig. 4.13: Răspunsul detectorului la filtrarea mediană, imagine test "Boat" pentru metoda din [CKLS97] (linie continuă), metoda propusă, detectorul 1 ("o"), detectorul 2 ("+").

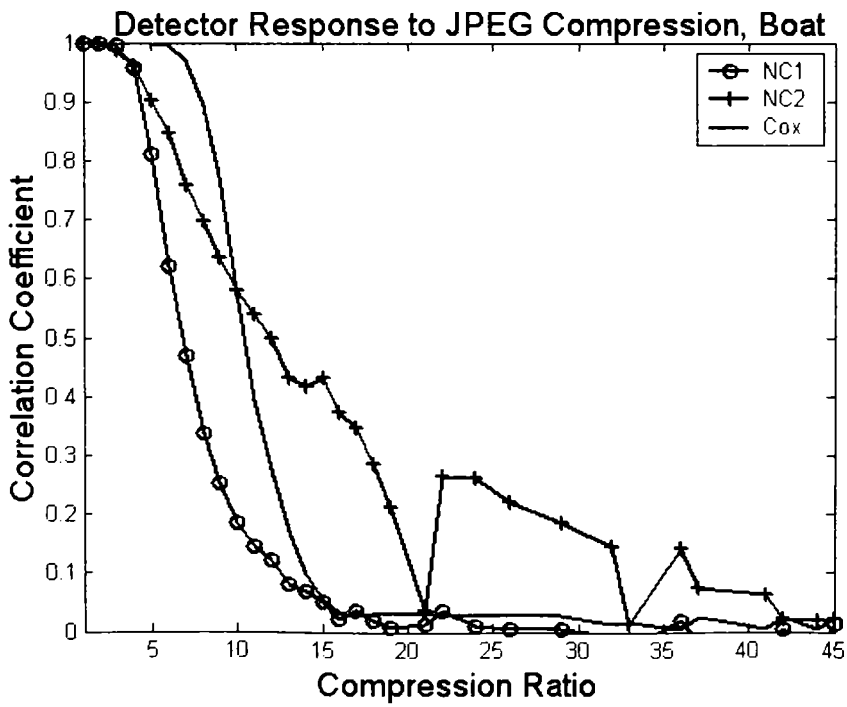


Fig. 4.14: Răspunsul detectorului la compresie JPEG, imagine test "Boat" pentru metoda din [CKLS97] (linie continuă), metoda propusă, detectorul 1 ("o"), detectorul 2 ("+").

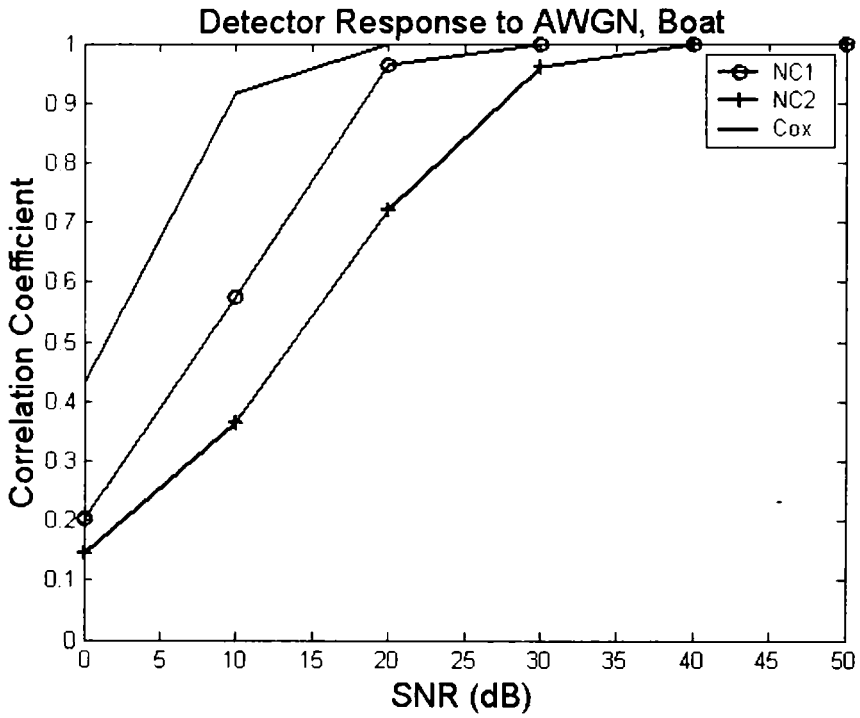


Fig. 4.15: Răspunsul detectorului la AWGN, imagine test "Boat" pentru metoda din [CKLS97] (linie continuă), metoda propusă, detectorul 1 ("o"), detectorul 2 ("+").

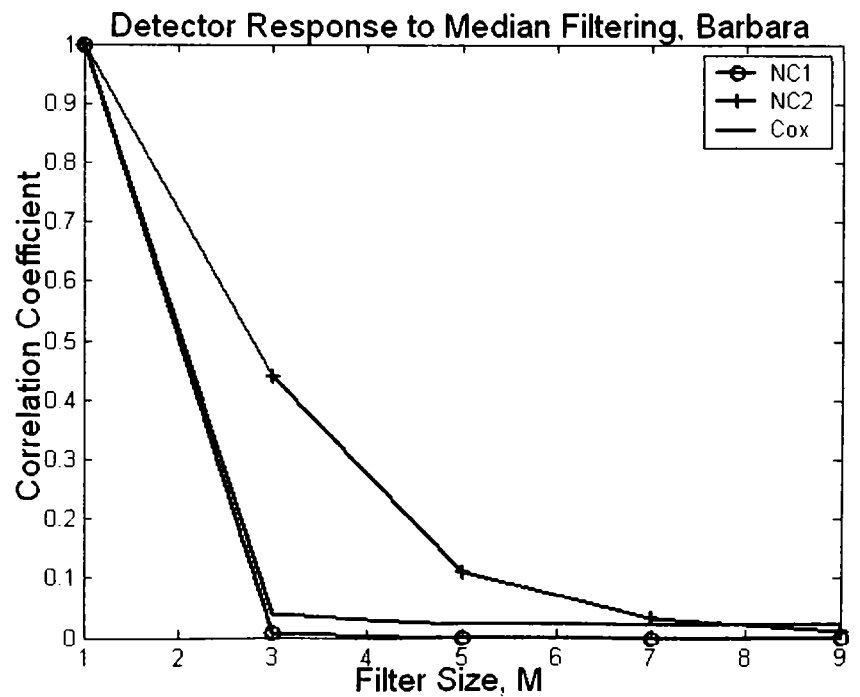


Fig. 4.16: Răspunsul detectorului la filtrarea mediană, imagine test "Barbara" pentru metoda din [CKLS97] (linie continuă), metoda propusă, detectorul 1 ("o"), detectorul 2 ("+").

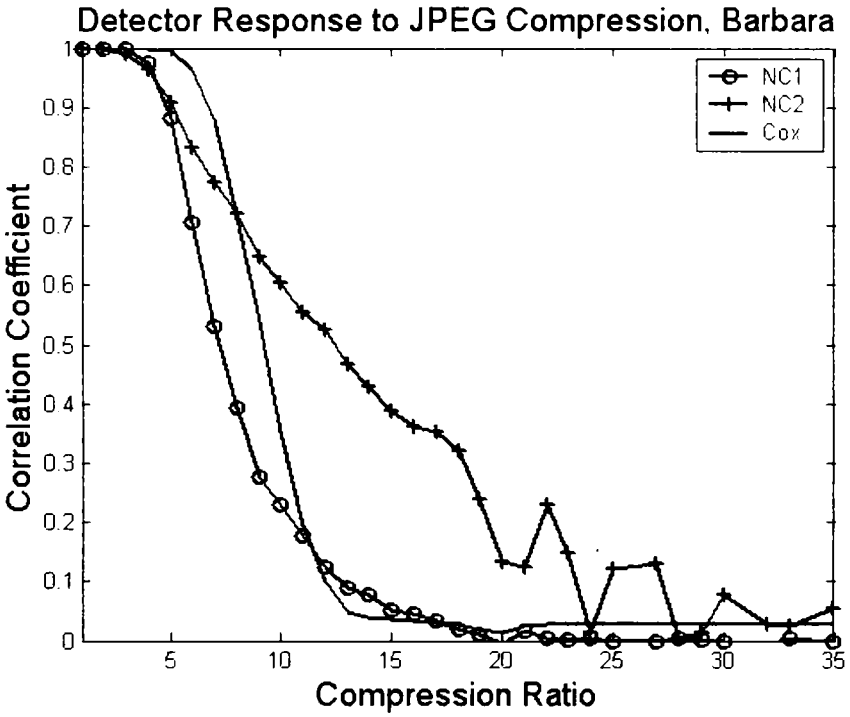


Fig. 4.17: Răspunsul detectorului la compresie JPEG, imagine test "Barbara" pentru metoda din [CKLS97] (linie continuă), metoda propusă, detectorul 1 ("o"), detectorul 2 ("+").

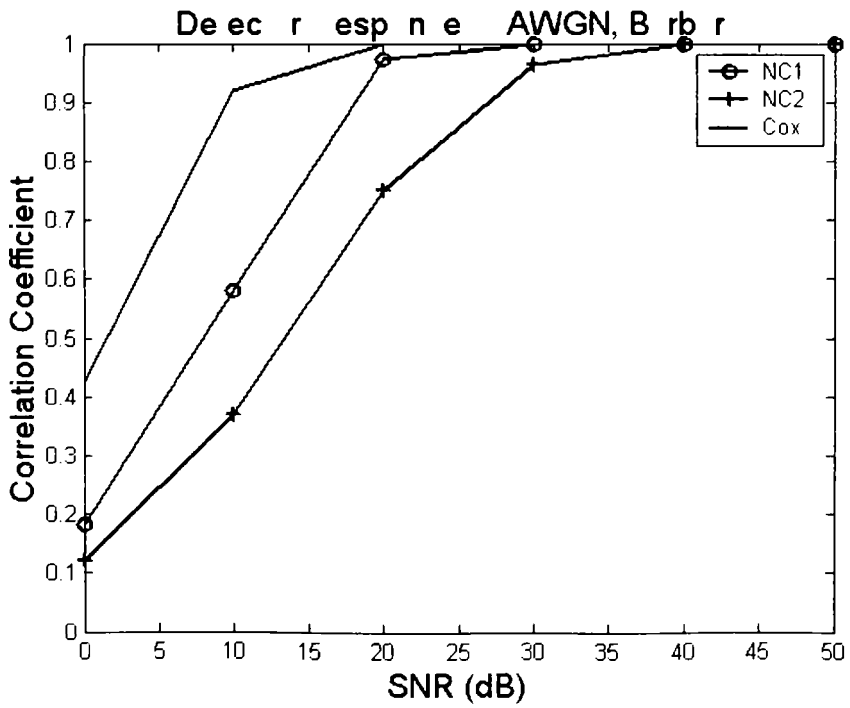


Fig. 4.18: Răspunsul detectorului la AWGN, imagine test "Barbara" pentru metoda din [CKLS97] (linie continuă), metoda propusă, detectorul 1 ("o"), detectorul 2 ("+").

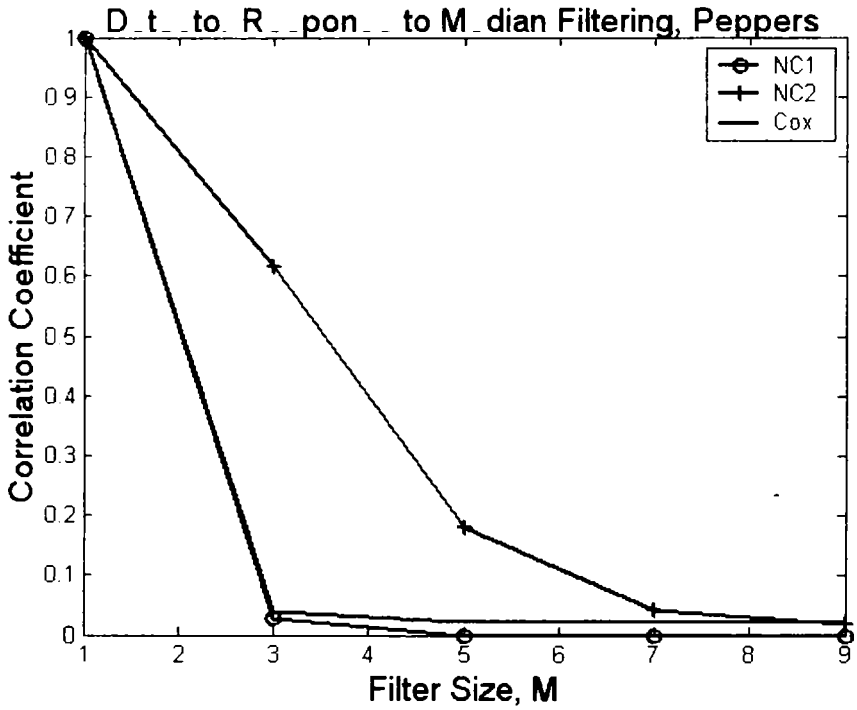


Fig. 4.19: Răspunsul detectorului la filtrarea mediană, imagine test "Peppers" pentru metoda din [CKLS97] (linie continuă), metoda propusă, detectorul 1 ("o"), detectorul 2 ("+").

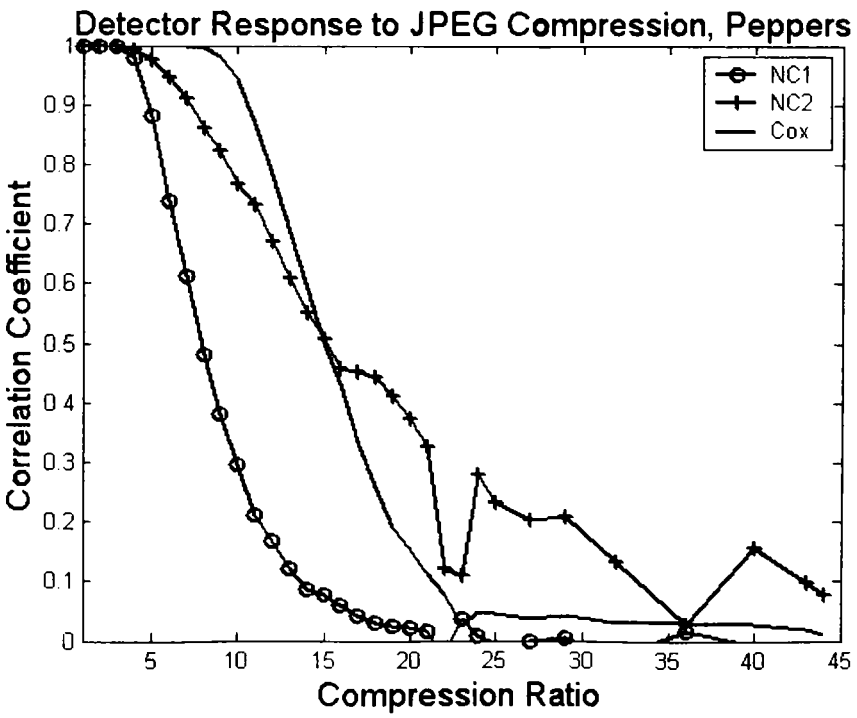


Fig. 4.20: Răspunsul detectorului la compresie JPEG, imagine test "Peppers" pentru metoda din [CKLS97] (linie continuă), metoda propusă, detectorul 1 ("o"), detectorul 2 ("+").

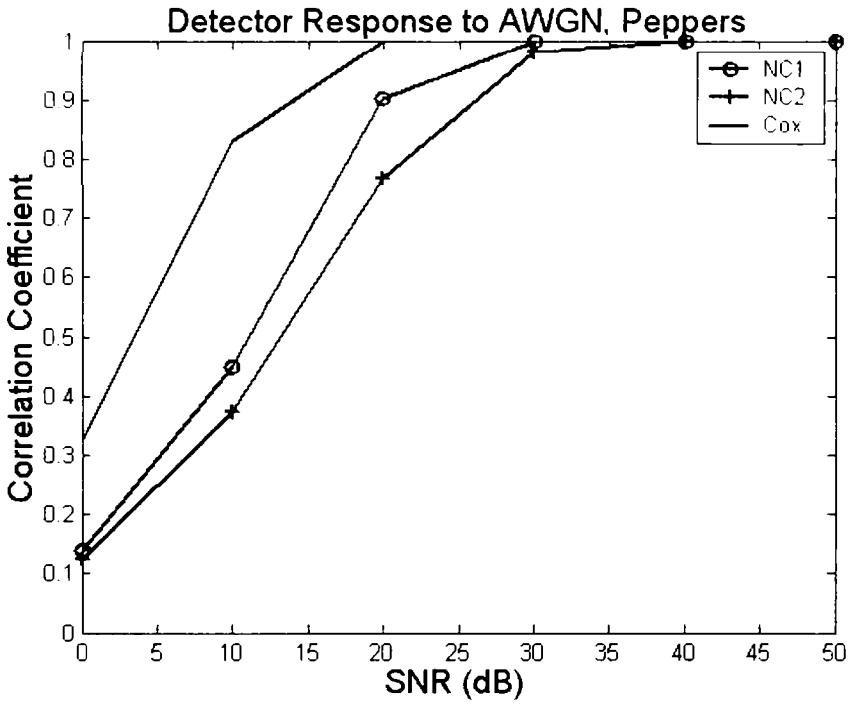


Fig. 4.21: Răspunsul detectorului la AWGN, imagine test "Peppers" pentru metoda din [CKLS97] (linie continuă), metoda propusă, detectorul 1 ("o"), detectorul 2 ("+").

Punând valoarea pragului la 0.5 în procesul de detecţie avem următoarele rezultate.

Atac prin filtrare mediană: Pentru imaginile marcate Lenna, Barbara şi Peppers, atacul prin filtrare mediană cu mărimea filtrului mai mare sau egal decât M=3 duce la o corelaţie mai mică decât 0.5.

De fapt numai detectorul NC2 detectează marcajul cu succes în urma filtrării cu M=3. Pentru imaginea Boat nici măcar detectorul NC2 nu reuşeste să detecteze marcajul.

Compresie JPEG: Pentru Lenna, corelaţia este mai mică decât 0.5 la o rată de compresie 16 (pentru detectorul NC2 şi Cox) şi respectiv CR 10 (NC1). Pentru Boat şi Barbara, corelaţia este mai mică decât 0.5 la o rată de compresie de 13 pentru NC2, 10 pentru Cox şi 7 pentru NC1. Pentru imaginea Peppers, valorile ratei de compresie pentru care corelaţia este mai mică decât 0.5 este 15 (NC2, Cox) şi respectiv 8 (NC1).

Atac AWGN: Pentru Lenna şi Peppers, răspunsul detectorului pentru metoda lui Cox ş.a. este peste 0.5 la un raport semnal-pe-zgomot de 5 dB, având o performaţă considerabil mai bună decât detectoarele NC1 (12 dB) şi NC2 (15 dB).

Pentru Boat şi Barbara, valorile detectorului sunt aproximativ egale pentru fiecare metodă: 3 dB (Cox), în jur de 14 dB (NC2) şi 7 dB (NC1).

O metodă robustă de marcare transparentă a fost prezentată în [Naf04b] ce inserează marcajul în coeficienţi selectaţi în aşa manieră încât schimbările să nu fie vizibile în imagine. Marcajul este inserat în texturi şi muchii ale imaginii folosind sistemul vizual uman. Ambele metode sunt dependente de imagine. Aparent metoda lui Cox şi alţii este superioară în cazul atacului AWGN, comparabilă cu detectorul NC2 pentru compresia JPEG, şi inferioară pentru filtrarea mediană. Aceste teste au fost efectuate însă pentru imagini marcate puternic în cazul metodei [CKLS97]. Metoda prezentată de mine este comparabilă sau mai bună decât metoda lui Cox ş.a. În cele ce urmează prezint **al treilea set de experimente**, care ia în considerare acest aspect.

Pentru toate simulările, care vor fi prezentate în continuare s-a folosit imaginea „Peppers" (256x256) şi o marcă binară având lungimea $N_w = 256$. S-a utilizat transformata wavelet cu funcţia mother wavelet Daubechies 5, cu 3 nivele de rezoluţie. Marcajul a fost generat aleator.

În toate testele s-au folosit următorii parametri: $q_1 = 0.06$, $q_2 = 0.04$, $q_3 = 0.02$. Mai exact, au fost afectaţi 8448 de coeficienţi din totalul de 65536 (incluzând subbanda LL), prin urmare numărul de repetiţii al marcajului original a fost pentru această imagine M=33. Intensitatea de marcare α a avut una dintre valorile 0.1, 0.2 şi 0.3.

Extragerea marcajului a fost realizată în două moduri [Naf05a]:

- din toate nivelele de rezoluţie, prin mediere, respectiv,
- din ultimul nivel de rezoluţie al transformatei, care poate fi afectat mai puţin de distorsiuni obişnuite ale semnalului.

S-a comparat metoda propusă [NBK04, Naf04b, NB05, Naf05b] cu tehnica spread-spectrum în domeniul DCT propusă de Cox ş.a.[CKLS97]. Pentru a face posibilă compararea cu metoda propusă, se inserează acelaşi marcaj binar şi acelaşi număr de repetiţii a marcajului ca în [NB05]. Imaginile rezultate pentru tehnica propusă de Cox ş.a. [CKLS97] sunt vizibil distorsionate faţă de cele originale, având raportul maxim semnal-pe-zgomot (PSNR) în jur de 25 dB, ceea ce este inacceptabil. Fixând valoarea β = 0,01, 0,02 şi 0,03, imaginile marcate cu tehnica SS au PSNR comparabil cu cele marcate cu tehnica propusă. Sunt considerate separat trei cazuri: a) α = 0.1 şi β = 0.01; b) α = 0.2 şi β = 0.02; c) α = 0.3 şi β = 0.03.

Imaginea originală Peppers, precum şi imaginile marcate cu cele două metode sunt prezentate în Figurile 4.22, 4.23 şi 4.24. Observatorii umani nu pot face distincţie între imaginea originală şi imaginile marcate.

În Tabelul 4.2 se prezintă valorile PSNR pentru fiecare imagine marcată (Peppers, Lena, Boat şi Barbara) ca o măsură a distorsiunilor introduse de marcaj.

Tab. 4.2: Valori PSNR [dB] pentru imaginile marcate, tabel din [NB05]

Metodă / Imagine	Metoda propusă [NB05]			Metoda lui Cox [CKLS97]		
	α=0.1	α=0.2	α=0.3	β=0.01	β=0.02	β=0.03
Peppers	45.54	40.28	36.94	45.75	39.73	36.21
Lena	45.39	40.12	36.77	47.19	41.17	37.65
Boat	44.35	38.86	35.45	45.35	39.33	35.81
Barbara	44.18	38.7	35.27	46.44	40.42	36.90

Fig. 4.22: Imagine originală Peppers

Fig. 4.23 (a): Imagine marcată [NB05], pentru α =0.1, PSNR=45.54 dB.

Fig. 4.23(b): Imagine marcată [NB05], pentru α = 0.2, PSNR=40.28 dB

Fig. 4.23(c): Imagine marcată [NB05], pentru α = 0.3, PSNR=36.94 dB

Fig. 4.24(a): Imagine marcată cu metoda SS din [CKLS97], pentru β=0.01, PSNR=45.75 dB

Fig. 4.24(b): Imagine marcată cu metoda SS din [CKLS97], pentru β=0.02, PSNR = 39.73dB

Fig. 4.24(c): Imagine marcată cu metoda SS din [CKLS97], pentru β=0.03, PSNR = 36.21dB

Pentru a demonstra robusteţea noii metode [NB05], se investighează efectul distorsiunilor obişnuite asupra coeficientului de corelaţie între marcajul original şi cel recuperat. Se compară performanţele acestei metode cu cele ale metodei propuse de Cox ş.a. [CKLS97]. Imaginile marcate au fost atacate prin filtrare mediană, compresie JPEG, zgomot aditiv alb Gaussian, AWGN, compresie JPEG2000, redimensionare, ajustarea contrastului, decupare. În Tabelele 4.3, 4.4 şi 4.5 se prezintă răspunsul detectorului pentru cele două metode, atunci când imaginile marcate sunt distorsionate prin compresie cu pierderi (JPEG şi JPEG2000) cu rate de compresie diferite, atac AWGN cu raportul semnal-pe-zgomot 11.4 dB, redimensionare la jumătate, filtrare mediană cu dimensiunea filtrului 3x3, ajustarea contrastului şi decupare. Din valorile din tabele se observă că metoda propusă funcţionează mai bine decât cea a lui Cox, pentru toate atacurile, cu mici excepţii, când oricum, marca nu este detectabilă în ambele cazuri (de exemplu, în Tabelul 4.3, α=0.1 şi β=0.01 la ajustarea contrastului). De fapt, rezultatele pentru metoda lui Cox sunt mult mai slabe şi nu detectează marca în prezenţa celor mai multe atacuri (compresie JPEG cu rata de compresie mai mare decât 10, decupare, redimensionare, filtrare mediană, ajustarea contrastului, compresie JPEG2000 cu rata de compresie mai mare de 10).

În ceea ce priveşte rezultatele obţinute cu metoda originală, detectorul 2 are performanţe mai bune în cazul compresiei cu pierderi, filtrare mediană, rescalare, în timp ce detectorul 1 are rezultate mai bune pentru atacul AWGN. În cazul decupării, cele două tipuri de detectoare au aceleaşi rezultate. În cazul ajustării contrastului, marcajul este detectat de ambele detectoare numai pentru α = 0.3. Răspunsurile detectoarelor, obţinute pentru imaginile comprimate cu JPEG2000, sunt mult mai

mari decât cele obţinute pentru imaginile comprimate cu JPEG, evidenţiindu-se astfel robusteţea marcajului inserat în domeniul DWT.

Cu cât este mai mare intensitatea de marcare α, cu atât sunt mai bune performanţele metodei [NB05]. Cu toate acestea există un *compromis între robusteţe şi invizibilitate*, pe baza căruia intensitatea de inserare ar trebui limitată la α=0.2.

Tab. 4.3: Răspunsul detectorului pentru imagini marcate distorsionate [NB05]

Metodă / Atac	Metoda propusă [NB05], α=0.1		Metoda Cox ş.a. β=0.01
	Detector 1	Detector 2	
JPEG, Q=75 (CR=5.5)	0.78	**0.98**	0.59
JPEG, Q=50 (CR=8.3)	0.50	**0.92**	0.35
JPEG, Q=25 (CR=12.8)	0.16	**0.65**	0.04
JPEG, Q=20 (CR=15)	0.09	**0.54**	0
Decupare, 1/2	0.30	**0.34**	0
AWGN, SNR=11.4dB	**0.55**	0.36	0.12
Redimensionare 256->128->256	0	**0.14**	0
Filtrare mediană, 3*3	0.02	**0.60**	0
Ajustarea contrastului	0	0.03	0
JPEG2000, CR = 5	**0.96**	0.89	0.47
JPEG2000, CR = 10	0.20	**0.66**	0.14
JPEG2000, CR = 15	0.03	**0.43**	0.03
JPEG2000, CR = 20	0	**0.32**	0
JPEG2000, CR = 25	0	**0.27**	0

Tab. 4.4: Răspunsul detectorului pentru imagini marcate distorsionate [NB05]

Metodă / Atac	Metoda propusă [NB05], α=0.2		Metoda Cox ş.a., β=0.02
	detector 1	detector 2	
JPEG, Q=75 (CR=5.5)	0.97	**0.99**	0.89
JPEG, Q=50 (CR=8.3)	0.71	**0.97**	0.56
JPEG, Q=25 (CR=12.8)	0.32	**0.80**	0.11
JPEG, Q=20 (CR=15)	0.21	**0.78**	0.03
Decupare, 1/2	0.42	0.40	0.007
AWGN, SNR=11.4dB	**0.86**	0.78	0.38
Redimensionare 256->128->256	0.08	**0.52**	0
Filtrare mediană, 3*3	0.13	**0.82**	0
Ajustarea contrastului	0	**0.22**	0
JPEG2000, CR = 5	**0.99**	0.98	0.85
JPEG2000, CR = 10	0.56	**0.93**	0.24
JPEG2000, CR = 15	0.24	**0.78**	0.04
JPEG2000, CR = 20	0	**0.59**	0.01
JPEG2000, CR = 25	0	**0.51**	0

Tab. 4.5: Răspunsul detectorului pentru imagini marcate distorsionate [NB05]

Metodă / Atac	Metoda propusă [NB05], α=0.3		Metoda Cox et al., β=0.03
	detector 1	detector 2	
JPEG, Q=75 (CR=5.5)	0.99	**1**	0.99
JPEG, Q=50 (CR=8.3)	0.85	**1**	0.67
JPEG, Q=25 (CR=12.8)	0.40	**0.89**	0.18
JPEG, Q=20 (CR=15)	0.25	**0.89**	0.09
Decupare, 1/2	0.44	**0.45**	0
AWGN, SNR=11.4dB	**0.89**	0.78	0.39
Redimensionare 256->128->256	0.015	**0.53**	0
Filtrare mediană, 3*3	0.25	**0.96**	0
Ajustarea contrastului	**1**	**0.95**	0
JPEG2000, CR = 5	**1**	0.99	0.92
JPEG2000, CR = 10	0.67	**0.97**	0.34
JPEG2000, CR = 15	0.35	**0.84**	0.10
JPEG2000, CR = 20	0.12	**0.71**	0.01
JPEG2000, CR = 25	0.07	**0.66**	0

4.5 Detecţie îmbunătăţită prin metoda max-correlation

Al treilea detector extrage fiecare estimată, $\hat{w}_r$, a marcajului original, şi calculează coeficientul de corelaţie dintre $\hat{w}_r$ şi w [Naf05b]. Marcajul pentru care se înregistrează valoarea maximă a corelaţiei cu marcajul original se consideră rezultatul aplicării detectorului 3. Se face o comparaţie cu celelalte două detectoare, pentru cazul $\alpha = 0.2$, pentru diverse atacuri (Tabelul 4.6). Al treilea detector are performanţe mai bune faţă de primul, iar detectorul 2 are performanţe mai bune sau similare decât detectorul 3, cu excepţia atacului prin decupare sau ajustare a contrastului.

Tab. 4.6: Comparaţie între cele trei detectoare pentru diverse atacuri [Naf05b]

Atac vs. răspunsul detectorului	Tip detecţie		
	1	2	3
JPEG, CR = 14.85	0.21	0.78	0.69
Filtrare mediană, 3*3	0.13	0.82	0.81
Redimensionare, 256->128->256	0.03	0.45	0.31
AWGN, SNR = 11.4 dB	0.82	0.57	0.49
Decupare ½	0.42	0.44	**0.64**
Ajustarea contrastului	0	0.22	**0.31**
JPEG 2000, CR=10	0.56	0.93	0.85
JPEG 2000, CR=15	0.24	0.78	0.64

În Tabelul 4.7 se prezintă răspunsul celor trei tipuri de detectoare pentru atacul de coliziune, prin medierea a patru imagini marcate. Este evident că al treilea detector este mai bun decât primele două, deoarece estimarea marcajului se face în

funcţie de marcajul original care este posibil inserat în imagine. Cu alte cuvinte, marcajul rezultat este cel mai asemănător cu cel original.

Tab. 4. 7: Comparaţie între cele trei detectoare pentru atacul de coliziune (mediere a patru imagini marcate) [Naf05b]

Tip detecţie vs. răspunsul detectorului	Marca originală			
	W_1	W_2	W_3	W_4
Tip I	0.35	0.25	0.41	0.49
Tip II	0.36	0.30	0.39	0.44
Tip III, W = W_1	**0.47**	0.35	0.30	0.38
Tip III, W = W_2	0.37	**0.40**	0.29	0.42
Tip III, W = W_3	0.39	0.30	**0.42**	0.38
Tip III, W = W_4	0.28	0.35	0.36	**0.49**

În Figurile 4.25-4.32 se prezintă valorile coeficienţilor de corelaţie pentru 1000 de marcaje generate aleator. Pentru majoritatea atacurilor (cu excepţia celui de coliziune) numai marca numărul 500 ar trebui să fie pozitiv detectată. În cazul atacului de coliziune, ar trebui detectate marcajele cu numerele 200, 400, 600 şi 800, deoarece acestea au fost mediate. De asemenea se dau valorile PSNR dintre imaginile marcate distorsionate şi cele marcate nedistorsionate.

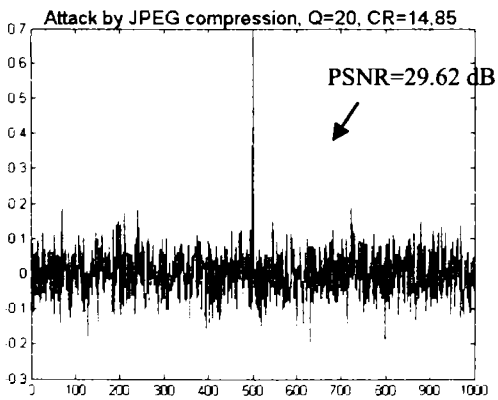


Fig. 4.25: Răspunsul detectorului 3 la 1000 marcaje generate aleator după compresie JPEG [Naf05b].

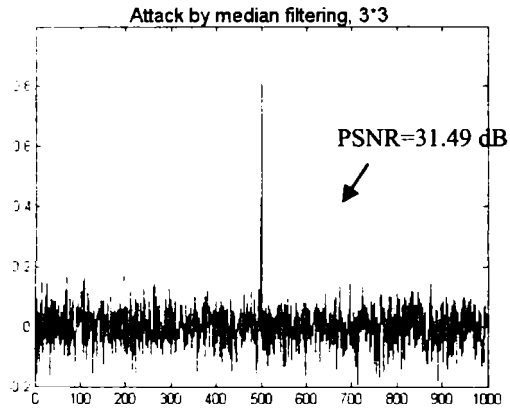


Fig. 4.26: Răspunsul detectorului 3 la 1000 marcaje generate aleator după atacul de filtrare mediană [Naf05b].

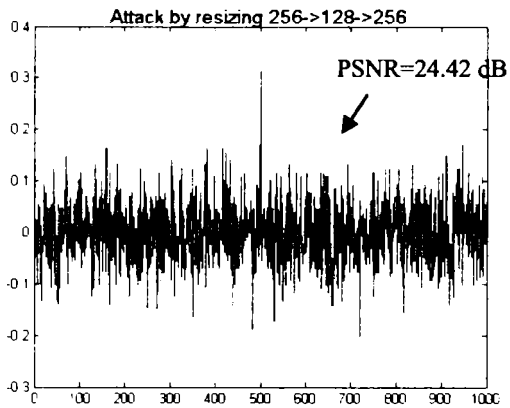


Fig. 4.27: Răspunsul detectorului 3 la 1000 marcaje generate aleator după atacul de redimensionare [Naf05b].

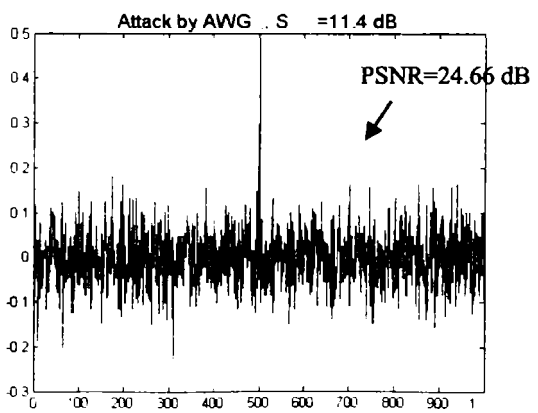


Fig. 4.28: Răspunsul detectorului 3 la 1000 marcaje generate aleator după atacul AWGN [Naf05b].

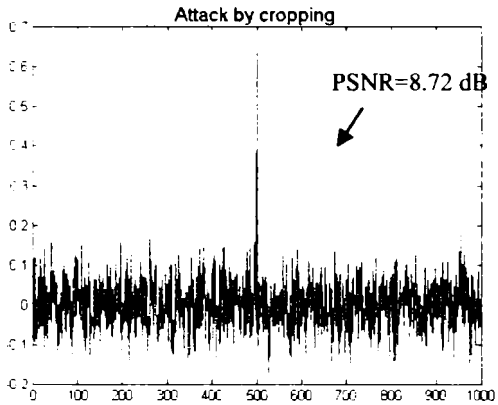


Fig. 4.29: Răspunsul detectorului 3 la 1000 marcaje generate aleator după atacul de decupare [Naf05b].

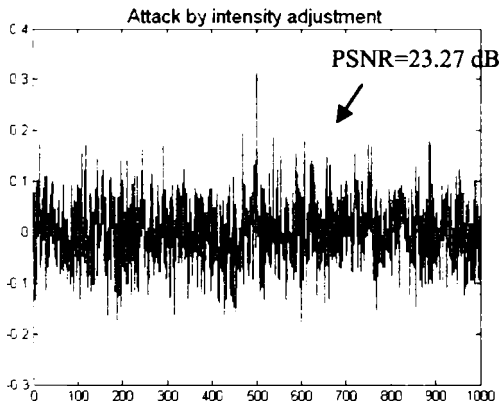


Fig. 4.30: Răspunsul detectorului 3 la 1000 marcaje generate aleator, după modificarea contrastului [Naf05b].

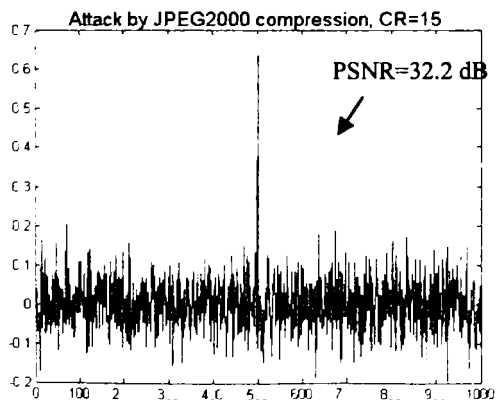


Fig. 4.31: Răspunsul detectorului 3 la 1000 marcaje generate aleator, după compresie JPEG 2000 [Naf05b].

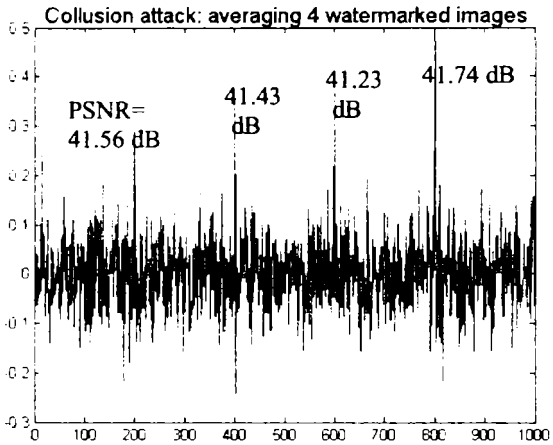


Fig. 4.32: Răspunsul detectorului 3 la 1000 marcaje generate aleator ($W_{orig}=W_4$), după coliziune [Naf05b].

4.6 A treia metodă de marcare informată. O abordare statistică

La fel ca mai înainte, imaginea originală se descompune pe trei nivele de rezoluţie, adică într-o imagine de aproximaţie $f_{a,3}$ şi câte trei imagini de detaliu pentru fiecare nivel de rezoluţie. Operaţia definită de $\oplus$ din relaţia (4.4) este de această dată:

$$f_{s,l}^{w}(m,n) = f_{s,l}(m,n) + \alpha \cdot \left| f_{s,l}(m,n) \right| w(m,n) \qquad (4.12)$$

unde $s \in \{h, v, d\}$, $l = 1,...,L$ iar α este o variabilă definită de utilizator, astfel încât $\alpha \in (0,1)$. Prin urmare, operaţia definită de Θ din relaţia (4.5) este în acest caz:

$$\hat{w}(m,n) = \frac{r_{s,l}(m,n) - f_{s,l}(m,n)}{\alpha \cdot \left| f_{s,l}(m,n) \right|} \qquad (4.13)$$

Dacă $r_{s,l}(m,n) = f_{s,l}(m,n)$ şi/sau dacă $f_{s,l}(m,n) = 0$, se face o alegere aleatoare pentru $w(m,n)$.

Generarea cheii se face pentru trei nivele de rezoluţie, cu relaţia (4.1b), folosind caracteristici statistice ale coeficienţilor wavelet [NIB05]. Pragurile $T_{s,l}$ sunt definite după cum urmează:

$$T_{s,l} = m_{s,l}\sigma_{s,l} \tag{4.14}$$

unde $\sigma_{s,l}$ reprezintă abaterea standard a coeficienţilor wavelet pentru subbanda *s*, din nivelul de rezoluţie *l*, iar parametrii $m_{s,l}$ sunt selectaţi pe baza unei *analize statistice* a transformatei DWT [IML05].

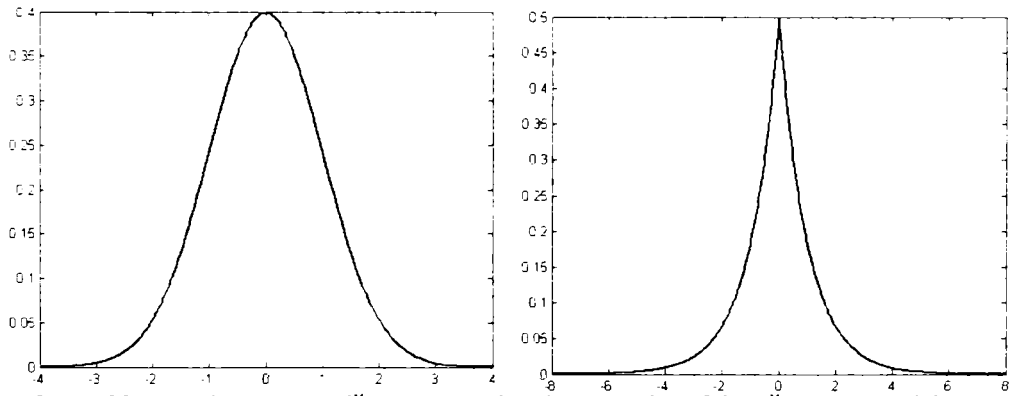


Fig. 4.33: Distribuţia normală, respectiv distribuţia Laplace folosită pentru modelarea caracteristicilor statistice ale coeficienţilor wavelet.

Funcţia de densitate de probabilitate, pdf, a coeficienţilor de detaliu wavelet scade mai repede decât pdf gaussiană (fiind o distribuţie *"heavy tailed"*), de aceea am ales ca model de repartiţie a coeficienţilor de detaliu distribuţia Laplace [SS02], reprezentată în Figura 4.33 :

$$f_{f_{s,l}}(y) = \frac{1}{2\sqrt{2}\sigma_{s,l}} \cdot \exp\left(-\frac{|y|}{\sqrt{2}\sigma_{s,l}}\right) \tag{4.15}$$

Probabilitatea de a selecta un coeficient wavelet de detaliu cu valoarea absolută mai mare decât pragul $T_{s,l}$ este dată de:

$$P_{T_{s,l}} = P\left(\left|f_{s,l}\right| > T_{s,l}\right) = 2 \cdot \exp\left(-\frac{T_{s,l}}{\sqrt{2}\sigma_{s,l}}\right) - 1 \tag{4.16}$$

Astfel, pragurile pot fi calculate după cum urmează:

$$T_{s,l} = \sqrt{2} \cdot \sigma_{s,l} \cdot \ln\left(\frac{2}{P_{T_{s,l}} + 1}\right) \tag{4.17}$$

Dacă se alege $P_{T_{s,l}} = 0,5$ şi dacă se ţine seama de relaţia dată în [IML05]:

$$\sigma_{s,l}^2 = 2^{2l-2} \cdot \sigma_{s,1}^2, \tag{4.18}$$

valorile de prag devin [NIB05]:

$$T_{s,l} = 0.2 \cdot 2^l \cdot \sigma_{s,1} \tag{4.19a}$$

Deci jumătate din coeficienţii wavelet de detaliu $f_{s,l}$ dintr-o anumită subbandă şi nivel de rezoluţie (*s*,*l*) sunt mai mari în valoare absolută decât pragurile $T_{s,l}$.

Dupa experimente s-a constatat că inserarea marcajului în mai puţini coeficienţi duce la o robusteţe crescută; astfel am folosit următoarele praguri:

$$T_{s,l} = 2^l \cdot \sigma_{s,1} \tag{4.19b}$$

Pe de altă parte, fiindcă se cere inserarea aceluiaşi marcaj original de mai multe ori, este nevoie de mai mulţi coeficienţi în fiecare subbandă (măcar N_w coeficienţi sau cu alte cuvinte, cel puţin o repetiţie a marcajului, mai ales pentru valori mari ale lui *l*). De aceea selecţia pragurilor se face adaptiv, cu iniţializarea la valorile indicate în relaţia (4.17). La fiecare iteraţie, valorile pragurilor descresc:

$$T_{s,l}(0) = T_{s,l}$$
$$T_{s,l}(p) = T_{s,l}(p-1) - 0.25$$

până când este satisfăcută condiţia ca măcar un marcaj să fie inserat într-o subbandă.

S-au efectuat simulări [NIB05] folosind tot imaginea Peppers, 256 x 256, şi o marcă de 256 de biţi. De asemenea, s-a folosit funcţia mother wavelet Daubechies 5 pentru a produce coeficienţii wavelet, cu un număr de nivele de rezoluţie *L* = 3.

Intensitatea de marcare a fost fixată la α = 0.1. Prin alegerea noilor praguri, s-au afectat numai 2816 coeficienţi din 65536, astfel că numărul de repetiţii al marcajului original este în final M=11. Imaginea nu este afectată de procesul de marcare care este transparent, valoarea PSNR fiind în acest caz de 44.95 dB.

Din nou se analizează robusteţea metodei la aceleaşi tipuri de atacuri, şi se face o comparaţie cu metoda propusă de Cox ş.a. [CKLS97]. De data aceasta, marcajul binar de 256 de biţi este înserat o singură dată în coeficienţii DCT cei mai mari, aşa cum am descris mai sus.

În Tabelul 4.8 este prezentat răspunsul detectorului pentru cele două metode comparate, atunci când imaginea marcată este atacată prin compresie cu pierderi JPEG, cu factor de calitate 75, 50, 25, 20 şi JPEG2000, cu rata de compresie 5, 10 şi 15, cu AWGN cu raportul semnal-pe-zgomot SNR=11.4 dB, prin redimensionare la jumătate, prin filtrare mediană cu dimensiunea filtrului 3 şi 5,

prin ajustarea contrastului şi prin decupare. Din valorile din tabel de observă că metoda este mai performantă decât cea din [CKLS97] pentru toate atacurile.

Tab. 4.8: Comparaţie între metoda propusă în [NIB05] şi metoda lui Cox [CKLS97].

Atac vs. Răspunsul detectorului	Metoda propusă [NIB05]			Metoda Cox et al.
	Detector 1	Detector 2	Detector 3	
JPEG, Q=75	0.9688	**1**	0.9922	0.8984
JPEG, Q=50	0.8281	**0.9531**	0.9063	0.7031
JPEG, Q=25	0.4219	**0.7813**	0.6875	0.4531
JPEG, Q=20	0.3281	**0.6797**	0.6641	0.3047
Filtrare mediană, 3*3	0.2891	0.7500	**0.7734**	0.4375
Filtrare mediană, 5*5	0.0234	0.2344	**0.3672**	0.1563
Redimensionare, 256->128->256	0.0703	0.2422	**0.2422**	0.0469
AWGN, SNR = 11.4 dB	**0.6484**	0.6094	0.5469	0.2734
Decupare ½	0.4219	0.3906	**0.5703**	-0.0156
Ajustarea contrastului	0.0234	0.0859	**0.1641**	0.0547
JPEG 2000, CR=15	0.5859	**0.6563**	0.6016	0.4844
JPEG 2000, CR=10	**0.9766**	0.8984	0.7891	0.6484
JPEG 2000, CR=5	**1**	0.9922	0.9922	0.8750

Se observă că detectorul 2 are rezultate mai bune pentru compresia cu pierderi, filtrare mediană, redimensionare şi ajustarea contrastului, în timp ce detectorul 1 are rezultate mai bune la atacul AWGN şi la compresia JPEG2000.

Detectorul 3 are performanţe mai bune decât detectorul 1, în cazul majorităţii atacurilor, şi performanţe comparabile cu detectorul 2, sau chiar mai bune în cazul filtrării, redimensionării, decupării, şi a ajustării contrastului.

În Tabelul 4.9 se prezintă răspunsurile detectoarelor 1 şi 2 pentru atacul de coliziune, cu medierea a patru imagini marcate cu marcaje diferite. Se observă că toate cele 4 marcaje sunt detectate.

Figura 4.34 arată imaginea marcată, folosind metoda propusă, marcajul ca imagine diferenţă. precum şi cheia de marcare care indică coeficienţii selectaţi pentru fiecare subbandă. Evident, aceştia se concentrează mai ales în zona contururilor şi a texturilor, (deoarece au fost selecţionaţi coeficienţii de detaliu cu cele mai mari valori), ceea ce face marcajul imperceptibil.

Tab. 4.9: Rezultate pentru atacul de coliziune, prin medierea a patru imagini marcate [NIB05]

Tip de detecţie	Marca originală			
	W_1	W_2	W_3	W_4
Tip 1	0.37	0.34	0.39	0.40
Tip 2	0.38	0.36	0.39	0.36

Fig.4.34(a): Imaginea marcată, PSNR=44.95 dB [NIB05]

Fig. 4.34(b): Marcaj ca diferenţă între imaginea originală Peppers şi cea din Figura 4. 34(a). Se observă că marcajul este concentrat în jurul contururilor şi texturilor [NIB05].

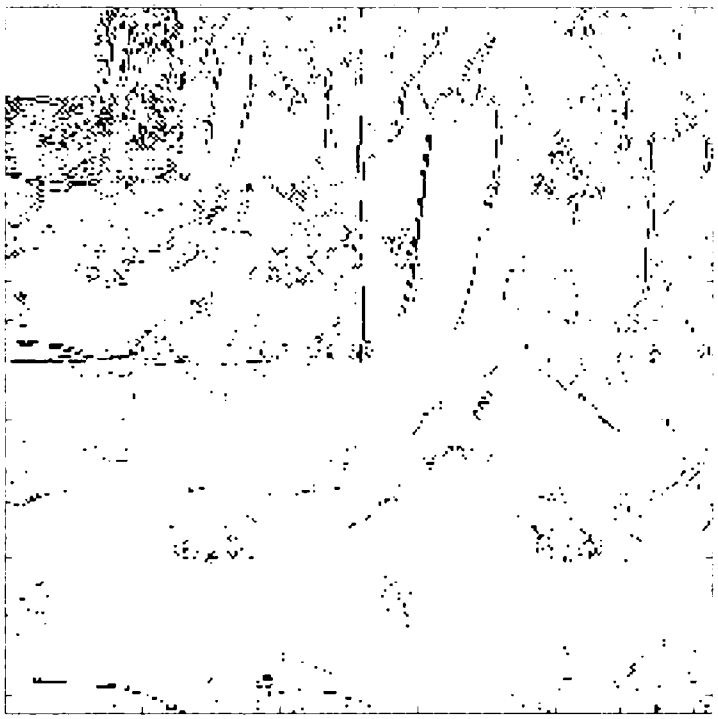


Fig.4.34(c): Cheia de marcare K, care indică coeficienţii selectaţi din fiecare subbandă pentru imaginea originală Peppers [NIB05].

4.7 Concluzii

S-au prezentat trei metode de marcare informată [NI03, NBK04, Naf04b, NB05, Naf05b, Naf05a, NIB05]. Metodele se bazează pe descompunerea multirezoluţie a imaginii cu transformata wavelet discretă. Se fac schimbări asupra unor coeficienţi wavelet, care nu vor avea un impact vizual asupra unui observator uman.

Coeficienţii au fost selectaţi folosind o detecţie cu logică de prag [NI03, NBK04, Naf04b, NB05, Naf05b]. Pragul depinde de coeficienţii wavelet ai fiecărei imagini de detaliu. Marcajul este înserat în texturi şi muchii ale imaginii folosind sistemul vizual uman.

Prima metodă [NI03] înserează şi detectează marcajul în/din subbanda de detalii diagonale al primului nivel de rezoluţie, respectiv în toate subbenzile primului nivel; evident, deşi a doua abordare afectează mai mult imaginea, marcajul se dovedeşte a fi mai robust la prelucrări obişnuite de semnal (compresie JPEG, filtrare mediana, zgomot AWGN). Metoda este comparata cu cea din [KH98]. Coeficientul de intercorelaţie pentru metoda propusă este mai mare decât pentru metoda propusă în [KH98], în cazul compresiei JPEG şi zgomot alb gaussian aditiv. Cu toate acestea, metoda propusă nu prezintă robusteţe împotriva filtrării mediane, comparativ cu metoda din [KH98].

A doua metodă inserează marcajul în cele trei nivele de rezoluţie, exceptând imaginea de aproximare, folosind acelaşi mod de selecţie a coeficienţilor

wavelet. Detecţia se face din **(1)** toate nivele mediat, prin decizie majoritară, sau **(2)** din ultimul nivel de rezoluţie, mai puţin afectat de diverse prelucrări de semnal.

Un **set preliminar de experimente** [Naf04a] face o comparaţie a metodei cu metoda de tip cuantizare prezentată în [KH98], se dovedeşte că metoda mea este mai robustă. Se observă că performanţele metodei propuse [Naf04a] sunt superioare metodei din [KH98]. De asemenea, coeficientul de intercorelaţie este mai mare dacă extragerea marcajului se face numai din ultimul nivel de rezoluţie. Acest lucru se datoreşte faptului că distorsiunile obişnuite ale semnalului sunt mai semnificative pentru componentele spectrale mai înalte ale imaginii.

Un al doilea set de experimente a fost efectuat folosind patru imagini; s-a făcut o comparaţie a metodei propuse [Naf04b] cu cea de tip spread-spectrum prezentată în [CKLS97]. Aparent metoda lui Cox şi alţii este superioară în cazul atacului AWGN, comparabilă cu detectorul NC2 pentru compresia JPEG, şi inferioară pentru filtrarea mediană. Aceste teste au fost efectuate pentru imagini marcate puternic în cazul metodei [CKLS97].

Al treilea set de experimente [NB05] ia în considerare acest aspect, selectând intensitatea de marcare mai mică astfel încât imaginile să nu fie vizibil afectate de procesul de marcare pentru metoda din [CKLS97]. Imaginea Peppers este marcată cu diverse intensităţi şi apoi prelucrată cu diverse atacuri, compresie cu pierderi (JPEG şi JPEG2000), zgomot AWGN, redimensionare, filtrare mediană, ajustarea contrastului şi decupare. Metoda propusă funcţionează mai bine decât cea a lui Cox, pentru toate atacurile, cu mici excepţii, când, oricum, marca nu este detectabilă în ambele cazuri (de exemplu, pentru, α=0.1 şi β=0.01 la ajustarea contrastului). De fapt, rezultatele pentru metoda lui Cox sunt mult mai slabe şi nu detectează marca în prezenţa celor mai multe atacuri (compresie JPEG cu rata de compresie mai mare decât 10; decupare; redimensionare; filtrare mediană; ajustarea contrastului; compresie JPEG2000 cu rata de compresie mai mare de 10). Detectorul 2 are performanţe mai bune în cazul compresiei cu pierderi, filtrare mediană, rescalare, în timp ce detectorul 1 are rezultate mai bune pentru atacul AWGN.

În cazul decupării, cele două tipuri de detectoare au aceleaşi rezultate. În cazul ajustării contrastului, marcajul este detectat de ambele detectoare numai pentru α=0.3.

Răspunsurile detectoarelor, obţinute pentru imaginile comprimate cu JPEG2000, sunt mult mai mari decât cele obţinute pentru imaginile comprimate cu JPEG, evidenţiindu-se astfel robusteţea marcajului inserat în domeniul DWT.

Cu cât este mai mare intensitatea de marcare α, cu atât sunt mai bune performanţele metodei [NB05]. Cu toate acestea există un *compromis între robusteţe şi invizibilitate*, pe baza căruia intensitatea de inserare ar trebui limitată la valoarea α=0.2.

A treia metodă de marcare informată propune **o abordare statistică** [NIB05], unde se selectează *mai puţini coeficienţi wavelet* în care se înserează marcajul, deci numărul de repetiţii este mai mic, faţă de metoda 2. Răspunsul detectorului este mai bun faţă de metoda a doua, deoarece coeficienţii mari nu sunt atât de afectaţi de atacurile obişnuite (compresie, filtrare, etc.). Selecţia pragurilor este bazată pe proprietăţile statistice ale coeficienţilor wavelet.

Se observă că detectorul 2 are rezultate mai bune pentru compresia cu pierderi, filtrare mediană, redimensionare şi ajustarea contrastului, în timp ce detectorul I are rezultate mai bune la atacul AWGN şi la compresia JPEG2000.

Detectorul III are performanţe mai bune decât detectorul 1, în cazul majorităţii atacurilor, şi performanţe comparabile cu detectorul 2, sau chiar mai bune în cazul filtrării, redimensionării, decupării, şi a ajustării contrastului. Pentru atacul de coliziune, cu medierea a patru imagini marcate cu marcaje diferite, în cazul detectoarelor 1 şi 2, toate cele 4 marcaje sunt detectate.

Pentru metoda doi şi trei, s-au analizat **trei tipuri de detectoare** [NB05, Naf05b], care pot da rezultate diferite în funcţie de atacul la care a fost supusă imaginea:

- din toate nivelele de rezoluţie, prin mediere, respectiv,
- din ultimul nivel de rezoluţie al transformatei, care poate fi afectat mai puţin de distorsiuni obişnuite ale semnalului,
- prin **corelaţie maximă** cu marcajul căutat [Naf05b].

Este evident că al treilea detector este mai bun decât primele două, deoarece estimarea marcajului se face în funcţie de marcajul original care este posibil inserat în imagine. Cu alte cuvinte, marcajul rezultat este cel mai asemănător cu cel original.

Performanţele metodelor propuse [NI03, NBK04, Naf04b, NB05, Naf05b, Naf05a, NIB05] au fost comparate cu cele ale metodei propuse de Cox şi alţii în [CKLS97] respectiv cu metoda propusa de Kundur si Hatzinakos [KH98]. Metoda a demonstrat o performanţă mai bună în cazul tuturor atacurilor, în special din cauza utilizării transformatei DWT şi a analizei statistice a coeficienţilor wavelet.

5. APLICAREA TRANSFORMĂRII WAVELET ÎN MARCAREA PERCEPTUALĂ NEINFORMATĂ A IMAGINILOR

5.1 Introducere

Se studiază o metodă de marcare perceptuală [BBP01], care operează în domeniul wavelet. Aceasta se bazează pe tehnica de tip *spread spectrum* propusă de Cox ş.a. [CKLS97]. Detecţia nu foloseşte semnalul original, deci sistemul este public.

Masca perceptuală ţine cont de sensibilitatea la zgomot, textura si luminanţa tuturor subbenzilor. Prezentăm o mască perceptuală îmbunătăţită, unde conţinutul texturii este estimat folosind deviaţia standard locală a imaginii originale, comprimată în domeniul DWT, pentru a avea aceeaşi mărime ca şi marcajul de inserat. Eficienţa noii măşti este comparată cu cea propusă de Barni ş.a. [BBP01].

Capitolul de faţă are următoarea structură. În paragraful 5.2 se explică şi se exemplifică conceptul de marcare perceptuală. Scopul paragrafului 5.3 este descrierea metodei din [BBP01]. În paragrafele 5.4 şi 5.5 se prezintă construcţia noii măşti, [NIB06a], precum şi rezultate obţinute în urma simulărilor. Următorul paragraf prezintă o mască perceptuală şi mai generală, propusă în [NIB06b], care permite ascunderea datelor şi în subbenzile de frecvenţă mai joasă, ceea ce duce la o robusteţe crescută. Concluziile sunt enunţate în ultimul paragraf.

5.2 Marcare perceptuală

O cerinţă impusă unui sistem de marcare este imperceptibilitatea. Aceasta se poate îndeplini utilizând diverse metode.

O metodă este folosirea caracteristicilor statistice ale coeficienţilor wavelet a imaginii originale. Varianţa coeficienţilor wavelet poate fi estimată la orice nivel de rezoluţie, şi se pot detecta, folosind această estimare, coeficienţii cu valoare absolută mare, cu ajutorul unui detector de prag. Dacă se inserează marcajul în aceşti coeficienţi, corespunzând primelor trei nivele de rezoluţie, se obţine un marcaj robust. Robusteţea este proporţională cu valoarea pragului. Aceasta soluţie a fost propusă în [NIB05], unde robusteţea este crescută prin inserări multiple ale marcajului în subbenzile respective. Toţi biţii marcajului sunt inseraţi cu aceeaşi intensitate. Coeficienţii cu valoare absolută mare corespund contururilor, coeficienţii cu valoare absolută medie corespund texturilor, iar cei cu valoare absolută mică corespund zonelor omogene din imaginea originală.

Totuşi, această tehnică are dezavantaje: este dificil de inserat întregul mesaj în contururi, în special când mesajul este lung, deoarece numai o parte din pixeli se află pe contururile imaginii originale. Pentru mesaje mai lungi (care produc o încărcătură mai mare), valoarea pragurilor trebuie scăzută, ajungându-se astfel ca marcajul să fie inserat şi în texturile imaginii originale. Se poate spune deci că metoda enunţată foloseşte o mascare perceptuală. Dar analiza robusteţii acestei

metode nu este deloc simplă, în special când numărul de repetiţii ale marcajului este mare. Robusteţea se îmbunătăţeşte cu creşterea numărului de repetiţii, dar descreşte odată cu scăderea pragurilor. De fapt, există unii coeficienţi care nici nu sunt folosiţi pentru inserare.

Acesta este motivul pentru care în [BBP01] este propusă o abordare diferită pentru înglobarea marcajului. Se preferă să se insereze marcajul în toţi coeficienţii wavelet de detaliu dar se folosesc intensităţi diferite. Pentru coeficienţii din contururi se foloseşte o intensitate mai mare, pentru coeficienţii corespunzători texturilor se foloseşte o intensitate medie, iar pentru cei corespunzători zonelor omogene se foloseşte o intensitate mică. Aceasta este în concordanţă cu analogia între *water-filling* si *watermarking* propusă de Deepa Kundur în [Kun00].

5.3 Marcarea perceptuală propusă de Barni, Bartolini şi Piva

În continuare se prezintă mai întâi soluţia propusă în [BBP01] de Barni, Bartolini şi Piva.

A. Înserarea marcajului

Imaginea I, de marime 2M × 2N este descompusă pe 4 nivele de rezoluţie, folosind transformata wavelet discretă, Daubechies-6, unde I_l^θ este subbanda din nivelul $l \in \{0,1,2,3\}$ şi orientarea $\theta \in \{0,1,2,3\}$. Un marcaj binar $x_l^\theta(i,j)$ de lungime $3MN/2^l$ este inserat în toţi coeficienţii subbenzilor de detaliu de la nivelul l=0 (de frecvenţă înaltă/rezoluţie mare), prin adunare :

$$\tilde{I}_l^\theta(i,j) = I_l^\theta(i,j) + \alpha w_l^\theta(i,j) x_l^\theta(i,j) \tag{5.1}$$

unde α este intensitatea de marcare iar $w_l^\theta(i,j)$ este o funcţie de ponderare, a cărei valoare este egală cu jumătate din pasul de cuantizare, $q_l^\theta(i,j)$. Pasul de cuantizare este calculat în [BBP01] ca produsul ponderat a trei factori:

$$q_l^\theta(i,j) = \Theta(l,\theta)\Lambda(l,i,j)\Xi(l,i,j)^{0.2} \tag{5.2}$$

iar înserarea are loc doar în primul nivel de descompunere, l=0 (frecvenţă înaltă).

Primul factor reprezintă sensibilitatea la zgomot, depinzând de orientare şi de nivelul de rezoluţie:

$$\Theta(l,\theta) = \begin{Bmatrix} \sqrt{2}, & \theta = 1 \\ 1, & \text{altfel} \end{Bmatrix} \cdot \begin{Bmatrix} 1.00, & l = 0 \\ 0.32, & l = 1 \\ 0.16, & l = 2 \\ 0.10, & l = 3 \end{Bmatrix} \tag{5.3}$$

Al doilea factor ţine cont de luminozitatea locală, bazată pe nivelele de gri ale versiunii trece-jos a imaginii (adică sub-imaginea de aproximare de nivel 4 obţinută în urma calculului transformării wavelet):

$$\Lambda(l,i,j)=1+L'(l,i,j) \tag{5.4}$$

unde:

$$L'(l,i,j)=\begin{Bmatrix} 1-L(l,i,j), & L(l,i,j)<0.5 \\ L(l,i,j), & \text{altfel} \end{Bmatrix} \tag{5.5}$$

şi

$$L(l,i,j)=\frac{1}{256}I_3^3\left(1+\left\lfloor\frac{i}{2^{3-l}}\right\rfloor,1+\left\lfloor\frac{j}{2^{3-l}}\right\rfloor\right)$$

Al treilea factor este calculat după cum urmează:

$$\begin{aligned}\Xi(l,i,j)=&\sum_{k=0}^{3-l}\frac{1}{16^k}\sum_{\theta=0}^{2}\sum_{x=0}^{1}\sum_{y=0}^{1}\left[I_{k+l}^{\theta}\left(y+\frac{i}{2^k},x+\frac{j}{2^k}\right)\right]^2\\&\cdot\mathrm{Var}\left\{I_3^3\left(1+y+\frac{i}{2^{3-l}},1+x+\frac{j}{2^{3-l}}\right)\right\}_{\substack{x=0,1\\y=0,1}}\end{aligned} \tag{5.6}$$

Acesta reprezintă textura în vecinătatea unui pixel. El este compus din produsul a doi factori, primul fiind media locală pătratică a coeficienţilor wavelet din toate subimaginile de detaliu, în timp ce al doilea este dispersia locală a subbenzii de aproximare. Ambii factori sunt calculaţi într-o fereastră de 2 × 2 corespunzând pixelului localizat in (*i*, *j*). Primul factor poate reprezenta distanţa faţă de muchii în timp ce al doilea factor, textura.

Această estimare a dispersiei locale nu este prea de precisă, deoarece este calculată cu o rezoluţie joasă.

De aceea se prezintă o nouă metodă de estimare a texturii, dar şi a luminanţei [NIB06a, NIB06b].

B. Detecţia marcajului

Detecţia se face folosind coeficientul de corelaţie între coeficienţii wavelet marcaţi si biţii de marcaj:

$$\rho_l = \frac{4^l}{3MN} \sum_{\theta=0}^{2} \sum_{i=0}^{M/2^l-1} \sum_{j=0}^{N/2^l-1} \tilde{I}_l^{\theta}(i,j) x_l^{\theta}(i,j) \tag{5.7}$$

Corelaţia este comparată cu pragul T_l, calculat astfel încât probabilitatea de fals pozitiv sa aibă o anumită valoare, folosind criteriul Neyman-Pearson. De exemplu, dacă $P_f \le 10^{-8}$, pragul este $T_l = 3.97\sqrt{2\sigma_{\rho_l}^2}$, unde $\sigma_{\rho_l}^2$ este dispersia coeficienţilor wavelet, dacă imaginea a fost marcată cu un marcaj Y altul decât X:

$$\sigma_{\rho_l}^2 \approx \frac{16^l}{(3MN)^2} \sum_{\theta=0}^{2} \sum_{i=0}^{M/2^l-1} \sum_{j=0}^{N/2^l-1} \left(\tilde{I}_l^{\theta}(i,j)\right)^2 . \tag{5.8}$$

5.4 Masca perceptuală îmbunătăţită

Un alt mod de a genera al treilea factor din pasul de cuantizare, este prin segmentarea imaginii originale, găsindu-i contururile, texturile şi regiunile omogene, aşa după cum se poate observa în Figurile 5.1-5.6.

Criteriul folosit pentru această segmentare este valoarea deviaţiei standard locale a fiecărui pixel din imaginea originală [NIB06a]. Într-o fereastră glisantă pătratica $W(i,j)$, conţinând $W_S \cdot W_S$ pixeli, centrată pe fiecare pixel $I(m,n)$ din imaginea gazdă, media locală este calculată cu:

$$\hat{\mu}(i,j) = \frac{1}{W_S \cdot W_S} \sum_{I(m,n) \in W(i,j)} I(m,n) \tag{5.9}$$

iar dispersia locală este:

$$\hat{\sigma}^2(i,j) = \frac{1}{W_S \cdot W_S} \sum_{I(m,n) \in W(i,j)} \left(I(m,n) - \hat{\mu}(i,j)\right)^2 \tag{5.10}$$

Deviaţia standard locală estimată este radical din dispersia locală.

Fig. 5.1: Barbara

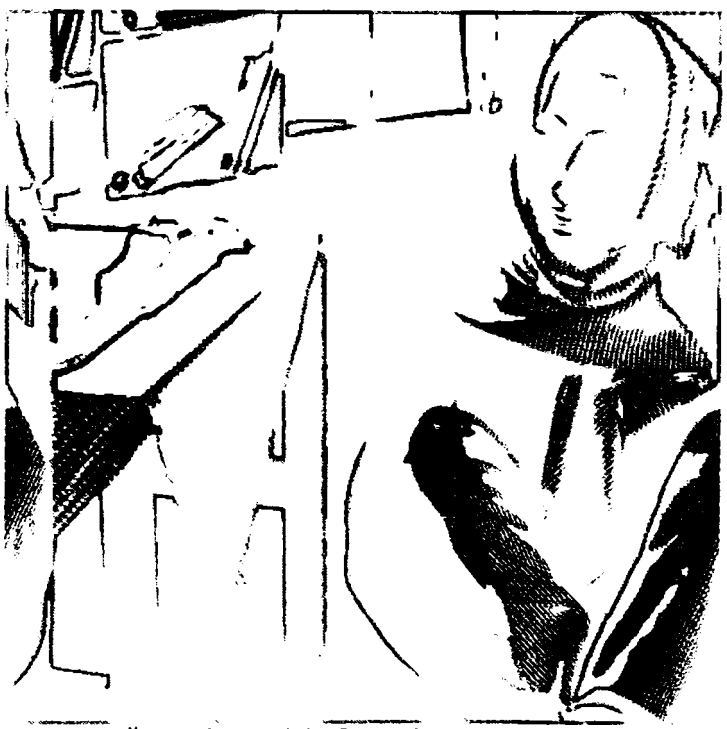


Fig. 5.2: Clasa corespunzătoare intervalului I_6 conţine contururi şi texturi grosiere [NIB06a]. Imaginea este complementara imaginii reale, adică zonele nesemnificative sunt reprezentate cu alb.

Fig. 5.3: Clasa corespunzătoare intervalului I_5 conţine contururi şi texturi [NIB06a]. Imaginea este complementara imaginii reale, adică zonele nesemnificative sunt reprezentate cu alb.

Fig. 5.4: Clasa corespunzătoare intervalului I_4 conţine texturi [NIB06a]. Imaginea este complementara imaginii reale, adică zonele nesemnificative sunt reprezentate cu alb.

Fig. 5.5: Clasa corespunzătoare intervalului I_3 conţine texturi [NIB06a]. Imaginea este complementara imaginii reale, adică zonele nesemnificative sunt reprezentate cu alb.

Fig. 5.6: Clasa corespunzătoare intervalului I_2 conţine texturi [NIB06a]. Imaginea este complementara imaginii reale, adică zonele nesemnificative sunt reprezentate cu alb.

Fig. 5.7: Clasa corespunzătoare intervalului I_1 conţine zone omogene [NIB06a]. Imaginea este complementara imaginii reale, adică zonele nesemnificative sunt reprezentate cu alb.

De exemplu, imaginea Barbara (Figura 5.1) poate fi segmentată în clase a căror elemente au ca valoare deviaţia standard normalizată [NIB06a], aparţinând unor intervale posibile $I_p = (\alpha_p, \alpha_{p+1})$, unde p ia valorile 1,...,6, iar $\alpha_1=0$, $\alpha_2=0.025$, $\alpha_3=0.05$, $\alpha_4=0.075$, $\alpha_5=0.1$, $\alpha_6=0.25$, $\alpha_7=1$ (Fig. 5.2-5.7).

Această imagine a fost aleasă pentru conţinutul bogat în contururi, texturi, dar şi zone omogene. În fiecare din Figurile 5.2-5.7 este reprezentată clasa corespunzând intervalului I_p, p = 1,...,6, celelalte elemente fiind ignorate (reprezentate cu alb). Trebuie menţionat că nivelele de gri reprezintă contururi şi texturi iar culoarea albă reprezintă zonele nesemnificative.

Aceste imagini demonstrează calitatea bună a segmentării bazate pe valorile deviaţiei locale standard. Astfel de imagini pot fi folosite pentru mascarea perceptuală în procesul de inserare a marcajului. Pasul de cuantizare pentru un coeficient wavelet este dat de o valoare direct proporţională cu deviaţia standard locală corespunzătoare pixelului din imaginea originală.

Pentru a asigura o mascare perceptuală, dimensiunile diferitelor subimagini de detalii trebuie să fie egale cu dimensiunile măştilor corespunzătoare. De aceea, imaginea de deviaţie standard locală este comprimată. Factorul de compresie cerut pentru o mască corespunzătoare nivelului de rezoluţie l este $4(l+1)$, pentru l = 0, ..., 3. Această compresie poate fi realizată în domeniul DWT.

Pentru generarea măştii folosite la inserarea marcajului în nivelul de rezoluţie l, se calculează transformata wavelet discretă a imaginii de deviaţie

standard locală, făcând / + 1 iteraţii. Imaginea de aproximare obţinută reprezintă rezultatul compresiei, sau cu alte cuvinte, masca cerută. Acest tip de compresie este ilustrat în Figura 5.8.

Fig. 5.8(a): Deviaţia standard locală a imaginii Barbara.
Imaginea este complementara imaginii reale.

Fig. 5.8(b): Deviaţia standard locală a imaginii Barbara, comprimată cu CR = 4.
Imaginea este complementara imaginii reale.

Fig. 5.8(c): Deviaţia standard locală a imaginii Barbara, comprimată cu CR=16.
Imaginea este complementara imaginii reale.

Diferenţa principală între sistemul de marcare propus în [BBP01] şi sistemul prezentat în [NIB06a], este dată de calculul dispersiei locale – al doilea factor – în relaţia (5.6). Pentru a obţine noile valori ale texturii, varianţa locală a imaginii este calculată, folosind relaţiile (5.9)-(5.10), cu dimensiunea ferestrei glisante $W_S = 7$.

Deviaţia standard locală este descompusă în domeniul wavelet şi este păstrată doar imaginea de aproximare a acesteia, normată cu media ei. Pentru obţinerea texturii este prezentată în Figura 5.9 o schemă generală.

Relaţia (5.6) este înlocuită cu:

$$\Xi(l,i,j) = \sum_{k=0}^{3-l} \frac{1}{16^k} \sum_{\theta=0}^{2} \sum_{x=0}^{1} \sum_{y=0}^{1} \left[I_{k+l}^{\theta}\left(y + \frac{i}{2^k}, x + \frac{j}{2^k} \right) \right]^2 \cdot \cdot \mathrm{DWT}_l^3 \left\{ \mathrm{Std}(I)_{x,y=\overline{0,7}} \right\} \tag{5.11}$$

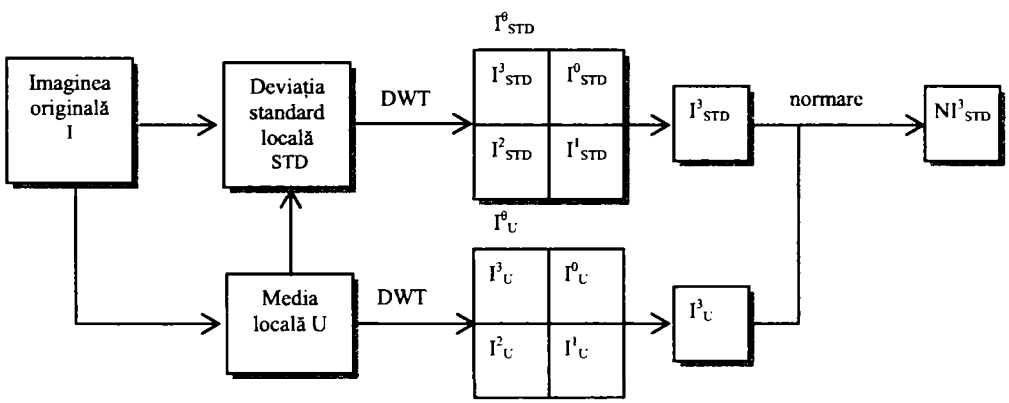


Fig. 5.9: O schemă generală pentru obţinerea texturii [NIB06a].

5.5 Testarea noii măşti perceptuale

Marcajul binar este înglobat în toate subimaginile de detaliu de la primul nivel de rezoluţie wavelet, folosind relaţiile (5.1)-(5.5). Imaginea Barbara a fost marcată cu diferite intensităţi de marcare α, între 0.1 şi 1.5.

Imaginea Barbara marcată pentru α=1.5 este prezentată în Figura 5.10. După cum se observă, nu există o diferenţă perceptibilă între imaginea originală şi cea marcată, valoarea raportului PSNR pentru această a doua imagine fiind de 45 dB.

Fiecare imagine marcată este comprimată JPEG folosind diverşi factori de calitate 5, 10, 15, 20, 25, 50.

Pentru a testa performanţa algoritmului, se prezintă în Figurile 5.11-5.14 rezultatele pentru compresie JPEG.

În Figurile 5.11 şi 5.12 se arată numai raportul ρ/T, ca funcţie de PSNR între imaginea marcată (neatacată) şi cea originală, respectiv ca funcţie de α. Pentru

fiecare PSNR şi fiecare factor de calitate Q, sunt calculate corelaţia ρ şi pragul T. Probabilitatea de fals pozitiv este 10^{-8}. Eficienţa sistemului de marcare propus poate fi măsurată folosind raportul ρ/T. Dacă ρ/T > 1, marcajul este detectat.

Fig. 5.10: Imaginea Barbara marcată cu α = 1.5, folosind metoda din [NIB06a].

Analizând Figura 5.11, se observă că marcajul poate fi detectat pentru un interval mare de valori PSNR, şi de factori de calitate Q. Pentru valori PSNR mai rnari decât 30 dB, marcajul este invizibil. Pentru factori Q ≥ 25, distorsiunea introdusă de compresia JPEG este tolerabilă.

Pentru valorile PSNR de la 30 dB la 35 dB, valori de interes practic, marcajul poate fi extras pentru toate valorile semnificative ale factorilor de calitate (Q ≥ 25). De aceea, sistemul propus este viabil.

Figura 5.12 arată dependenţa raportului ρ/T funcţie de puterea de marcare, α, în cazul compresiei JPEG. Dacă puterea de marcare creşte, valorile PSNR ale imaginilor marcate descresc, iar raportul ρ/T creşte.

Raportul ρ/T variază invers proporţional cu α, direct proporţional cu PSNR , şi invers proporţional cu rata de compresie.

Marcajul este detectabil pentru valori foarte mici ale lui α. Pentru factorul de calitate Q=5 (sau o rata de compresie CR=32), marcajul este detectabil chiar pentru valori mici ale lui α, adică 0.5.

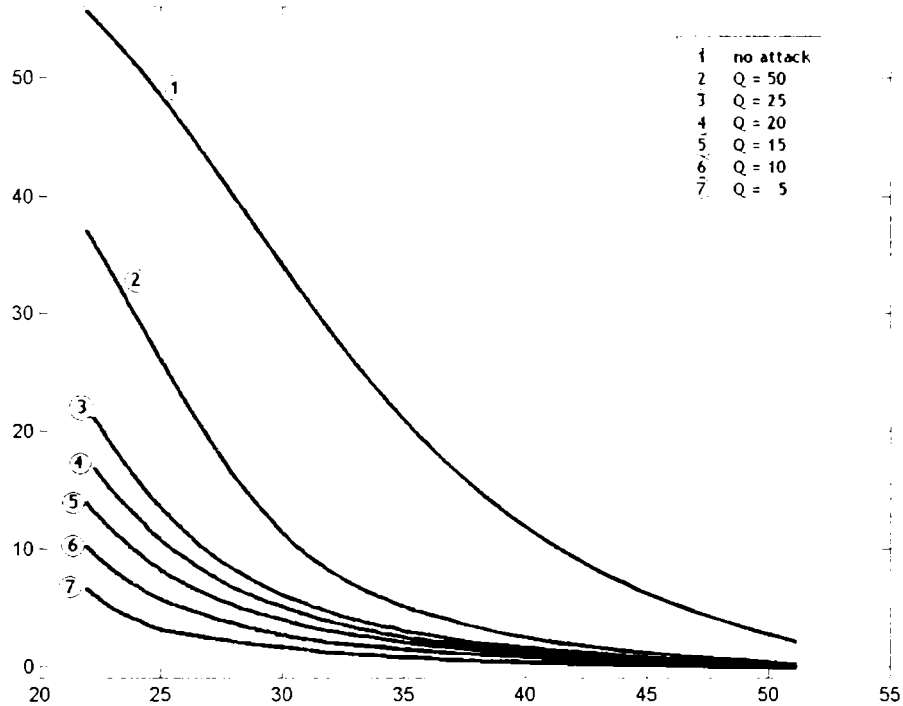


Fig. 5.11: Raportul ρ/T ca funcţie de valorile PSNR dintre imaginile marcate şi originală, pentru compresie JPEG, la diverşi factori de calitate. P_f este 10^{-8} [NIB06a].

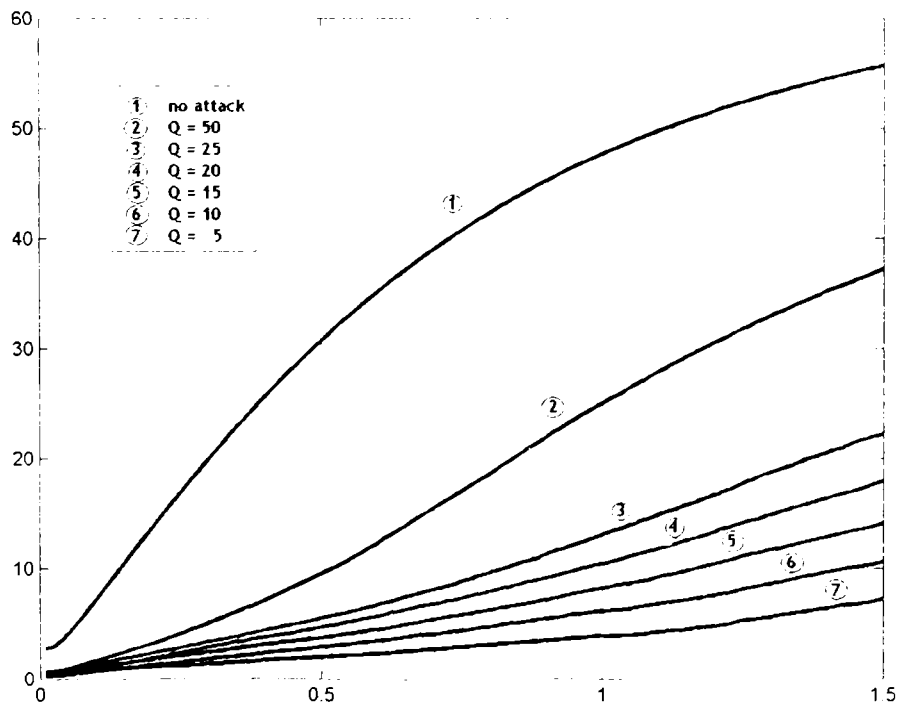


Fig. 5.12: Raportul ρ/T ca funcţie de puterea de marcare, pentru compresie JPEG, la diverşi factori de calitate. P_f este 10^{-8}, [NIB06a].

Figura 5.13 prezintă detecţia unui marcaj adevărat pentru cazul compresiei JPEG cu diverse valori Q, pentru marcarea cu α=1.5; pragul este mult mai mic decât răspunsul detectorului.

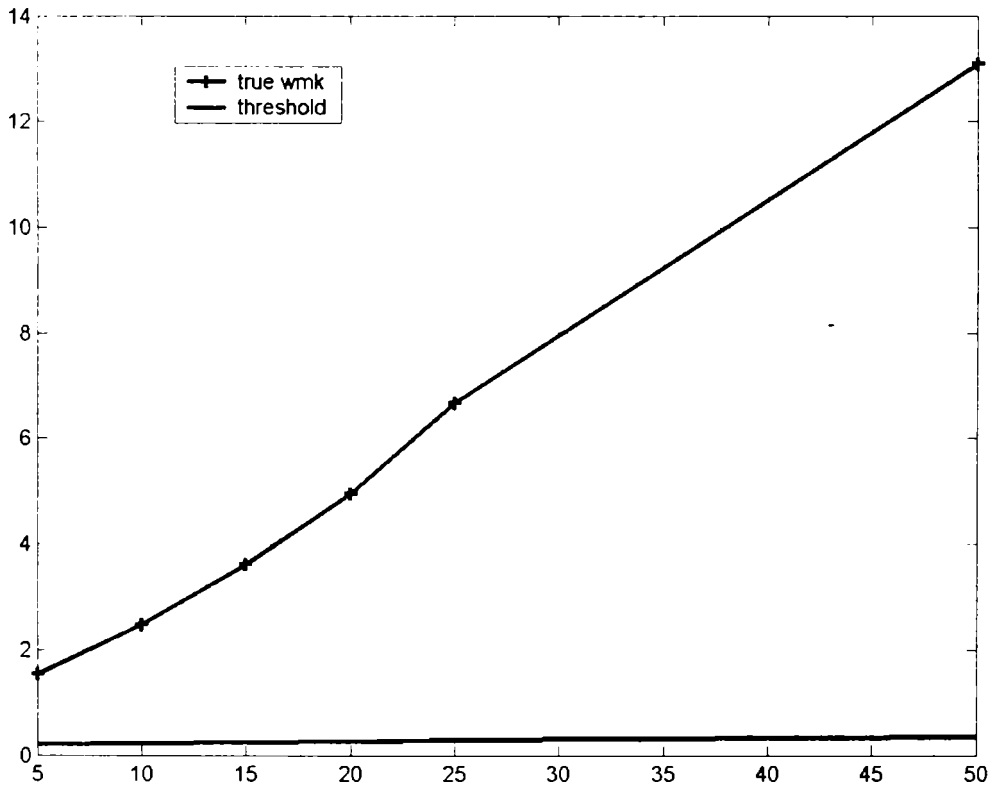


Fig. 5.13: Răspunsul detectorului ρ, pragul de detecţie T, ca funcţie de Q, factor de calitate în compresia JPEG. Marcajul este detectat cu succes. P_f este 10^{-8}, [NIB06a].

În fine, selectivitatea detectorului este ilustrată în Figura 5.14, când sunt testate 1000 de marcaje diferite (999 false şi unul adevărat). Al doilea răspuns al detectorului ca mărime (corespunzând unui fals) este arătat împreună cu valoarea de prag, pentru fiecare imagine atacată. Se observă că sunt rejectate falsurile pozitive.

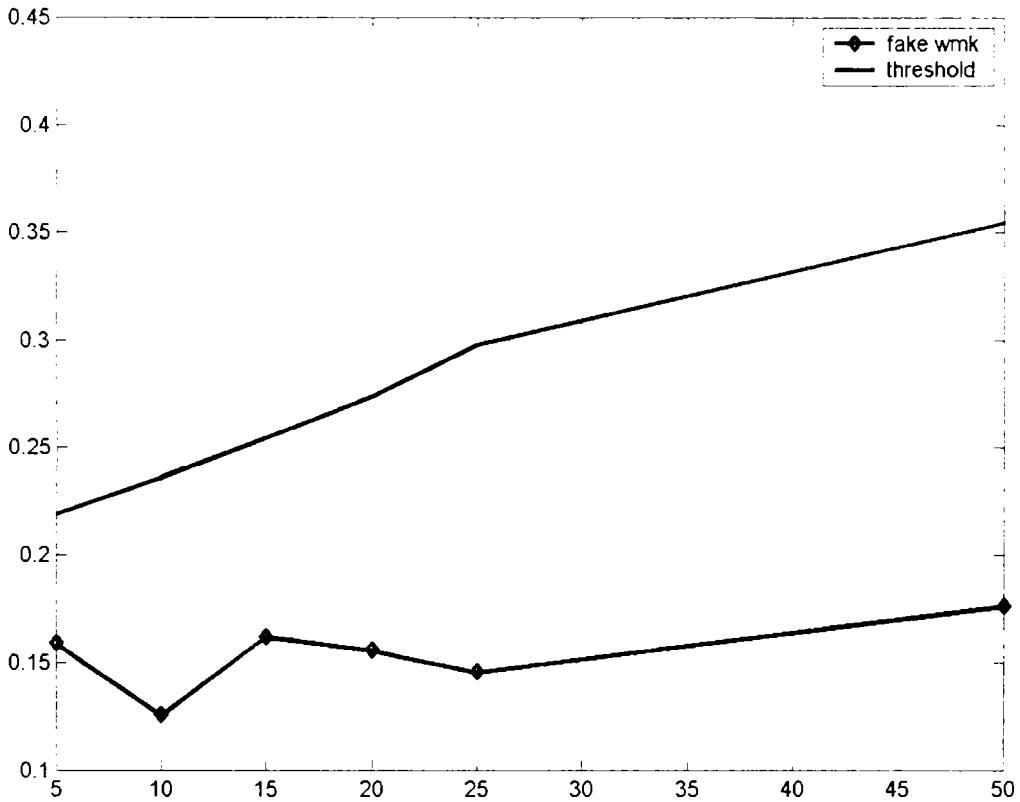


Fig. 5.14: Al doilea răspuns al detectorului ca mărime, ρ_2, corespunzând unui marcaj fals, şi pragul T. Pragul este deasupra lui ρ_2, [NIB06a].

În Tabelul 5.1 se prezintă o comparaţie între metoda propusă de mine şi prezentată în [NIB06a] şi cea din [BBP01]. De această dată, algoritmul a fost testat pe imaginea Lena, pentru σ=1.5 şi un factor de calitate Q = 5, corespunzând unei rate de compresie JPEG de 46. Valoarea lui P_f este 10^{-8} şi se testează răspunsul detectorului la 1000 de marcaje decorelate. Tabelul arată răspunsul detectorului pentru marcajul original, ρ, pragul de detecţie T, precum şi al doilea răspuns ca mărime, ρ_2. Răspunsul detectorului este mai mare decât în cazul metodei din [BBP01].

Noul tip de mască perceptuală reuşeşte să ascundă datele mai bine, datorită estimării mai precise a texturii, cu ajutorul deviaţiei standard locale a imaginii comprimate în domeniul wavelet.

Tab. 5.1. Comparaţie între metoda prezentată în [BBP01] şi cea propusă [NIB06a], compresie JPEG, rata de compresie CR=46.

Răspuns vs. Metodă	Noua metodă [NIB06b]	Metoda lui Barni ş.a. [BBP01]
ρ	0.3199	0.038
T	0.0844	0.036
ρ_2	0.0516	0.01

În continuare se prezintă o extensie a acestei metode [NIB06b], prin care marcajul se poate ascunde imperceptibil şi în subbenzile de frecvenţă mai joasă. Acest lucru aduce un nivel crescut de robusteţe.

5.6 Înserare în subbenzile de frecvenţă mai joasă

Din moment ce imaginea de aproximare a ultimului nivel de rezoluţie (4 în cazul prezentat în paragrafele anterioare), conţine prea puţină informaţie, imaginea de luminanţă poate fi estimată mai bine pornind de la o imagine de aproximare wavelet de rezoluţie mai bună.

De aceea, în continuare masca de luminanţă se va calcula diferenţiat, pe subimaginea de aproximare de la nivelul *l*, unde urmează să fie înserat marcajul [NIB06b].

Prin urmare, relaţia (5.6) este înlocuită cu:

$$L(l,i,j)=\frac{1}{256}I_l^3(i,j) \tag{5.12}$$

unde I_l^3 reprezintă imaginea de aproximare de la nivelul *l*. Deoarece masca de luminanţă este mai dependentă de nivelul de rezoluţie, funcţia de sensibilitate la zgomot devine:

$$\Theta(l,\theta)=\begin{cases}\sqrt{2}, & \text{dacă } \theta=1\\ 1, & \text{altfel}\end{cases} \tag{5.13}$$

Imaginea originală, precum şi cele două măşti obţinute folosind metodele din [NIB06b] şi din [BBP01] sunt prezentate în Figura 5.15. Îmbunătăţirea este vizibilă în jurul muchiilor şi contururilor.

Fig. 5.15(a): Imaginea originală Lena

Fig. 5.15(b): Masca obţinută folosind metoda propusă de Barni ş.a. în [BBP01]. Imaginea este complementară imaginii reale, imagine reprodusă din [NIB06b].

Fig. 5.15(c): Masca de nivel 0, obţinută folosind metoda din [NIB06b]. Imaginea este complementară imaginii reale.

Fig. 5. 16(a): Imagine marcată pentru metoda prezentată [NIB06b], cu α = 1.5, nivelul 0 (PSNR = 38 dB).

Fig. 5. 16(b): Imagine marcată pentru metoda prezentată în [NIB06b], cu α = 1.5, nivelul 1 (PSNR = 43 dB).

Fig. 5.16(c): Imagine marcată folosind masca din [BBP01], cu α = 1.5, nivelul 0 (PSNR = 20 dB).

În cele ce urmează se prezintă testele făcute asupra metodei de înserare derivată pe baza relaţiilor (5.12) şi (5.13), pentru două cazuri diferite [NIB06a]:

1) marcajul este înserat numai în nivelul 0, respectiv,

2) marcajul este înserat exclusiv în nivelul 1.

Pentru evaluarea performanţei, se consideră atacul prin compresie JPEG. Imaginea Lena este marcată în toate subbenzile de detaliu de la nivelul 0 şi respectiv în toate subbenzile de detaliu de la nivelul 1, cu diferite intensităţi de marcare, începând de la 1.5 la 5. Marcajul binar este înserat aşa cum s-a descris mai sus. Pentru α=1.5, imaginile marcate, la nivelul 0 respectiv 1, precum şi imaginea marcată folosind masca din [BBP01], sunt prezentate în Figura 5.16.

În mod evident, calitatea imaginilor marcate este păstrată folosind această mască. Valorile PSNR sunt 38 dB (nivelul 0), respectiv 43 dB (nivelul 1), comparativ cu cea din [BBP01], cu un PSNR de 20 dB.

Valorile PSNR sunt date în Figura 5.17 ca funcţie de intensitatea de marcare α. Marcajul este încă imperceptibil, chiar şi pentru valori mari ale lui α.

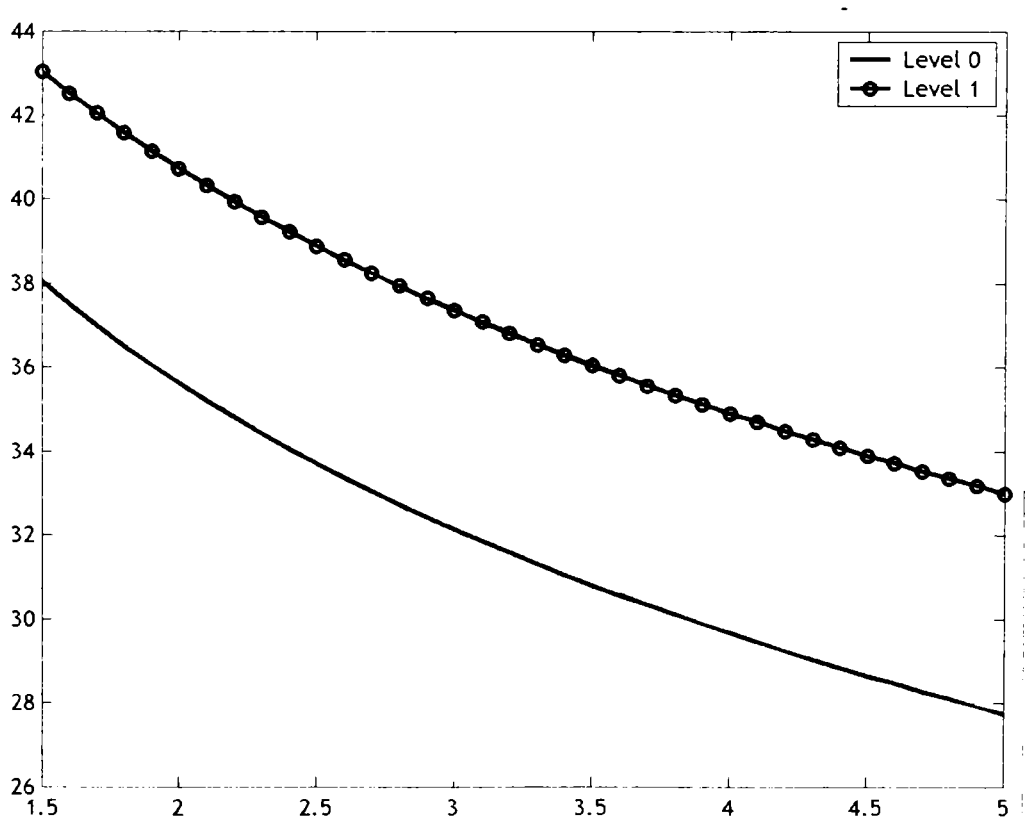


Fig. 5.17: Valorile PSNR ca funcţie de α. Inserarea marcajului a fost făcută în nivelul 0, respectiv 1 [NIB06b].

Pentru verificarea algoritmului folosind această mască, se prezintă în Figurile 5.18-19 rezultatele pentru compresia JPEG. Fiecare imagine marcată este comprimată folosind standardul JPEG, pentru şase factori de calitate diferiţi, $Q \in \{5,$

10, 15, 20, 25, 50}. Pentru fiecare imagine atacată, se calculează corelaţia ρ şi pragul T. În toate experimentele, probabilitatea de fals pozitiv este 10^{-8}. Eficienţa noului sistem de marcare poate fi măsurată, la fel ca şi înainte, folosind raportul ρ/T. Dacă raportul este mai mare decât 1, atunci marcajul este detectat.

Figurile 5.18-5.19 prezintă dependenţa acestui raport funcţie de α. Se observă că marcajul este detectat cu succes pentru un interval mare de factori de compresie. Pentru valori PSNR mai mari decât 30 dB, marcajul este invizibil. Pentru factori de calitate $Q \geq 10$, distorsiunea introdusă de compresia JPEG este acceptabilă. Pentru toate valorile lui α, marcajul este detectat pentru toţi factorii de calitate semnificativi ($Q \geq 10$).

Dacă puterea de marcare creşte, valoarea PSNR a imaginii marcate scade, iar raportul ρ/T creşte. Pentru Q = 10 (sau o rată de compresie CR = 32), marcajul este încă detectabil chiar pentru valori mici ale lui α.

Figura 5.20 prezintă detecţia unui marcaj adevărat de la nivelul 0, pentru diferiţi factori de calitate, în cazul α=1.5; pragul este sub răspunsul detectorului.

Selectivitatea detectorului este de asemenea ilustrată, în cazul testării a 999 de marcaje false: al doilea răspuns ca mărime este arătat, pentru fiecare factor de calitate. Se observă şi de această dată că deciziile de fals pozitiv sunt rejectate.

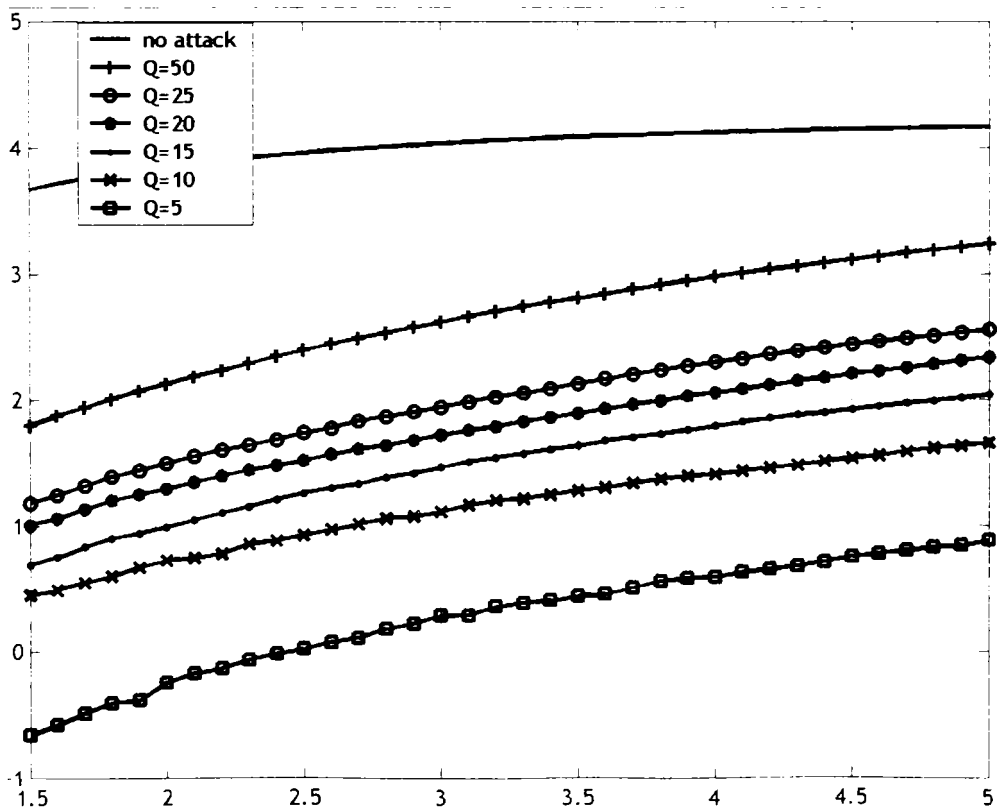


Fig. 5.18: Log(ρ/T) ca funcţie de α, pentru compresie JPEG (marcaj înserat la nivelul 0) [NIB06b].

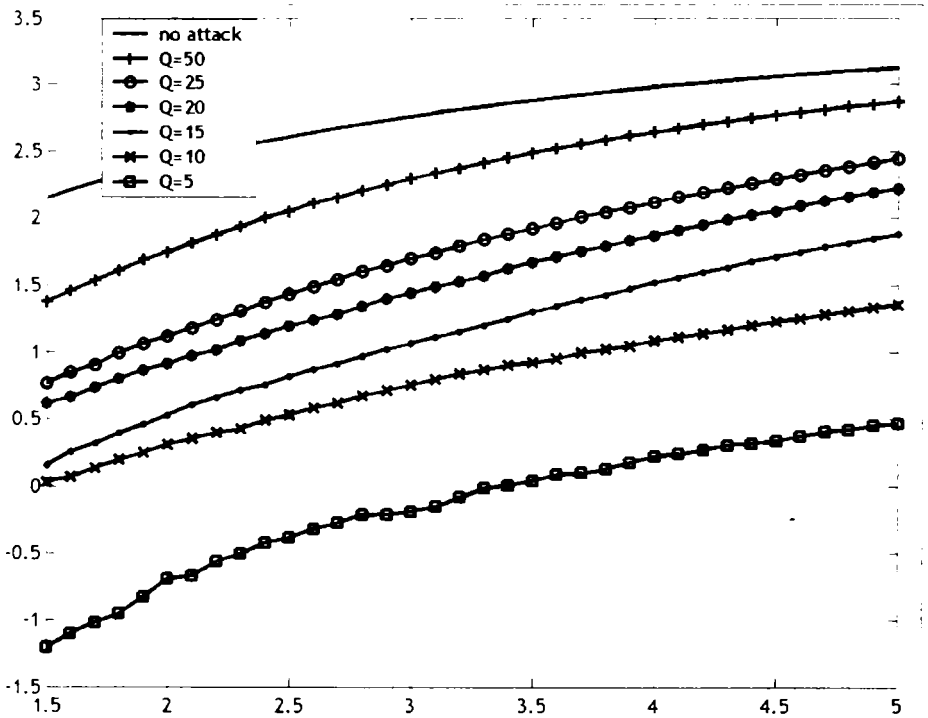


Fig. 5.19: Log(ρ/T) ca funcţie de α, pentru compresie JPEG (marcaj înserat la nivelul 1) [NIB06b].

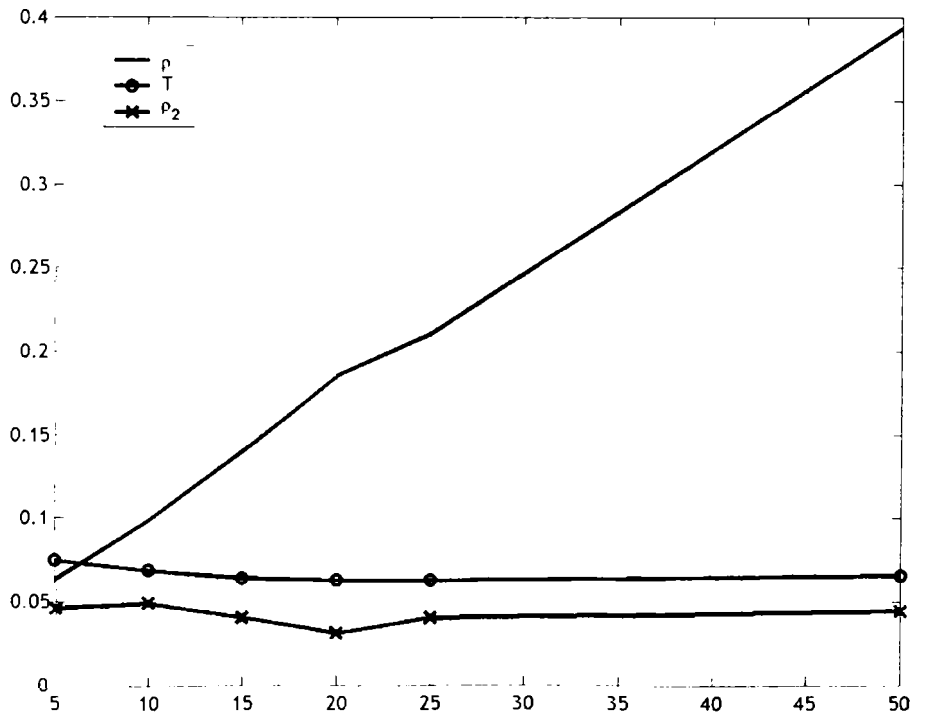


Fig. 5.20: Răspunsul detectorului ρ, pragul de detecţie T, al doilea răspuns ca mărime ρ_2, corespunzând unui marcaj fals, ca funcţie de diferiţi factori de calitate JPEG. Marcajul este detectat. Au fost testate 999 de marcaje false [NIB06a].

În Tabelul 5.2 se dă o comparaţie între această mască [NIB06a] şi cea prezentată în [BBP01], pentru compresie JPEG, cu Q = 10, echivalent unei rate de compresie de 32 pentru imaginea Lena. Se dau răspunsul detectorului, pentru marcajul original, ρ, pragul de decizie, T, precum şi al doilea răspuns ca mărime al detectorului, corespunzând unui marcaj fals, ρ_2, atunci când marcajul a fost inserat în nivelul 0. Răspunsul detectorului este mai mare decât pentru metoda din [BBP01].

Tab. 5.2: Comparaţie între metoda prezentată în [NIB06a] şi cea propusă de Barni ş.a. [BBP01], pentru compresie JPEG, rata de compresie CR=32

Răspuns vs. Metodă	Noua metodă [NIB06a]	Metoda lui Barni ş.a. [BBP01]
ρ	0.0750	0.062
T	0.0636	0.036
ρ_2	0.0461	0.011

5.7 Evaluarea robusteţii marcajelor perceptuale

Într-un sistem de marcare, evaluarea robusteţii ar trebui făcută numai atunci când criteriile de invizibilitate sunt satisfăcute. În acest scop, propunem măsurarea impactului perceptual al marcajului asupra imaginii folosind bine cunoscutul criteriu al raportului maxim (de vârf) semnal-pe-zgomot, PSNR şi, în plus, un model spaţial care indică pixelii modificaţi vizibil faţă de imaginea originală. În aceasta secţiune, studiem sistemul propus de Barni şi alţii [BBP01] precum şi metoda propusă în [NIB06a] ambele bazate pe mascare pixel cu pixel în domeniul wavelet. Limităm intensitatea de marcaj astfel încât PSNR să fie în jur de 35 dB, iar media pixelilor afectaţi vizibil mai mică decât 25%. Sunt testate mai multe imagini cu mai multe tipuri de atacuri (compresie JPEG, filtrare mediană, redimensionare, decupare şi corecţie de gamma) pentru a evidenţia efectele acestor atacuri asupra rezultatelor detectorului. Rezultatele arată limitările acestori tehnici atunci când se impune constrângerea de invizibilitate.

Marcajele perceptuale sunt folosite pentru a satisface cele două cerinţe de transparenţă precum şi invizibilitate în acelaşi timp. Studiem două tehnici de marcare perceptuală care inserează marcajul în domeniul wavelet. In [BBP01] marcajul este mascat conform caracteristicilor sistemului vizual uman, (HVS), ţinând cont de textura şi luminanţa tuturor subbenzilor de detaliu ale transformatei wavelet. In [NIB06a] o altă mască perceptuală este folosită, bazată pe deviaţia standard locală a imginii (a se vedea paragraful anterior).

Aceste tehnici sunt perceptuale, dar nu trebuie testată robusteţea unei metode decât dacă sunt satisfăcute unele criterii de invizibilitate. Aşa cum a sugerat Fridrich şi alţii în [FG99], un model spaţial care indică numărul şi localizarea pixelilor afectaţi de marcare [Gir89] poate fi folosit pentru a cuantifica invizibilitatea procesului de marcare. Acest model a fost folosit şi pentru "corectarea" marcajului în domeniul spaţial în [SZT96].

Mai mult, un estimat al robusteţii [FG99] este folosit pentru a demonstra validitatea algoritmilor atunci când criteriile de invizibilitate sunt satisfăcute.

Cele două tehnici de marcare au fost descrise anterior. Ca şi până acum, la detecţie vom considera raportul între corelaţia ρ din relaţia (5.7) şi pragul dependent de imagine, T_ρ, astfel încât detectorul este o funcţie neliniară cu prag

fix. În cele ce urmează vom nota metoda din [BBP01] cu "metoda 1" iar cea descrisă în [NIB06a] cu "metoda 2".

Rezultate obţinute în urma simulării. Mai multe imagini din baza de date din [USC] au fost marcate la nivelul l=0 cu diferite intensităţi de marcare α. Un marcaj binar este inserat în toate subimaginile de detaliu, ale primului nivel de rezoluţie, l=0, aşa cum s-a văzut în paragraful 5.4.

Pentru α=0.2 (metoda 1) şi α=0.4 (metoda 2), imaginile sunt neafectate de procesul de marcare. Această afirmaţie se bazează atât pe valorile PSNR obţinute, cât şi pe modelul spaţial de mascare care indică numărul şi localizarea pixelilor afectaţi din imagine [Gir89, Fri99b]. Imaginea Lena originală şi marcată cu cele două metode este prezentată în fig. 5.23, împreună cu pixelii afectaţi din imagine, conform modelului lui Girod.

Media intensităţii de marcare $\bar{\alpha}$, valorile PSNR precum şi procentajul de pixeli afectaţi sunt prezentaţi în tabelul 5.3. Aceste valori sunt prezentate şi în Figura 5.21 (a)-(c).

Tab. 5.3: Comparaţie a invizibilităţii între imaginile marcate cu cei doi algoritmi, tabel din [Naf07a].

Imagine	*Intensitate medie*		*PSNR (dB)*		*Pixeli modificaţi (%)*	
	1	***2***	***1***	***2***	***1***	***2***
IM1	2.95	5.19	33.33	34.33	40.39	22.95
IM2	3.00	3.98	32.83	35.76	36.87	14.92
IM3	1.97	3.76	35.90	36.19	8.71	6.75
IM4	2.36	3.21	35.28	38.38	25.30	2.59
IM5	3.84	5.91	30.97	32.90	58.20	31.36
IM6	1.99	3.06	36.39	38.40	11.84	4.55
IM7	2.48	4.35	34.38	34.86	18.25	13.14
IM8	3.23	3.56	32.60	37.12	48.29	7.58
IM9	2.55	3.14	34.40	37.89	28.79	4.96
IM10	2.34	3.79	35.05	36.72	18.48	6.73
IM11	2.48	3.47	34.98	37.78	26.65	4.66
IM12	2.13	3.60	35.94	37.16	13.80	3.82
IM13	2.80	5.96	33.61	33.08	16.04	19.90
IM14	3.21	4.51	32.66	35.52	53.26	10.69
IM15	1.79	2.86	37.61	39.56	4.25	1.17
IM16	0.96	2.54	41.75	39.82	0.21	2.21
IM17	1.72	3.25	38.03	38.62	2.80	0.99
IM18	1.76	2.95	37.90	39.42	2.37	0.38
IM19	2.60	3.54	34.61	37.79	38.90	1.76
IM20	2.57	3.19	34.74	38.71	42.05	0.64
IM21	2.08	3.35	36.56	38.49	6.87	0.40
IM22	1.24	2.73	40.40	40.05	1.09	0.43
IM23	1.97	3.58	36.91	37.84	9.76	1.55
IM24	1.76	2.96	37.92	39.52	1.31	0.13

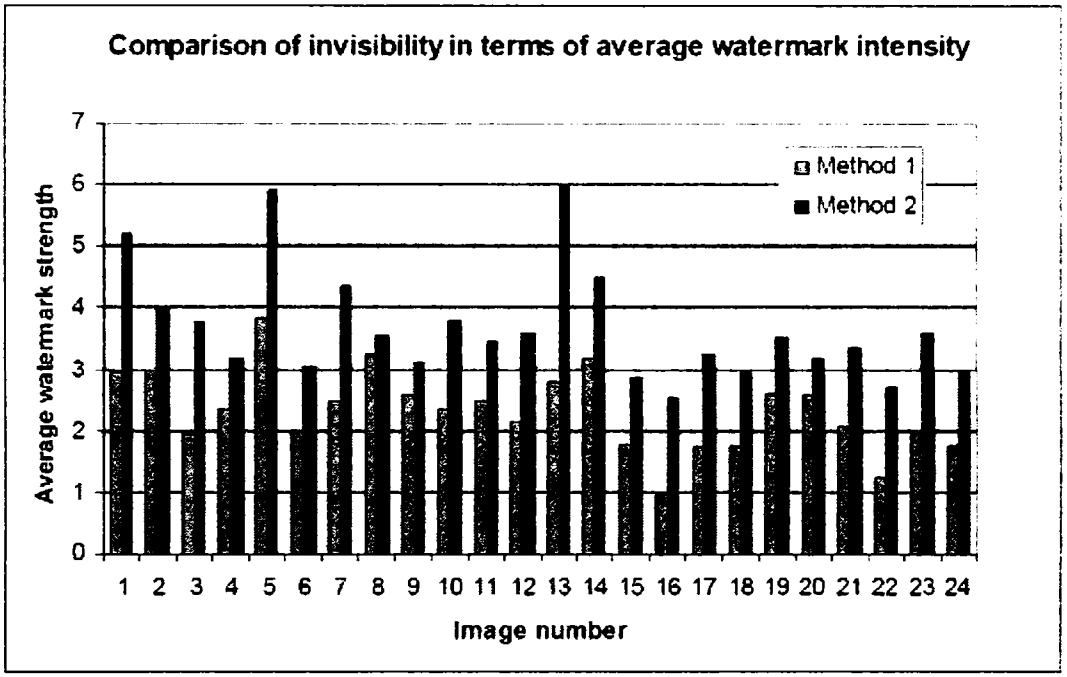


Fig. 5.21(a): Comparaţie a invizibilităţii între imaginile marcate cu cei doi algoritmi funcţie de intensitatea de marcare medie

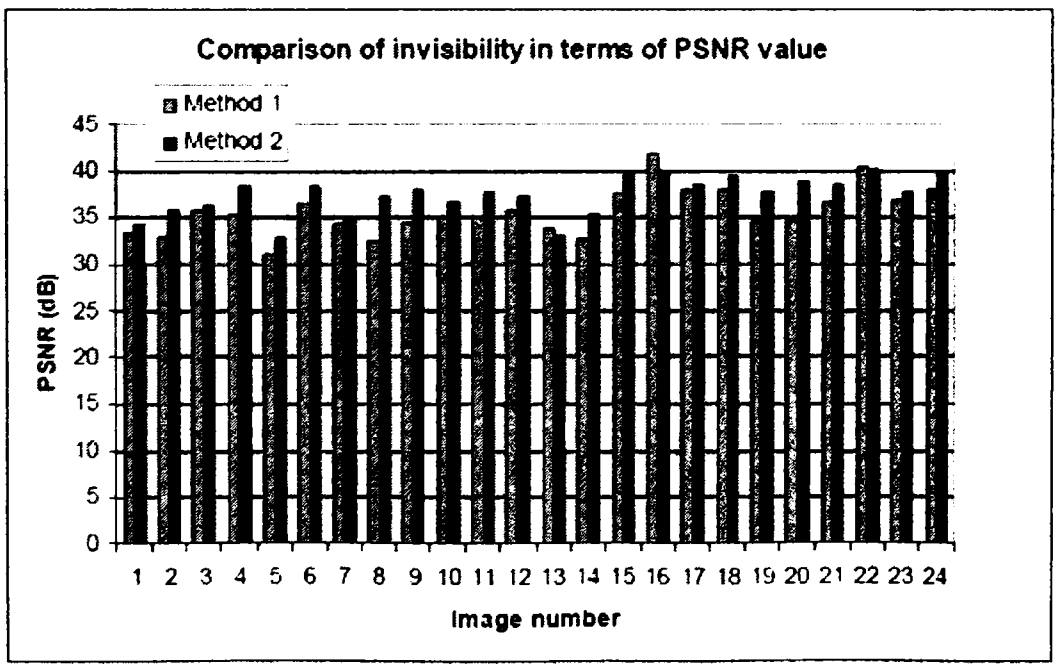


Fig. 5.21(b): Comparaţie a invizibilităţii între imaginile marcate cu cei doi algoritmi funcţie de valoarea PSNR dintre imaginea marcată şi originală

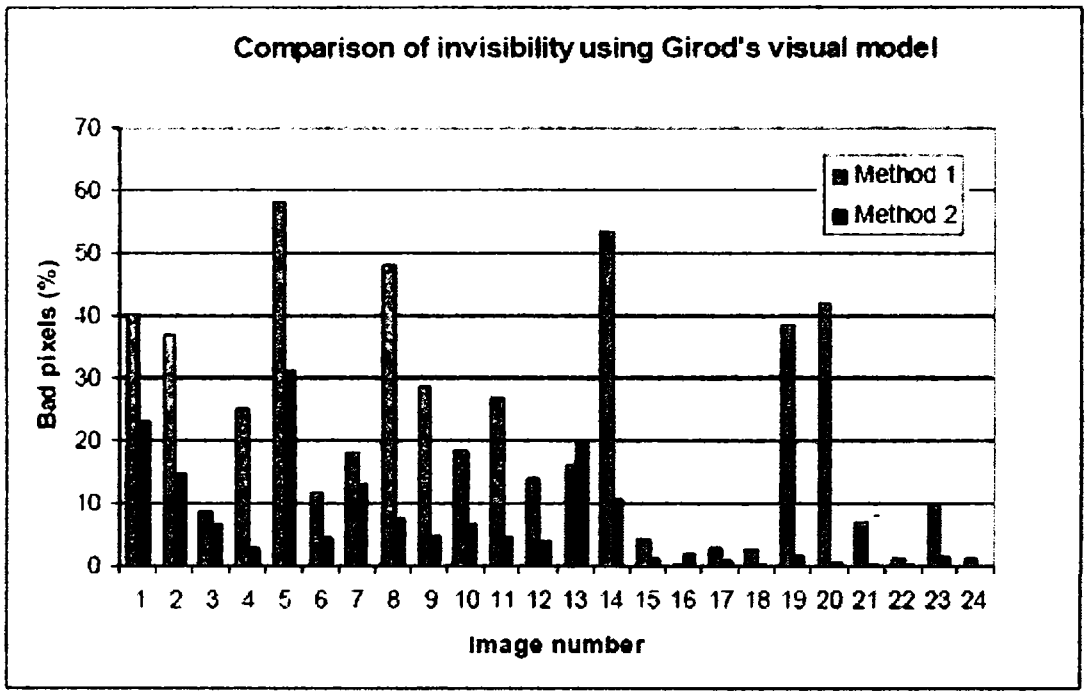


Fig. 5.21(c): Comparaţie a invizibilităţii între imaginile marcate cu cei doi algoritmi funcţie de procentajul de pixeli afectaţi folosind modelul lui Girod

Tab. 5.4: Comparaţie a robusteţii [Naf07a].

Imagine	*Raport ρ/T*		*Robusteţe*	
	1	*2*	*1*	*2*
IM1	33.22	22.78	0.80	0.72
IM2	37.25	20.00	0.91	0.65
IM3	39.40	31.33	0.59	0.57
IM4	59.00	29.18	0.79	0.56
IM5	37.70	23.95	0.81	0.65
IM6	66.33	38.25	0.66	0.53
IM7	30.75	21.95	0.68	0.65
IM8	44.14	21.62	0.63	0.37
IM9	51.20	28.63	0.76	0.51
IM10	46.60	29.23	0.71	0.59
IM11	62.00	34.70	0.82	0.60
IM12	35.16	23.33	0.40	0.34
IM13	40.28	35.11	0.69	0.73
IM14	39.50	23.73	0.86	0.62
IM15	59.66	31.77	0.67	0.54
IM16	47.50	36.28	0.35	0.43
IM17	57.33	36.00	0.61	0.57
IM18	58.00	32.11	0.56	0.47
IM19	52.20	29.66	0.90	0.62
IM20	51.60	26.33	0.88	0.56
IM21	51.75	30.54	0.75	0.60
IM22	41.66	34.00	0.48	0.50
IM23	49.25	32.45	0.69	0.62
IM24	58.66	36.87	0.65	0.54

Tabelul 5.4 prezintă raportul dintre corelaţie şi prag dar şi estimatul robusteţii aşa cum este definit în [FG99], *raportul dintre puterea marcajului şi puterea modificării acceptabile, folosind modelul lui Girod:*

$$\frac{\sum_{i,j} w^2(i,j)}{\sum_{i,j} m^2(i,j)} \tag{5.14}$$

unde $w(i, j)$ este marcajul, estimat ca diferenţa dintre doi pixeli ai imaginii, iar $m(i,j)$ este modificarea maximă acceptabilă pentru imaginea originală.

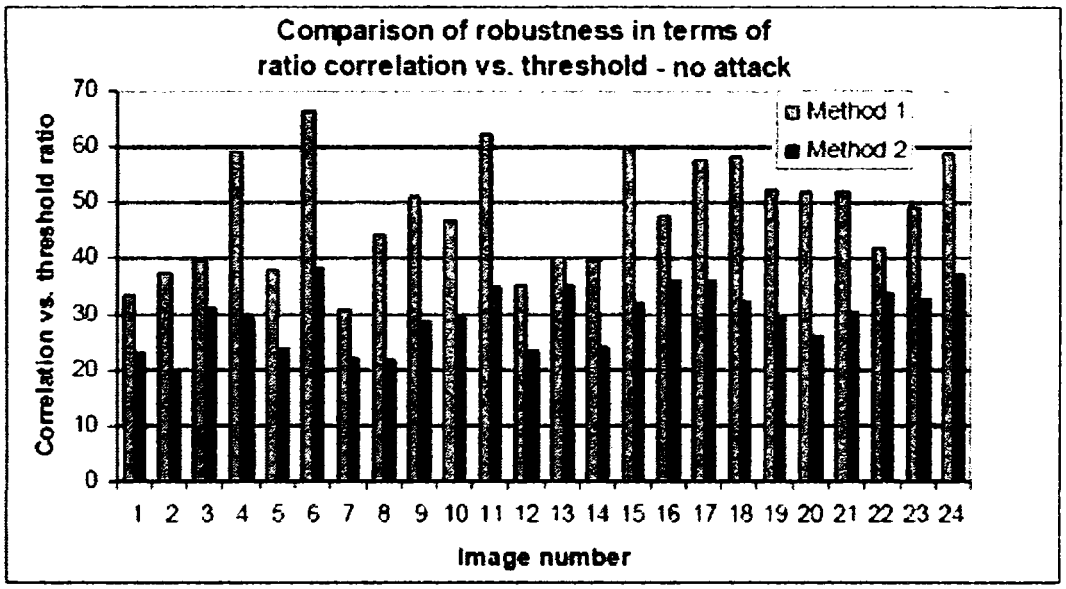


Fig. 5.22(a): Comparaţia robusteţii funcţie de raportul corelaţie per prag

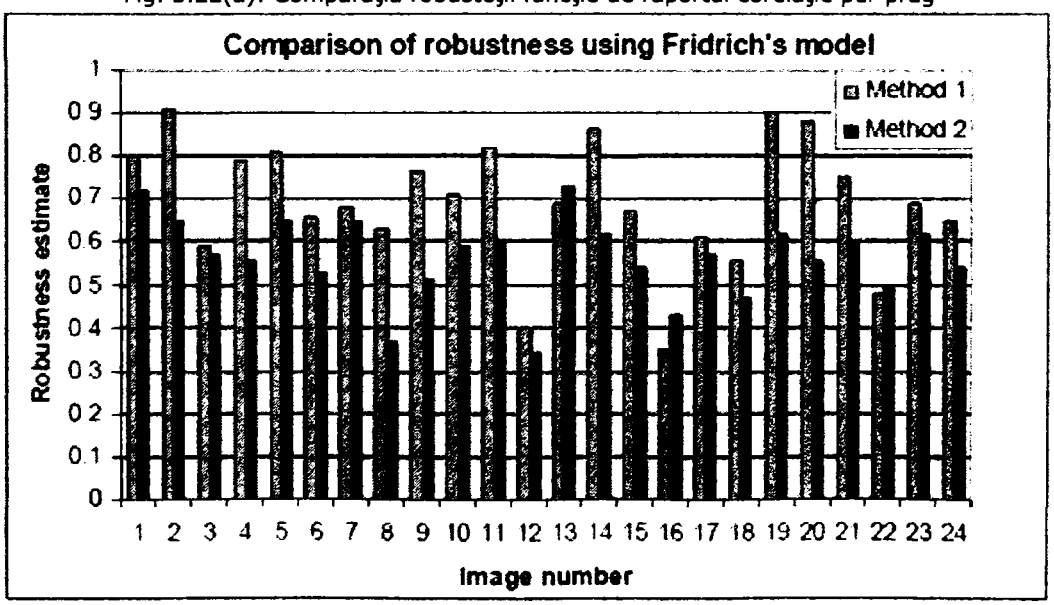


Fig. 5.22(b): Comparaţia robusteţii folosing modelul lui Fridrich

Fig. 5.23: Imaginea originală Lena (sus), imaginile marcate cu α=0.2 (metoda 1) [BBP01], PSNR=36.39 dB, 11.84% pixeli afectaţi, respectiv cu α=0.4 (metoda 2), [Naf07a], PSNR=35.92dB, 15.71% pixeli afectaţi. Pixelii afectaţi din imagini, conform modelului lui Girod sunt reprezentaţi cu negru [Naf07a].

Pentru a verifica validitatea algoritmilor prezentaţi anterior pentru aceste intensităţi de marcare, de exemplu α=0.2 (metoda 1) şi α=0.4 (metoda 2), am efectuat teste pentru compresie JPEG, filtrare mediană, decupare, redimensionare şi corecţie de gamma. Pentru fiecare imagine atacată, corelaţia ρ şi pragul T_ρ sunt calculate. Probabilitatea de fals pozitiv este fixată la valoarea 10^{-8}.

Tabelele 5.5, 5.6, 5.7, 5.8 prezintă raportul corelaţie/prag pentru fiecare imagine şi atac. Pentru o mai bună vizualizare a rezultatelor, prezentăm şi grafice cu valorile corelaţiilor în funcţie de imagini pentru fiecare atac.

Rezistenţa la compresia JPEG: marcajul este încă detectabil chiar la factori de calitate 10, în ambele cazuri. Metoda 2 are evident rezultate mai bune în fiecare caz; detectează marcajul pentru Q=5 pentru jumătate din imagini. Metoda 1 nu reuşeste să detecteze marcajul în cazul compresiei cu Q=5.

Rezistenţa la filtrarea mediană: marcajul de la metoda 2 a supravieţuit în aproape toate imaginile pentru filtrare mediană cu lungimea ferestrei filtrului până la 3. Pentru filtru cu dimensiune 5, marcajul inserat cu metoda 2 nu este detectabil. Metoda 1 nu a supravieţuit în nici unul dintre cazuri.

Rezistenţa la redimensionare: marcajul este detectat cu succes în ambele cazuri, atât pentru metoda 1 cât şi pentru metoda 2.

Rezistenţa la corecţia de gamma: aşa cum era de aşteptat pentru corelaţie normalizată, ambele metode sunt practic insensibile la ajustarea contrastului [Cox05].

Rezistenţa la decupare: marcajul inserat cu metoda 1 este detectat în imaginea decupată de 32x32 în cele mai multe cazuri, în timp ce marcajul inserat cu metoda 2 este detectat numai la unele imagini. Metoda 2 detectează marcajul până la imaginea decupată de mărime 64x64, inclusiv.

Performanţele metodei 1, uşor mai bune decât ale metodei 2 în cazul corecţiei gamma şi decupării, pot fi explicate prin faptul că *puterea marcajului* este mai mare în cazul metodei 1 decât în cazul metodei 2, aşa cum se vede din valorile estimate ale robusteţii din tabelul 5.4.

Concluzii. Am argumentat că nu ar trebui testată robusteţea unei metode, atâta timp cât criteriul (criteriile) de invizibilitate nu sunt satisfăcute. Ca şi constrângere de invizibilitate, am folosit raportul maxim semnal-pe-zgomot, precum şi modelul de mascare spaţială din [Gir89]. Au fost testate două măşti perceptuale, pe un număr mare de imagini. Intensitatea de marcare a fost fixată astfel încât procentajul de pixeli degradaţi din imaginea marcată să nu depăşească în medie 25%, iar valorile PSNR au fost în jur de 35 dB. Aceasta a indicat că imaginile nu sunt vizibil afectate de procesul de marcare.

Cele două seturi de imagini marcate au fost supuse la diferite tipuri de atacuri (compresie JPEG, filtrare mediană, redimensionare, decupare şi corecţie de gamă).

Rezultatele simulării au arătat că la impunerea constrângerii de invizibilitate bazată pe modelul lui Girod [Gir89], cele două metode au fost comparabile şi au detectat cu succes marcajul numai în cazul atacurilor uşoare. Aceste rezultate au fost prezentate în [Naf07a].

Tab. 5.5: Raport corelaţie/prag, comparaţia robusteţii în cazul compresiei JPEG pentru diverşi factori de calitate. Intensitatea maximă de marcare este dată de constrângerea de invizibilitate [Naf07a].

Imagine	*JPEG Q=20*		*JPEG Q=15*		*JPEG Q=10*		*JPEG Q=5*	
	1	*2*	*1*	*2*	*1*	*2*	*1*	*2*
IM1	4.79	6.09	3.76	5.04	2.58	3.90	0.17	2.41
IM2	2.92	3.45	2.34	3.02	1.71	2.37	0.32	1.60
IM3	2.55	3.74	1.88	2.99	1.27	2.01	0.27	1.23
IM4	3.18	3.84	2.28	3.01	1.45	2.07	0.24	1.06
IM5	4.52	5.36	3.66	4.36	2.49	3.16	0.29	1.83
IM6	2.38	3.46	1.52	2.70	0.97	2.03	0.56	0.91
IM7	2.37	4.15	1.82	3.28	1.13	2.08	0.12	1.31
IM8	4.67	4.12	3.69	3.39	2.66	2.40	0.12	1.38
IM9	2.29	2.45	1.72	1.91	1.20	1.29	0.13	0.50
IM10	2.88	4.04	2.40	3.40	1.74	2.75	0.35	1.42
IM11	2.89	3.60	2.06	2.66	1.31	1.64	0.16	0.83
IM12	2.14	2.83	1.61	2.05	1.16	1.41	0.35	0.73
IM13	4.55	7.22	3.74	6.00	2.60	4.19	0.14	2.52
IM14	5.11	5.19	3.88	4.32	2.51	2.97	0.33	1.55
IM15	3.18	3.82	2.40	2.86	1.54	1.82	0.24	0.75
IM16	1.76	2.61	1.29	2.01	0.96	1.26	0.19	0.50
IM17	2.82	4.43	2.14	3.09	1.22	1.80	0.23	0.17
IM18	2.49	3.59	1.72	2.57	0.94	1.28	0.27	0.30
IM19	4.81	5.49	3.60	4.11	2.29	2.77	0.39	1.36
IM20	4.79	4.42	3.55	3.59	2.00	2.34	0.20	0.62
IM21	3.74	5.05	2.80	4.00	1.58	2.54	0.22	0.82
IM22	2.40	3.49	1.79	2.19	1.28	1.29	0.43	0.58
IM23	3.39	4.97	2.60	3.42	1.73	2.22	0.18	0.90
IM24	3.21	4.37	2.15	3.30	1.29	1.63	0.13	0.47

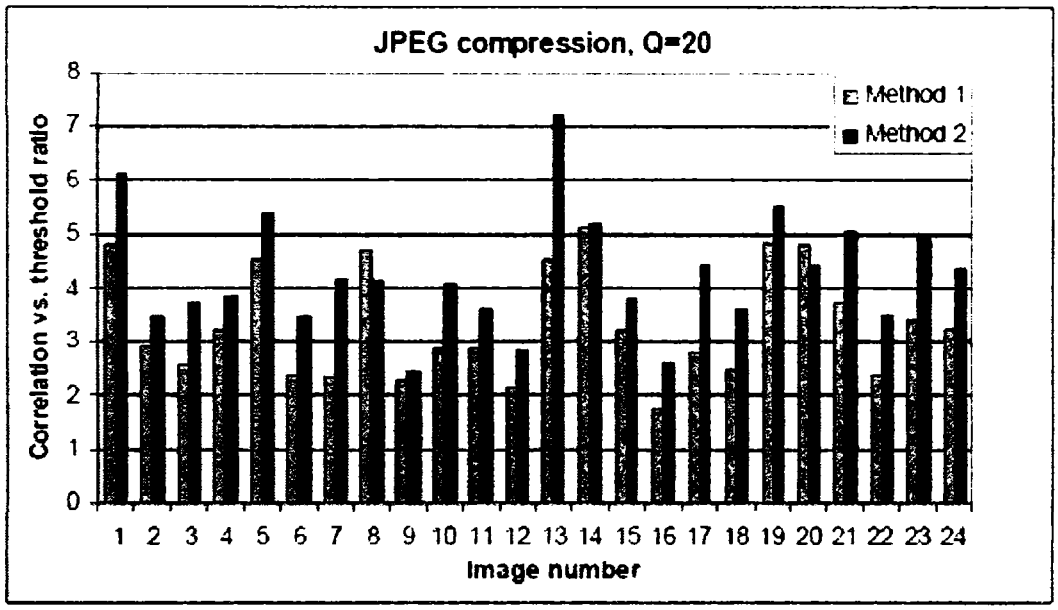


Fig. 5.24(a): Raport corelaţie/prag, comparaţia robusteţii în cazul compresiei JPEG, factor de calitate 20

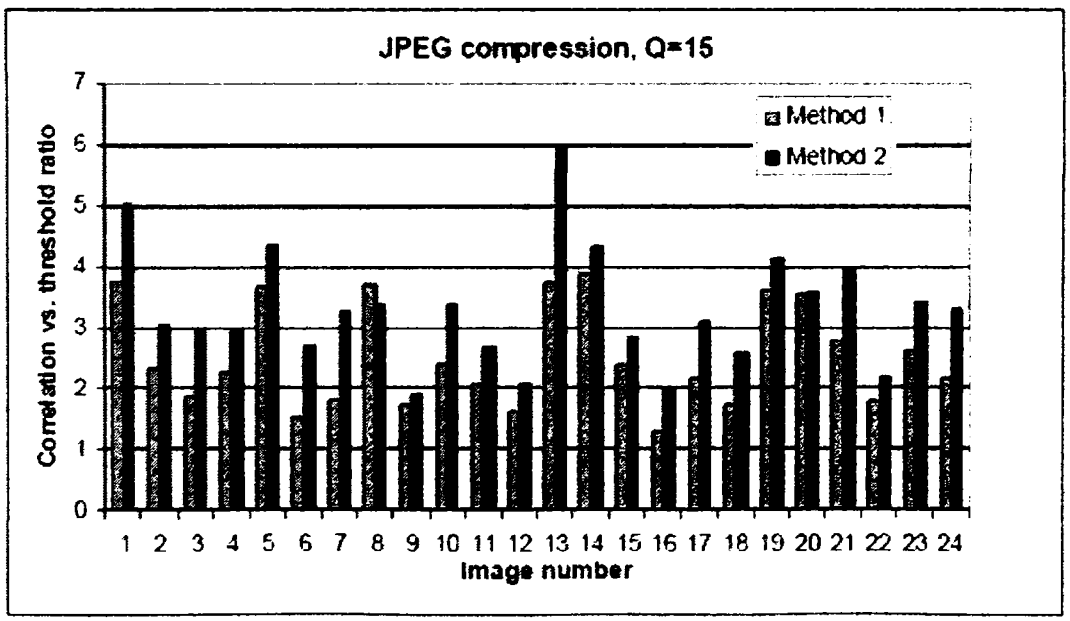


Fig. 5.24(b): Raport corelaţie/prag, comparaţia robusteţii în cazul compresiei JPEG, factor de calitate 15

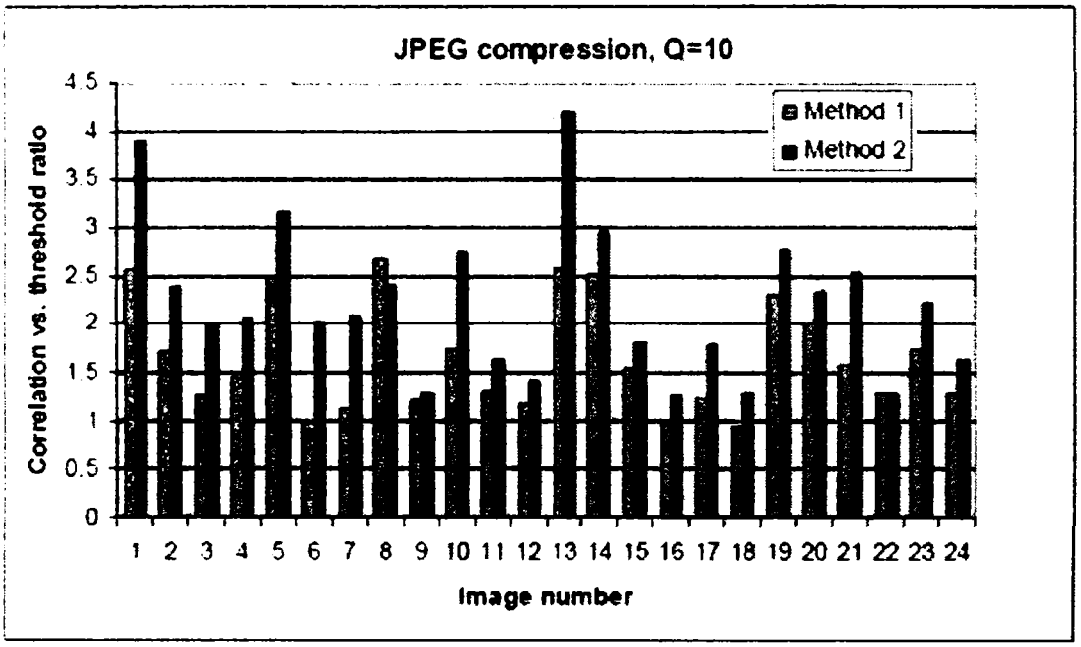


Fig. 5.24(c): Raport corelaţie/prag, comparaţia robusteţii în cazul compresiei JPEG, factor de calitate 10

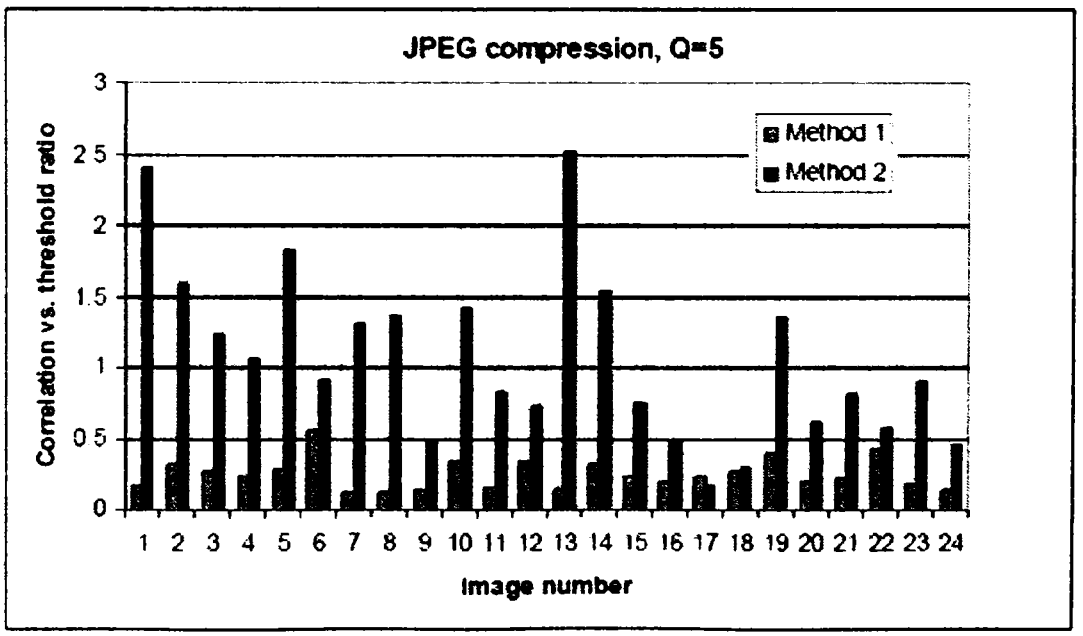


Fig. 5.24(d): Raport corelaţie/prag, comparaţia robusteţii în cazul compresiei JPEG, factor de calitate 5

Tab. 5.6: Raport corelaţie/prag, comparaţia robusteţii în cazul filtrării mediane şi a redimensionării. Intensitatea maximă de marcare este dată de constrângerea de invizibilitate [Naf07a].

Imagine	*Filtrare mediană M=3*		*Filtrare mediană M=5*		*Redimensionare 75%*		*Redimensionare 50%*	
	1	*2*	*1*	*2*	*1*	*2*	*1*	*2*
IM1	0.47	1.21	0.29	-0.46	8.95	12.33	2.13	0.85
IM2	1.22	2.53	0.38	0.69	10.21	11.37	2.11	1.02
IM3	0.34	1.65	0.13	0.41	8.49	14.22	1.59	1.27
IM4	0.68	1.41	0.05	0.52	11.52	14.09	1.34	1.32
IM5	0.68	1.74	0.23	0.59	9.15	12.48	1.84	1.07
IM6	1.57	2.83	0.59	1.39	14.09	17.55	2.31	1.40
IM7	0.62	1.29	0.24	0.27	7.02	11.93	1.29	1.27
IM8	0.54	1.52	0.00	0.42	12.10	11.18	1.85	0.83
IM9	1.02	1.33	0.55	0.66	11.96	12.42	2.14	1.47
IM10	0.73	2.40	0.27	0.92	10.88	15.37	1.98	1.35
IM11	0.92	0.54	0.36	0.46	16.97	17.33	1.99	1.76
IM12	0.50	0.97	0.13	-0.14	9.04	12.67	1.46	0.62
IM13	0.47	3.59	0.20	0.66	9.55	17.28	1.95	1.41
IM14	0.24	1.21	-0.02	0.02	10.20	12.57	1.66	1.30
IM15	0.67	1.61	0.15	-0.10	12.86	16.83	2.32	1.26
IM16	0.56	-1.04	0.22	-0.33	10.22	18.94	2.07	1.55
IM17	0.80	-0.08	0.50	-0.68	13.49	18.63	2.91	1.40
IM18	0.53	1.31	0.18	0.10	10.25	15.03	1.16	1.20
IM19	0.50	1.12	0.06	-0.20	14.19	15.42	2.83	1.09
IM20	0.29	1.54	-0.07	-0.27	14.10	14.14	2.70	1.06
IM21	0.24	1.27	0.00	-0.50	13.31	16.40	2.48	1.30
IM22	0.29	-0.63	0.24	-0.69	11.69	17.99	2.35	1.64
IM23	0.58	0.87	0.34	-0.60	11.64	16.74	2.48	1.05
IM24	0.75	1.98	0.30	-0.26	15.28	19.79	2.82	1.54

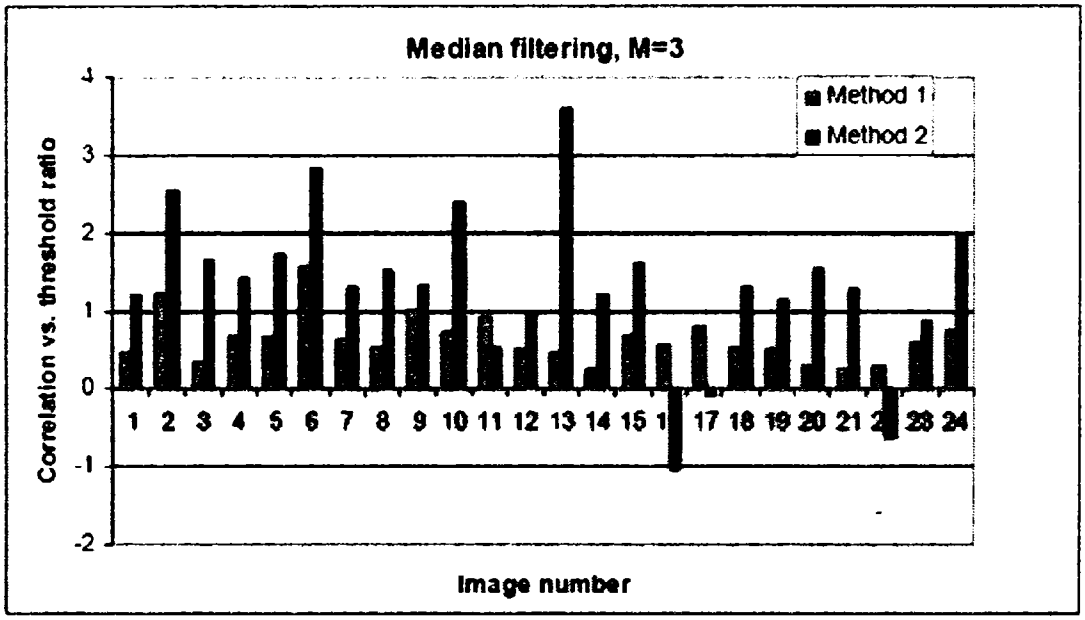


Fig. 5.25(a): Raport corelaţie/prag, comparaţia robusteţii în cazul filtrării mediene, dimensiune filtru 3

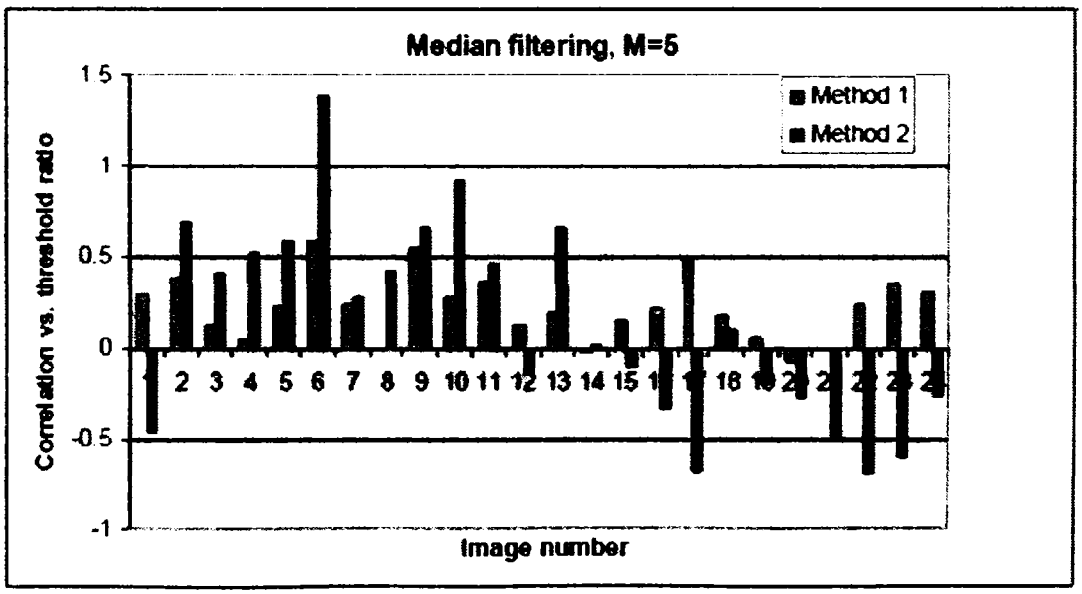


Fig. 5.25(b): Raport corelaţie/prag, comparaţia robusteţii în cazul filtrării mediene, dimensiune filtru 5

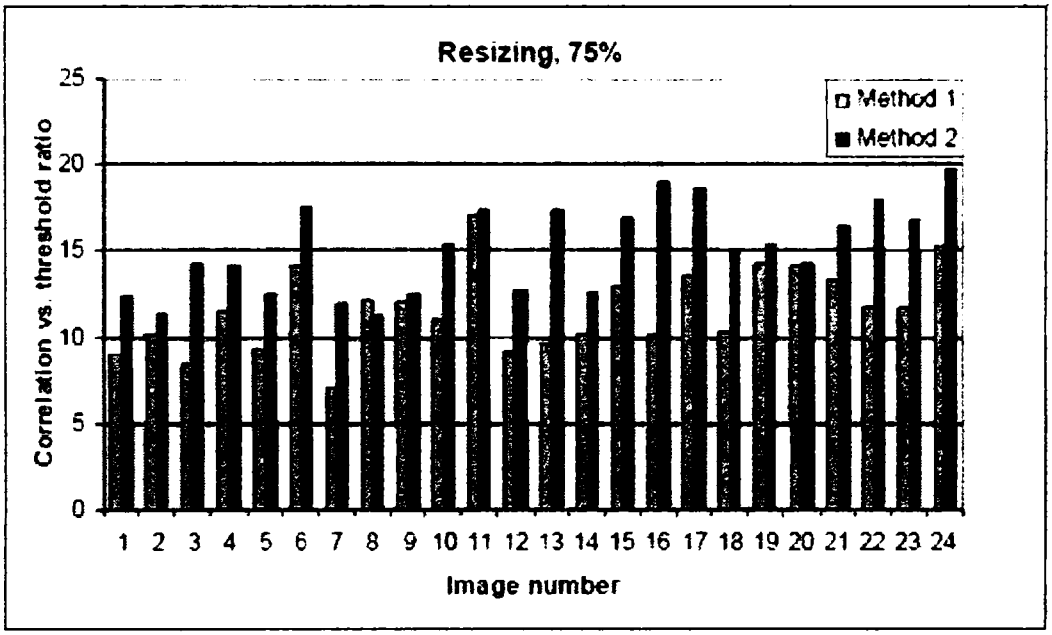


Fig. 5.26(a): Raport corelaţie/prag, comparaţia robusteţii în cazul redimensionare, 75%

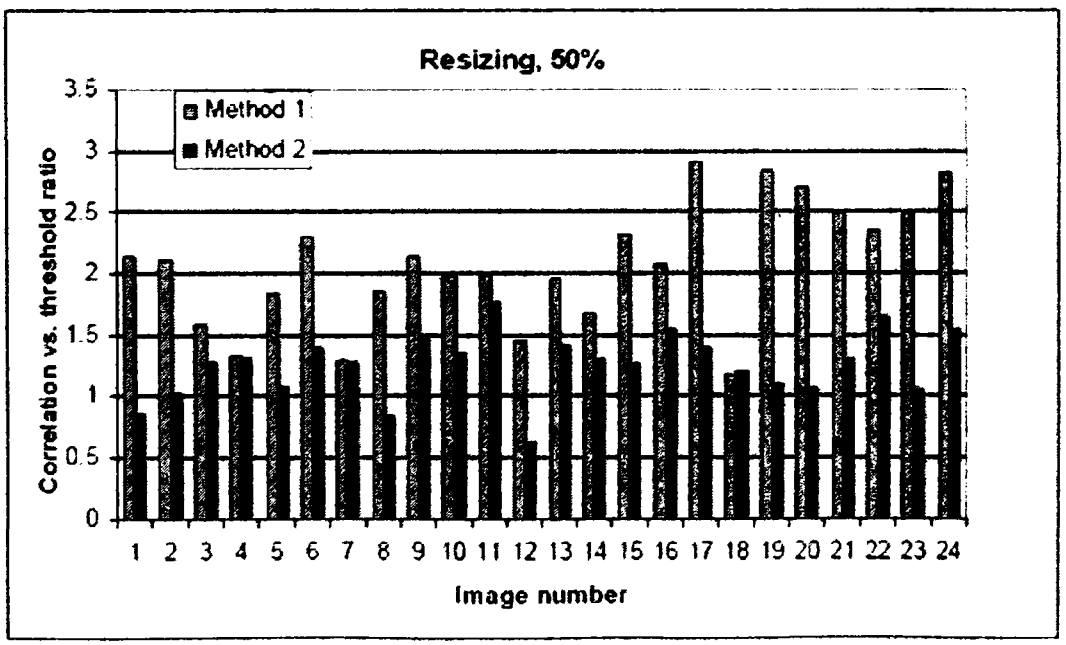


Fig. 5.26(b): Raport corelaţie/prag, comparaţia robusteţii în cazul redimensionării, 50%

Tab. 5.7: Raport corelaţie/prag, comparaţia robusteţii în cazul corecţiei de gamma. Intensitatea maximă de marcare este dată de constrângerea de invizibilitate [Naf07a].

Imagine	*γ=0.5*		*γ=1*		*γ=1.5*		*γ=2*	
	1	*2*	*1*	*2*	*1*	*2*	*1*	*2*
IM1	25.04	28.43	25.33	28.97	25.22	28.99	25.04	28.80
IM2	24.82	27.14	28.49	25.51	30.00	23.95	30.74	22.67
IM3	35.31	37.03	32.92	39.32	32.02	40.83	31.52	42.03
IM4	37.06	36.11	39.86	35.56	40.28	34.30	40.34	32.65
IM5	26.72	31.09	29.97	30.10	30.83	28.48	31.05	26.78
IM6	44.23	43.13	44.07	44.87	43.04	45.31	42.43	44.81
IM7	21.24	29.81	25.33	28.61	26.54	26.68	26.95	24.81
IM8	29.36	31.00	35.25	27.39	38.20	25.21	38.88	23.76
IM9	40.40	32.61	40.89	34.89	39.91	34.98	38.30	34.86
IM10	33.47	36.60	35.60	37.46	35.80	36.91	35.41	35.95
IM11	47.55	40.51	46.41	42.86	44.90	43.89	43.87	44.00
IM12	25.88	26.75	27.19	29.89	26.23	30.09	24.96	29.10
IM13	34.77	39.77	32.89	42.47	31.70	43.80	30.96	44.49
IM14	30.58	30.21	32.94	31.06	32.98	30.50	32.59	29.44
IM15	40.14	39.06	39.46	40.75	38.61	41.56	37.98	41.72
IM16	34.03	40.35	30.03	44.97	27.73	47.71	27.34	49.59
IM17	37.80	41.75	37.00	43.79	36.13	44.65	35.57	45.02
IM18	41.87	33.93	40.00	40.45	37.93	42.48	35.31	43.47
IM19	37.46	36.81	39.57	36.66	39.95	35.96	39.99	35.04
IM20	37.30	34.34	39.98	34.17	40.48	33.36	40.44	32.36
IM21	37.38	37.21	36.73	38.91	35.88	39.54	35.11	39.66
IM22	33.01	39.61	31.85	42.41	30.86	43.72	30.01	44.83
IM23	34.89	38.47	34.68	40.17	34.06	40.98	33.67	41.19
IM24	44.30	46.28	44.34	47.56	43.73	47.85	43.22	47.77

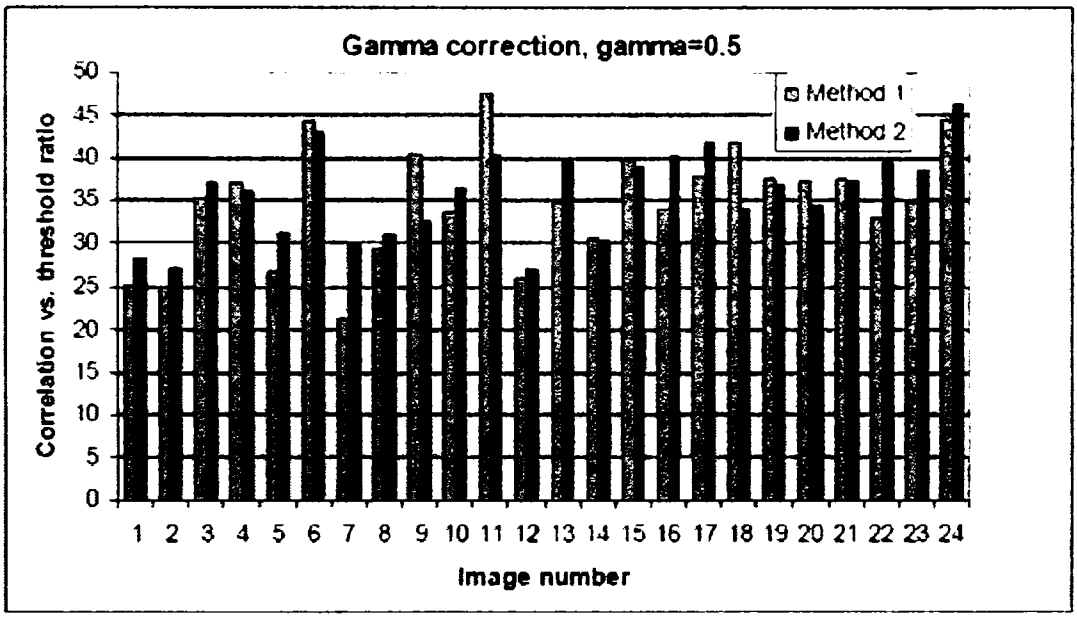


Fig. 5.27(a): Raport corelaţie/prag, comparaţia robusteţii în cazul corecţiei de gamma, γ=0.5

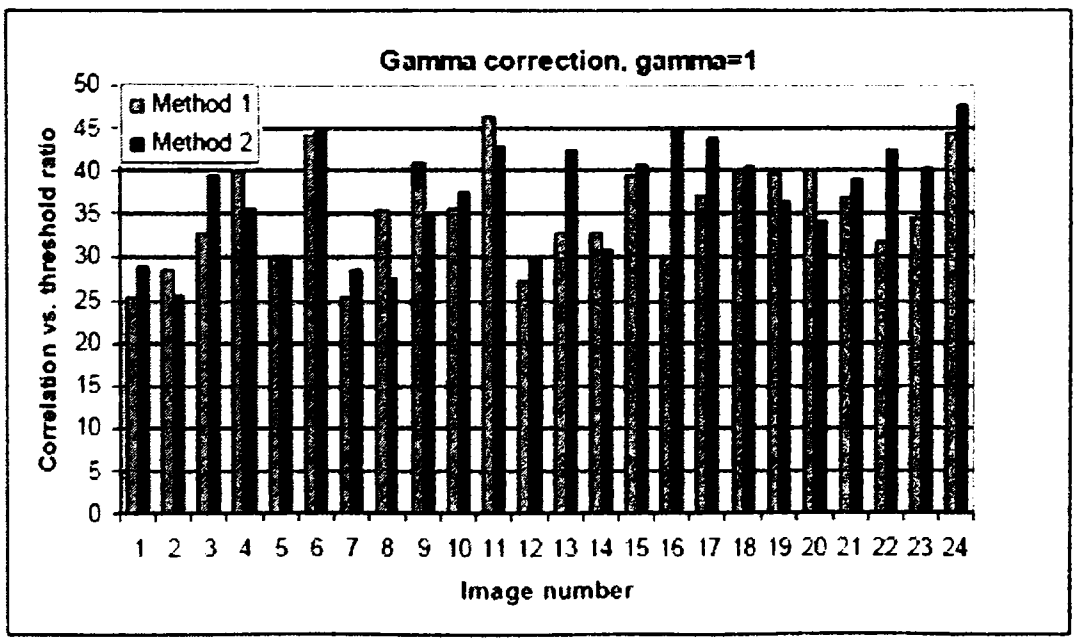


Fig. 5.27(b): Raport corelaţie/prag, comparaţia robusteţii în cazul corecţiei de gamma, γ=1

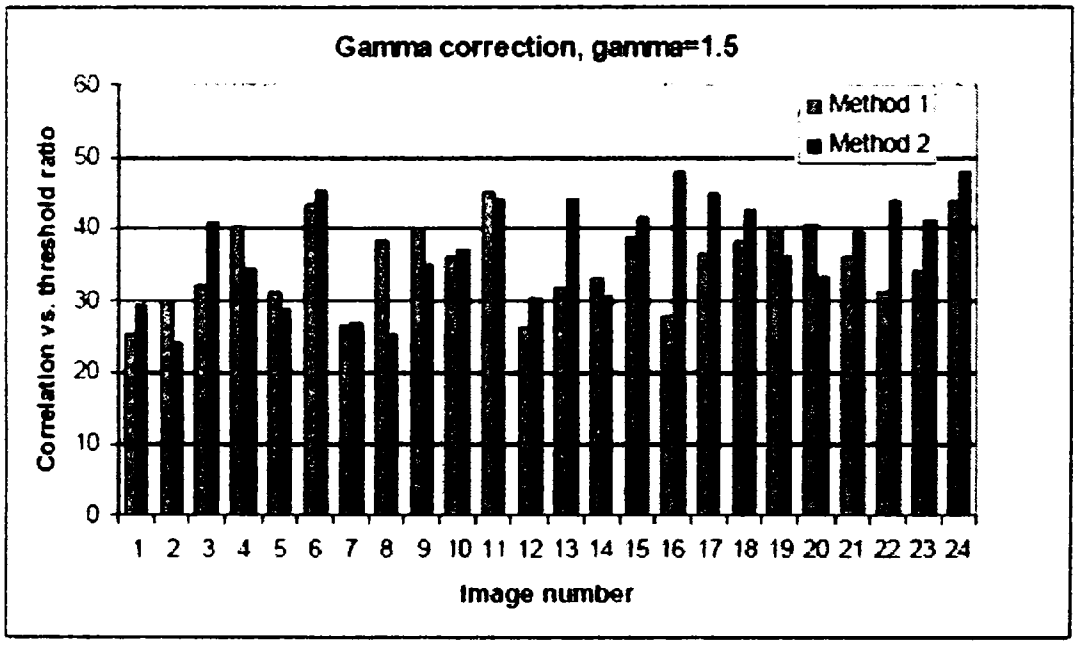


Fig. 5.27c): Raport corelaţie/prag, comparaţia robusteţii în cazul corecţiei de gamma, γ=1.5

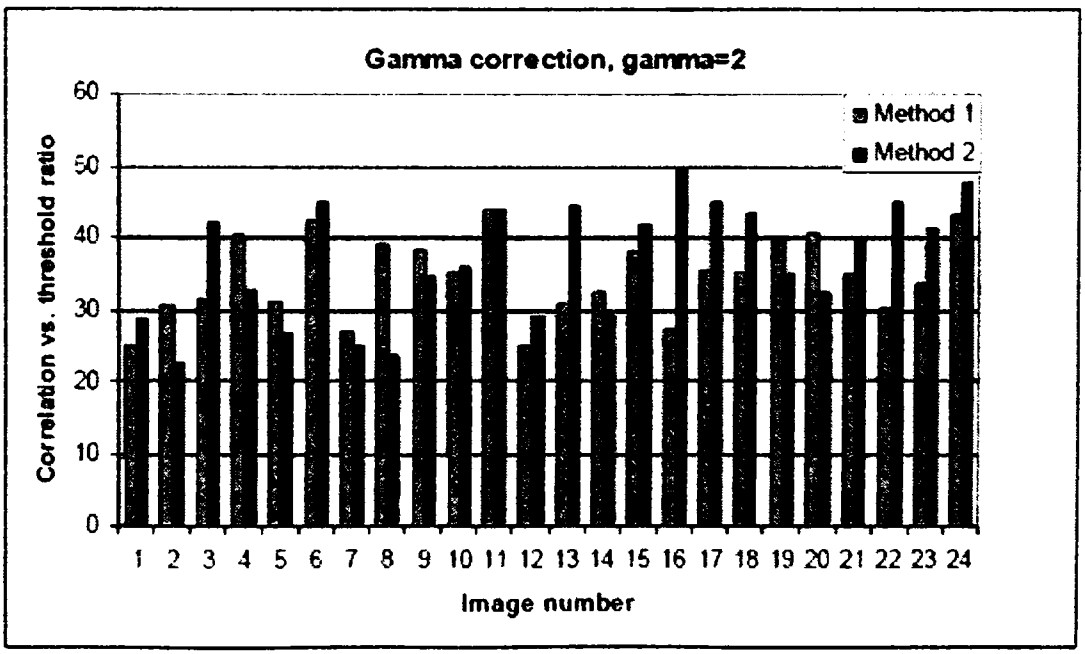


Fig. 5.27(d): Raport corelaţie/prag, comparaţia robusteţii în cazul corecţiei de gamma, γ=2

Tab. 5.8: Raport corelaţie/prag, comparaţia robusteţii în cazul decupării. Intensitatea maximă de marcare este dată de constrângerea de invizibilitate [Naf07a].

Imagine	*256x256*		*128x128*		*64x64*		*32x32*	
	1	*2*	*1*	*2*	*1*	*2*	*1*	*2*
IM1	14.11	15.62	8.61	5.15	3.19	2.39	1.61	0.90
IM2	12.86	11.94	5.46	4.79	2.46	1.61	1.29	0.50
IM3	17.68	14.82	8.23	6.71	3.67	2.75	1.61	1.16
IM4	15.82	13.64	7.42	5.79	2.62	2.62	1.21	1.04
IM5	14.14	13.92	7.38	6.23	3.40	2.69	1.60	1.36
IM6	18.08	14.60	8.01	5.11	3.92	2.13	1.85	0.79
IM7	10.56	13.98	4.74	7.38	1.99	3.56	0.83	1.51
IM8	15.17	10.56	6.68	3.21	2.18	2.26	1.05	1.33
IM9	18.32	13.72	8.23	6.01	3.53	2.42	1.80	0.97
IM10	15.66	15.44	8.21	7.04	3.48	2.78	2.13	0.83
IM11	18.59	13.82	8.48	6.15	3.38	2.63	1.52	1.04
IM12	16.15	13.81	6.97	6.09	2.50	2.79	1.08	1.00
IM13	16.32	16.41	7.30	6.64	2.84	2.90	1.48	1.26
IM14	15.72	15.02	7.53	5.72	2.45	2.46	1.30	1.18
IM15	14.64	13.37	5.57	6.02	1.62	2.19	0.76	0.81
IM16	13.33	11.24	6.59	5.35	2.65	2.50	1.02	1.07
IM17	14.95	13.34	6.22	5.96	2.18	2.96	0.93	1.21
IM18	13.97	14.48	6.57	5.43	2.23	2.29	1.00	0.80
IM19	15.41	14.52	6.95	6.45	2.44	2.60	1.04	0.87
IM20	15.46	14.18	6.51	6.13	2.62	2.63	1.05	1.00
IM21	14.15	13.54	6.09	5.13	2.68	2.03	1.06	0.99
IM22	11.87	11.54	5.52	4.87	1.78	3.17	0.79	1.00
IM23	14.55	13.52	6.19	6.64	3.17	2.31	1.09	0.96
IM24	15.69	14.18	6.63	6.32	2.01	2.64	0.94	0.78

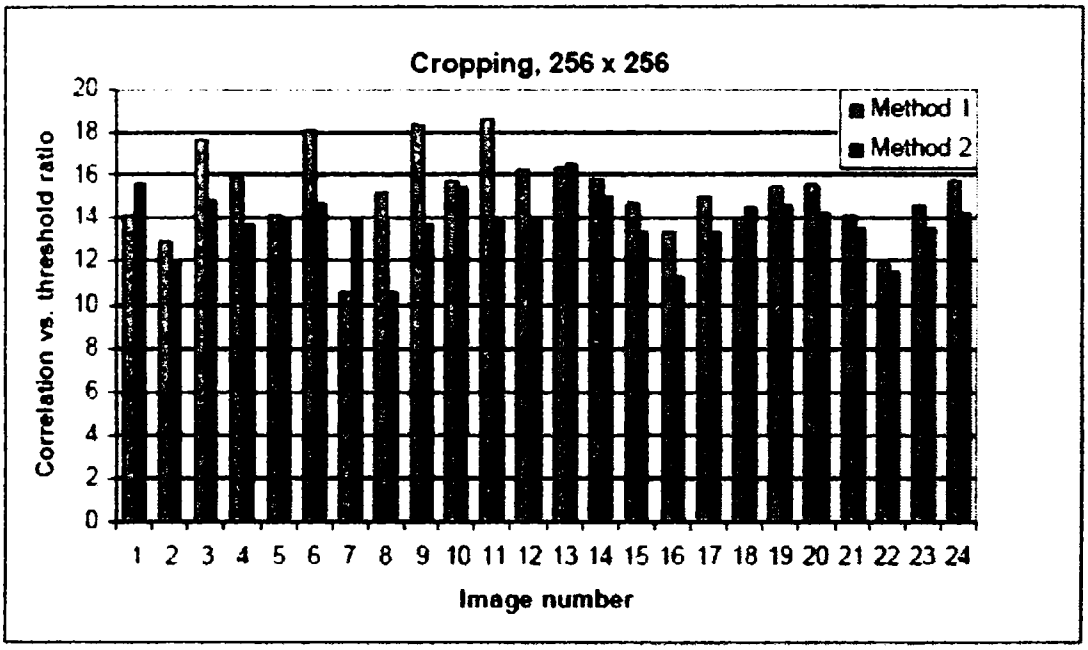


Fig. 5.28(a): Raport corelaţie/prag, comparaţia robusteţii în cazul decupării 256x256

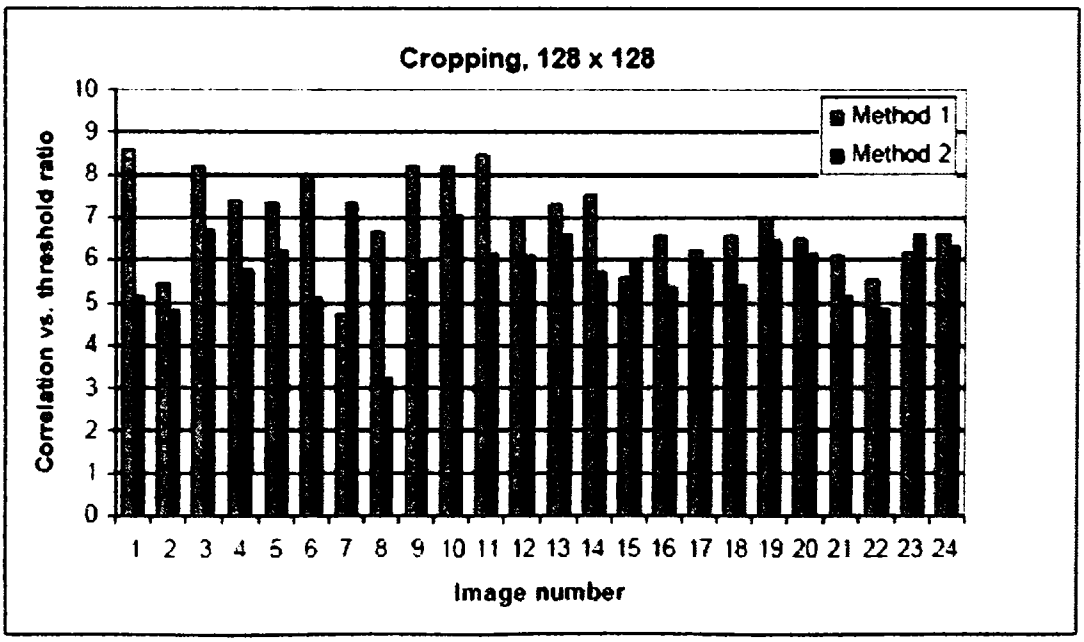


Fig. 5.28(b): Raport corelaţie/prag, comparaţia robusteţii în cazul decupării 128x128

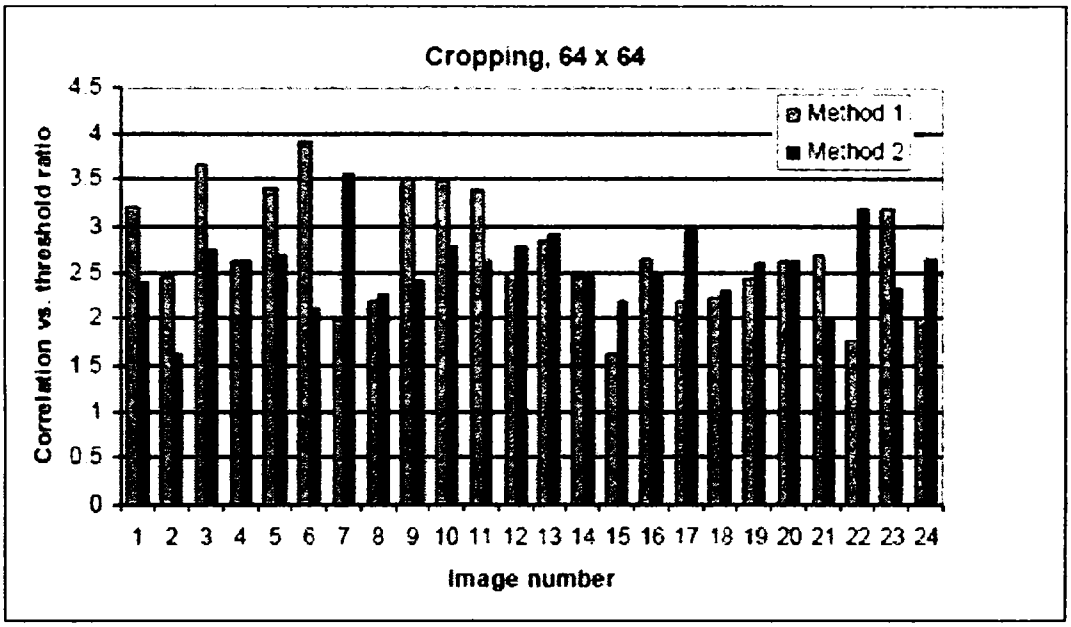


Fig. 5.28(c): Raport corelaţie/prag, comparaţia robusteţii în cazul decupării 64x64

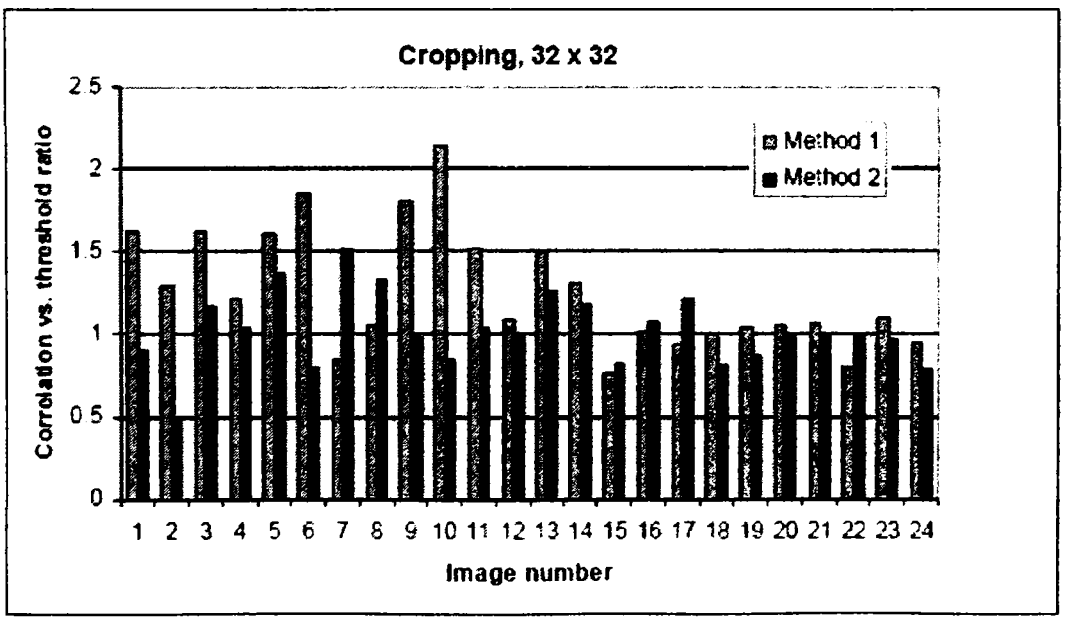


Fig. 5.28(d): Raport corelaţie/prag, comparaţia robusteţii în cazul decupării 32x32

5.8 Înserare în toate subnivelele de rezoluţie

În acest paragraf, se investighează folosirea mascării perceptuale prezentată mai sus pentru înserarea marcajului în **toate subnivelele** de rezoluţie [Naf07b]. Sunt folosite trei detectoare care folosesc avantajele descompunerii multirezoluţie a transformării wavelet. Marcajul este detectat din: 1) toate nivelele de rezoluţie, 2) separat din fiecare nivel, considerând maximul răspunsurilor de pe nivele, şi 3) separat din fiecare subbandă, considerând maximul răspunsurilor de pe subbenzi. Evaluarea corelaţiilor pe nivele de rezoluţie, respectiv subbandă, este câteodată avantajoasă. De exemplu pentru decupare, marcajul este mai greu de detectat în frecvenţe joase decât înalte, pe când filtrarea trece-jos afectează frecvenţele înalte. Astfel, se elimină nivelele sau subbenzile de rezoluţie cu corelaţie mică similar cu abordarea din [PZ98]. Acest tip de înserare combinat cu noile detectoare face algoritmul mai rezistent la atacuri gen ştergerea tuturor celor trei subbenzi care conţineau marcajul în nivelul zero. În [BBP01] detecţia este făcută aşa cum am văzut în paragrafele anterioare, folosind coeficientul de corelaţie pentru nivelul $l = 0$:

$$\rho(l) = \frac{4^l}{3MN} \sum_{\theta=0}^{2} \sum_{i=0}^{M/2^l-1} \sum_{j=0}^{N/2^l-1} \tilde{I}_l^{\theta}(i,j) x_l^{\theta}(i,j) \qquad (5.15)$$

Autorii au făcut presupuneri simplificatoare asupra variabilelor aleatoare. Valorile marcajului $x_l^{\theta}(i,j)$ sunt variabile aleatoare binare, de medie nulă. Este făcută o presupunere realistă privind coeficienţii wavelet, aceea că sunt variabile aleatoare gaussiene, statistic independente, de medie nulă. Conform teoremei limită centrală, $\rho(l)$ este de asemenea presupusă a fi distribuită normal. Fiind dată o imagine şi un marcaj , sunt posibile numai trei cazuri:

A. Imaginea nu este marcată
B. Imaginea este marcată cu o secvenţă Y alta decât X.
C. Imaginea este marcată cu secvenţa căutată, şi anume X.

Astfel există două ipoteze:

H_0: Marcajul căutat nu este înserat în imaginea recepţionată, incluzând cazul A şi B,
H_1: Marcajul adevărat este inserat în imaginea recepţionată, deci cazul C.

Printr-o analiză simplă autorii [BBP01] arată că în ambele ipoteze, H_0 şi H_1, corelaţiile sunt normal distribuite şi mediile lor sunt:

H_0: $\mu_{\rho(l)_0} = 0$.

H_1: $\mu_{\rho(l)_1} = \frac{4^l}{3MN} \alpha \sum_{\theta=0}^{2} \sum_{i=0}^{M/2^l-1} \sum_{j=0}^{N/2^l-1} E\left[w_l^{\theta}(i,j) \right]$.

Un marcaj X este prezent dacă $\rho(l) > T_{\rho(l)}$. Probabilitatea de fals pozitiv (de detecţie a marcajului când nu există) este $P_{fp} = \text{Prob}\left\{\rho(l) > T_{\rho(l)} \middle| H_0\right\}$. Pentru a estima această probabilitate, în [BBP01] sunt calculate dispersiile pentru corelaţiile din cazul A şi B:

$$\sigma^2_{\rho(l)_A} = \left(\frac{4^l}{3MN}\right)^2 \sigma_x^2 \sum_{\theta=0}^{2} \sum_{i=0}^{M/2^l-1} \sum_{j=0}^{N/2^l-1} E\left[\left(I_l^\theta(i,j)\right)^2\right]$$

$$\sigma^2_{\rho(l)_B} = \left(\frac{4^l}{3MN}\right)^2 \sigma_x^2 \sum_{\theta=0}^{2} \sum_{i=0}^{M/2^l-1} \sum_{j=0}^{N/2^l-1} E\left[\left(I_l^\theta(i,j)\right)^2\right] + \alpha^2\sigma_x^2 E\left[\left(w_l^\theta(i,j)\right)^2\right]$$

Cazul B este cazul cel mai nefavorabil, cu cât este mai mare varianţa cu atât mai mare este probabilitatea de eroare. Corelaţia este comparată cu pragul $T_{\rho(l)}$, calculat pentru a da o probabilitate de detecţie falsă (fals pozitiv), folosind criteriul Neyman-Pearson [Kay03]:

$$P_{fp} \le \frac{1}{2}\text{erfc}\left(\frac{T_{\rho(l)}}{\sqrt{2\sigma^2_{\rho(l)_B}}}\right)$$

Spre exemplu, dacă $P_{fp} \le 10^{-8}$, pragul este:

$$T_{\rho(l)} = 3.97\sqrt{\sigma^2_{\rho(l)}},$$

cu $\sigma^2_{\rho(l)}$ dispersia coeficienţilor wavelet, dacă imaginea a fost marcată cu un marcaj Y altul decât X:

$$\sigma^2_{\rho(l)} \approx \left(\frac{4^l}{3MN}\right)^2 \sum_{\theta=0}^{2} \sum_{i=0}^{M/2^l-1} \sum_{j=0}^{N/2^l-1} \left(\tilde{I}_l^\theta(i,j)\right)^2 \qquad (5.16)$$

Considerăm raportul dintre corelaţie $\rho(l)$ din relaţia (5.15) şi pragul dependent de imagine $T_{\rho(l)}$, ca şi în cazurile precedente. Urmărind acelaşi raţionament din

[BBP01], primul detector evaluează prezenţa marcajului în toate nivelele de rezoluţie:

$$d_1 = \frac{\rho_{d1}}{T_{d1}} \tag{5.17}$$

unde corelaţia este:

$$\rho_{d1} = \frac{1}{3MN\sum_{l=0}^{2} 4^{-l}} \sum_{l=0}^{2}\sum_{\theta=0}^{2}\sum_{i=0}^{M/2^l-1}\sum_{j=0}^{N/2^l-1} \tilde{I}_l^{\theta}(i,j)x_l^{\theta}(i,j) \tag{5.18}$$

şi pragul este determinat pentru $P_{fp} \le 10^{-8}$:

$$T_{d1} = 3.97\sqrt{\sigma^2_{\rho_{d1}}} \tag{5.19}$$

$$\sigma^2_{\rho_{d1}} \approx \frac{1}{\left(3MN\sum_{l=0}^{2} 4^{-l}\right)^2} \sum_{l=0}^{2}\sum_{=}^{2}\sum_{i=}^{M/2^l-1}\sum_{j=}^{N/2^l-1}\left(\tilde{I}_l^{\theta}(i,j)\right)^2 \tag{5.20}$$

În general, coeficienţii wavelet sunt consideraţi a fi variabile aleatoare cu anumite densităţi de probabilitate, cum ar fi cea gaussiană. Astfel de modele statistice simple sunt necorespunzătoare pentru coeficienţii wavelet dintr-o imagine naturală, deoarece nu sunt luate în considerare dependenţele între coeficienţi inter-scală şi intra-scală [SS02]. Există interdependenţe puternice între coeficienţi vecini cum ar fi un coeficient, părintele (localizat adiacent la un nivel de rezoluţie mai brut) şi fraţi (localizaţi adiacent în spaţiu).

Ignorând acest fapt, presupunem că există independenţa statistică a coeficienţilor wavelet de la nivele de rezoluţie diferite şi subbenzi diferite. Am trasat în acest scop histograma corelaţiilor pentru imaginea Lena, şi pentru imaginea marcată (Figura 5.29). Am efectuat testul Pearson chi-square pe ambele distribuţii empirice; ipoteza gaussiană a fost acceptată la un prag de semnificaţie 0.05, nivel de încredere de 95% şi am considerat că primul detector propus este valid [Naf07b].

Al doilea detector consideră răspunsurile detectoarelor de la diferite nivele, adică $d(l)=\rho(l)/T(l)$, cu $l \in \{0,1,2\}$, şi le elimină pe cele cu valoare de detecţie mai mică:

$$d_2 = \max_l\{d(l)\} \tag{5.21}$$

Al treilea detector consideră răspunsurile de la subbenzi şi nivele diferite, ca fiind $d(l, \theta) = \rho(l, \theta) / T(l, \theta)$, cu $l, \theta \in \{0,1,2\}$, şi le elimină pe cele cu valoare de detecţie mai mică:

$$d_3 = \max_{\theta,l}\left\{d(l,\theta)\right\} \tag{5.22}$$

Corelaţiile şi pragul sunt calculate folosind acelaşi raţionament per subbandă, indicându-i orientarea şi nivelul.

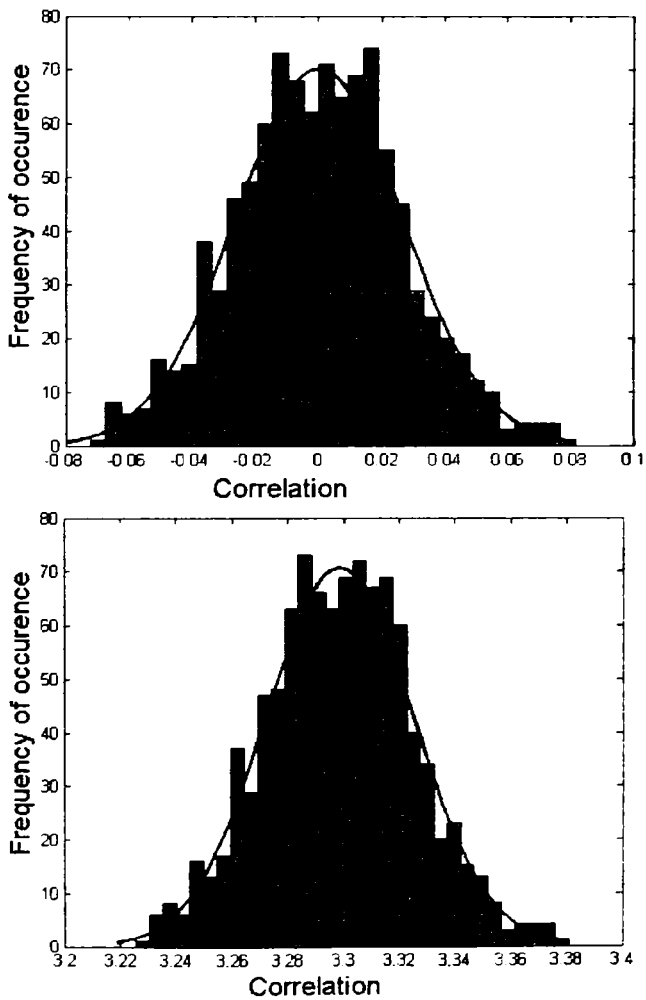


Fig.5.29: Distribuţii empirice ale corelaţiilor pentru primul detector, sus, imaginea originală şi jos, imaginea marcată cu α=1.5, [Naf07b].

Rezultate obţinute în urma simulărilor. Au fost marcate mai multe imagini de mărime 512×512, de această dată la toate nivelele $l \in \{0,1,2\}$, folosind masca perceptuală prezentată. Intensitatea de marcare α a fost fixată la 1.5 in toate experimentele privind metoda propusă. Imaginile marcate sunt neafectate de procesul de marcare faţă de originale.

Pentru metoda din [BBP01] am inserat un marcaj în toţi coeficienţii de detaliu de la primul nivel de rezoluţie, $l=0$, pentru $\alpha=0.2$, aşa cum s-a discutat şi în paragraful anterior. Aceasta rezultă într-adevăr într-o calitate similară a imaginilor, conform Fig. 5.30.

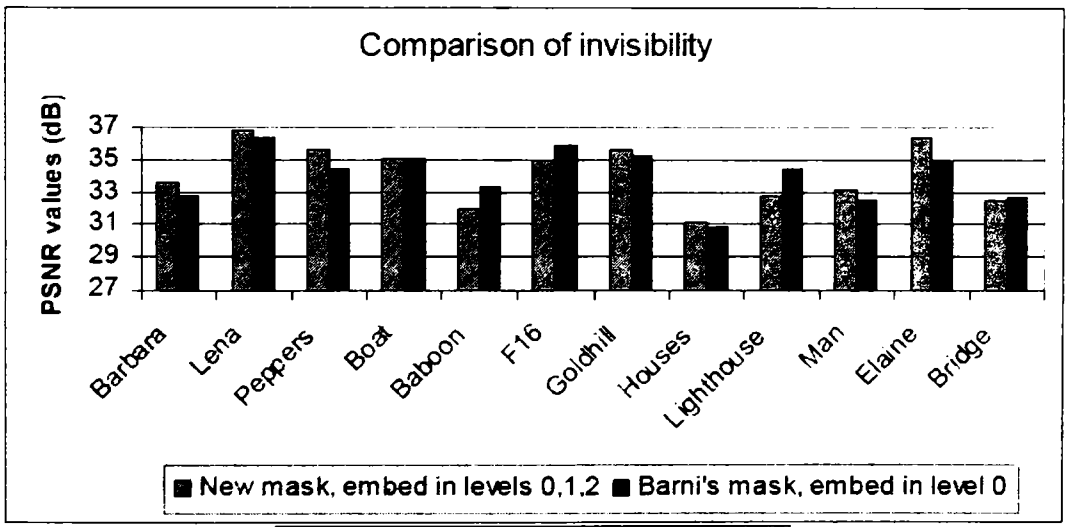
Ceea ce rămâne constant pentru comparare, sunt marcajele bidimensionale inserate în primul nivel, respectiv $x_0^{\theta}(i,j)$, precum şi calitatea imaginii. Nu comparăm metoda din [Naf07b] cu cea din [BBP01] atunci când marcajul este inserat în toate nivelele de rezoluţie, fiindcă masca lor nu este potrivită pentru inserare în alte nivele decât cel de rezoluţie înaltă.

Fig.5.30: Imaginea originală Lena, precum şi imaginile marcate pentru (stânga) metoda propusă [Naf07b], α=1.5, PSNR=36.86 dB, (dreapta) metoda lui Barni şi alţii [BBP01], α=0.2, PSNR=36.39 dB

Se prezintă rezultatele pentru unele imagini standard din baza de date USC-SIPI Image Database [USC], folosite şi anterior. Tabelul 5.9 prezintă valorile PSNR pentru ambele cazuri. În fig. 5.31, se prezintă un grafic cu valorile PSNR pentru fiecare imagine, precum şi o valoare medie per metodă.

Tab. 5.9. Compariţie a invizibilităţii

Imagine vs. PSNR (dB)	*Metoda propusă*	*Metoda lui Barni şi alţii*
Barbara	33.68	32.83
Lena	36.86	36.39
Peppers	35.61	34.40
Boat	35.05	35.05
Baboon	32.01	33.33
F16	34.92	35.90
Goldhill	35.64	35.28
Houses	31.17	30.97
Lighthouse	32.79	34.38
Man	33.28	32.60
Elaine	36.35	34.98
Bridge	32.58	32.66



Metoda propusă	Metoda lui Barni
34.16 dB	34.06 dB

Fig. 5.31: Valori PSNR, comparaţia invizibilităţii, împreună cu valorile medii pentru cele două metode.

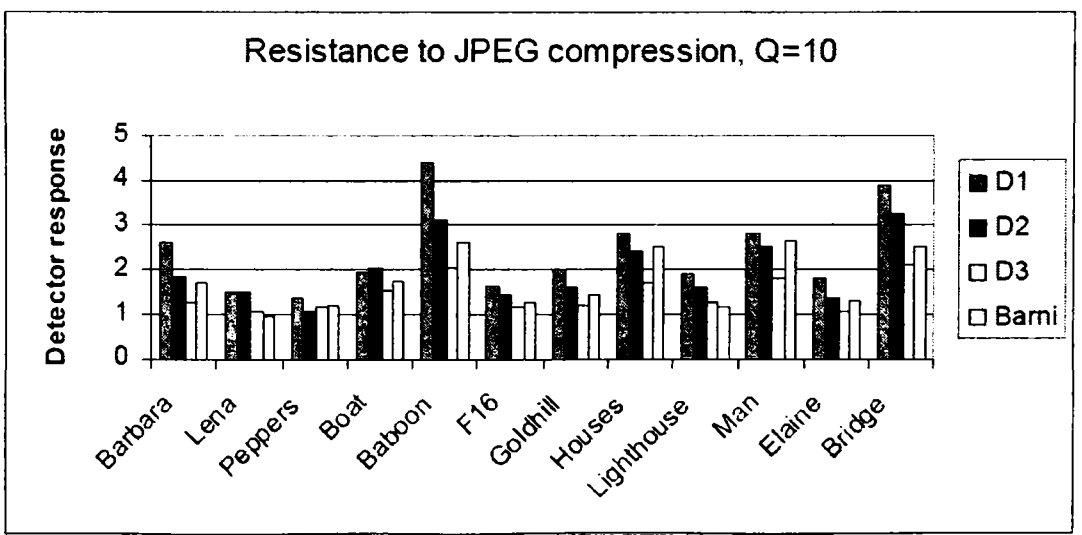
Pentru primul detector, prezentăm de asemenea un estimat al probabilităţii de detecţie falsă pentru imaginea Lena, înainte şi după compresia JPEG cu factor de calitate Q=10, ca şi funcţie de pragurile de detecţie, $T_{\rho 1}$. Valorile de prag au fost calculate folosind estimata dispersiei lui ρ_1 obţinute în urma experimentelor.

S-au efectuat teste folosind prelucrări de semnal obişnuite, compresie JPEG, filtrare mediană, decupare, redimensionare, corecţie gamma şi blurring. Pentru

fiecare imagine atacată, şi fiecare detector, sunt calculate valorile, d_i, pentru $i \in \{1,2,3\}$, raportul între corelaţie şi pragul dependent de imagine. Probabilitatea de fals pozitiv este fixată la 10^{-8}. Tabelele 5.10 – 5.15 prezintă răspunsul detectoarelor pentru fiecare imagine, atac şi metodă. Pentru o mai bună vizualizare a rezultatelor, prezentăm şi grafice cu valorile corelaţiilor în funcţie de imagini pentru fiecare atac, precum şi o valoare medie per detector.

Tab. 5.10. Rezistenţa la compresia JPEG, Q=10

Imagine vs. Răspunsul detectorului	***Metoda propusă***			***Metoda lui Barni***
	d1	***d2***	***d3***	
Barbara	2.61	1.87	1.27	1.71
Lena	1.50	1.51	1.04	0.97
Peppers	1.34	1.04	1.13	1.20
Boat	1.93	2.04	1.53	1.74
Baboon	4.39	3.11	2.06	2.58
F16	1.64	1.47	1.17	1.27
Goldhill	2.01	1.60	1.18	1.45
Houses	2.79	2.38	1.71	2.49
Lighthouse	1.89	1.62	1.24	1.13
Man	2.81	2.50	1.82	2.66
Elaine	1.78	1.37	1.06	1.31
Bridge	3.91	3.25	2.08	2.51



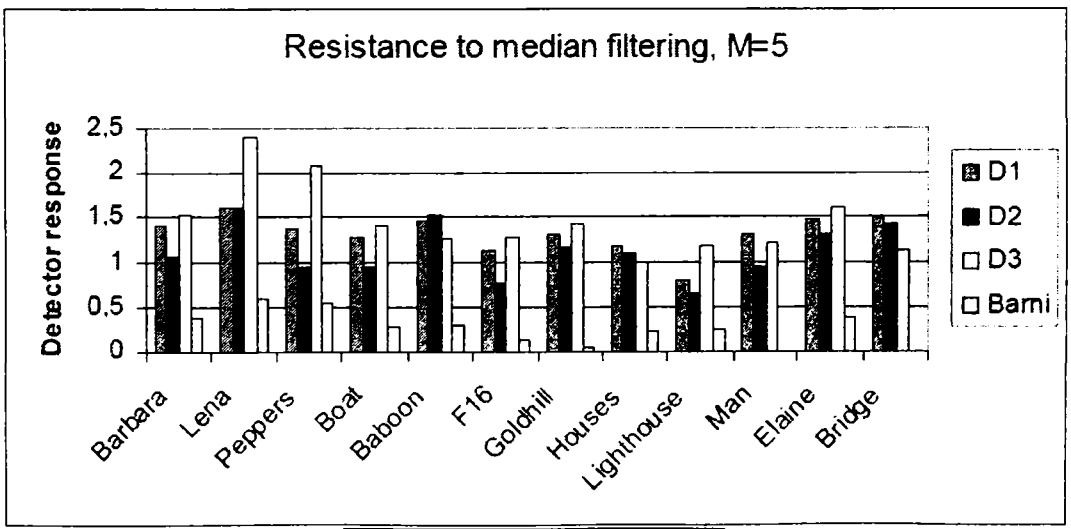
D1	D2	D3	Barni
2.38	**1.98**	**1.44**	**1.75**

Fig. 5.32: Raport corelaţie/prag, comparaţia robusteţii în cazul compresiei JPEG, Q=10, împreună cu valorile medii pentru detectoare.

Am ales parametrul atacului pentru care marcajul este încă detectabil cu cel puţin o metodă. La compresia JPEG, metoda propusă a detectat cu succes marcajul până la factorul de calitate 10. Primul detector este mai bun în toate cazurile. Metoda propusă în [Naf07b] are rezultate mai bune decât tehnica lui Barni [BBP01].

Tab. 5.11. Rezistenţa la filtrare mediană, M=5

Imagine vs. Răspunsul detectorului	***Metoda propusă***			***Metoda lui Barni***
	d1	***d2***	***d3***	
Barbara	1.41	1.06	1.53	0.38
Lena	1.60	1.60	2.40	0.59
Peppers	1.38	0.95	2.09	0.55
Boat	1.29	0.94	1.40	0.27
Baboon	1.45	1.53	1.27	0.29
F16	1.13	0.77	1.29	0.13
Goldhill	1.31	1.16	1.44	0.05
Houses	1.20	1.08	0.98	0.23
Lighthouse	0.78	0.65	1.19	0.24
Man	1.32	0.95	1.21	0.01
Elaine	1.49	1.32	1.60	0.36
Bridge	1.52	1.43	1.15	-0.02



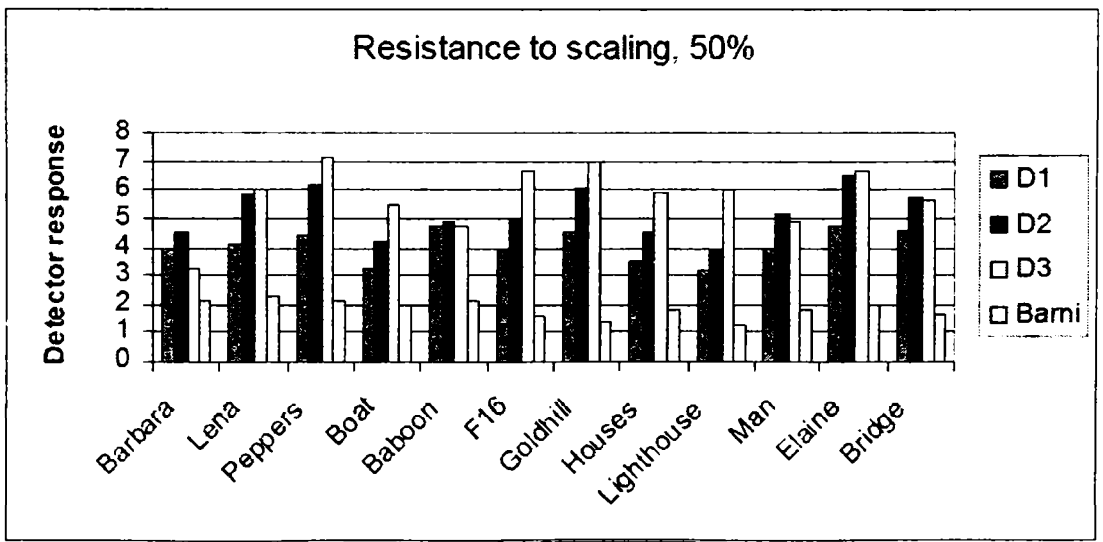
D1	D2	D3	Barni
1.32	1.12	1.46	0.25

Fig. 5.33: Raport corelaţie/prag, comparaţia robusteţii în cazul filtrării mediene, M=5, împreună cu valorile medii pentru detectoare.

Pentru ambele metode, marcajul a supravieţuit în toate imaginile pentru filtrare mediană cu lungimea ferestrei filtrului până la 3. Pentru M=5, marcajul înserat cu metoda propusă în [Naf07b] folosind primul şi al treilea detector poate fi recuperat, dar metoda lui Barni nu reuşeşte să găsească marcajul.

Tab. 5.12. Rezistenţa la redimensionare, 50%

Imagine vs. Răspunsul detectorului	***Metoda propusă***			***Metoda lui Barni***
	d1	***d2***	***d3***	
Barbara	3.94	4.50	3.26	2.11
Lena	4.13	5.86	6.01	2.31
Peppers	4.42	6.20	7.09	2.14
Boat	3.23	4.20	5.45	1.98
Baboon	4.74	4.89	4.73	2.13
F16	3.85	4.97	6.63	1.59
Goldhill	4.48	6.12	6.98	1.34
Houses	3.50	4.49	5.93	1.84
Lighthouse	3.15	3.87	6.00	1.29
Man	3.96	5.11	4.88	1.85
Elaine	4.78	6.53	6.62	1.99
Bridge	4.59	5.77	5.64	1.66



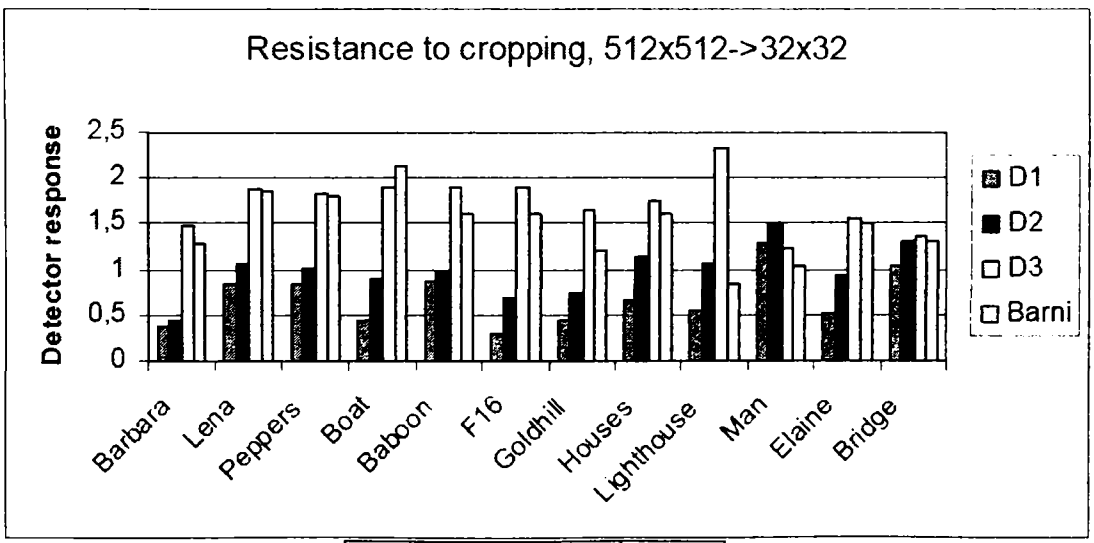
D1	D2	D3	Barni
4.06	**5.21**	**5.76**	**1.85**

Fig. 5.34: Raport corelaţie/prag, comparaţia robusteţii în cazul redimensionării, 50%, împreună cu valorile medii pentru detectoare.

În cazul redimensionării la 50%, marcajul a fost detectat cu succes în ambele cazuri, cu rezultate mai bune pentru metoda propusă [Naf07b]. Al treilea detector are o performanţă mai bună.

Tab. 5.13. Rezistenţa la decupare, 32x32

Imagine vs. Răspunsul detectorului	***Metoda propusă***			***Metoda lui Barni***
	d1	***d2***	***d3***	
Barbara	0.36	0.44	1.48	1.29
Lena	0.85	1.06	1.87	1.85
Peppers	0.85	1.02	1.82	1.80
Boat	0.45	0.89	1.91	2.13
Baboon	0.87	0.98	1.90	1.61
F16	0.29	0.69	1.90	1.61
Goldhill	0.45	0.75	1.66	1.21
Houses	0.68	1.14	1.76	1.60
Lighthouse	0.54	1.06	2.32	0.83
Man	1.29	1.52	1.25	1.05
Elaine	0.51	0.95	1.57	1.52
Bridge	1.03	1.30	1.37	1.30



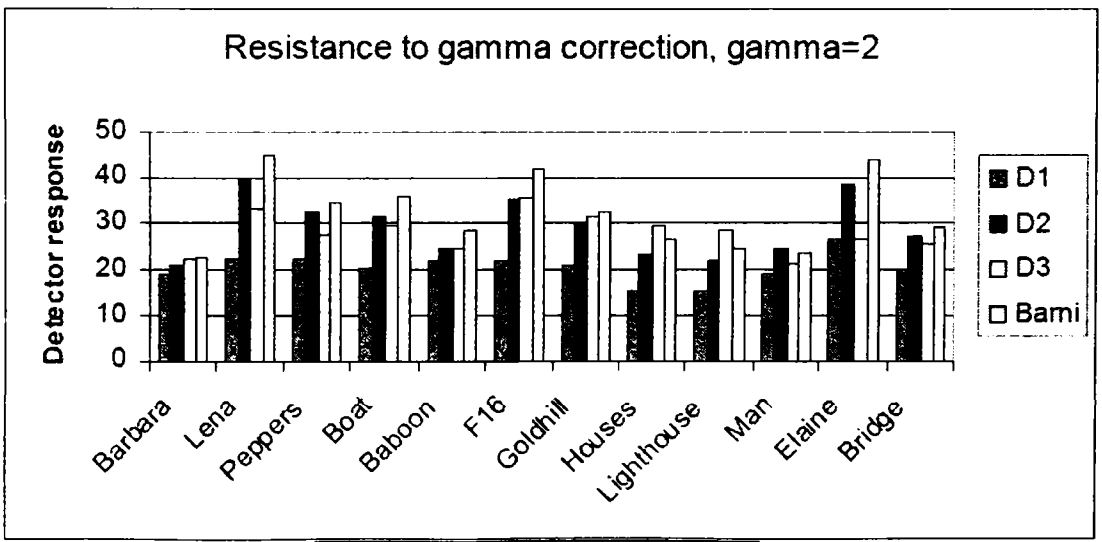
D1	D2	D3	Barni
0.68	**0.98**	**1.73**	**1.48**

Fig. 5.35: Raport corelaţie/prag, comparaţia robusteţii în cazul decupării, 32x32, împreună cu valorile medii pentru detectoare.

Marcajul inserat cu metoda propusă a fost detectat cu succes până la imaginea decupată de mărime 32x32, numai cu al treilea detector, care îi dovedeşte eficienţa. Metoda lui Barni detectează marcajul cu răspuns apropiat ca valoare ca şi al treilea detector.

Tab. 5.14. Resistenţa la corecţia de gamma, γ=2

Imagine vs. Răspunsul detectorului	***Metoda propusă***			***Metoda lui Barni***
	d1	***d2***	***d3***	
Barbara	18.72	20.57	22.11	22.67
Lena	22.41	39.62	32.97	44.81
Peppers	22.52	32.48	27.58	34.86
Boat	20.15	31.91	29.89	35.95
Baboon	21.76	24.92	24.67	28.80
F16	21.63	35.00	35.85	42.03
Goldhill	20.90	30.03	31.74	32.65
Houses	15.35	23.45	29.76	26.78
Lighthouse	15.37	21.65	28.47	24.81
Man	18.68	24.67	21.30	23.76
Elaine	26.77	38.83	26.70	44.00
Bridge	19.58	27.16	25.73	29.44



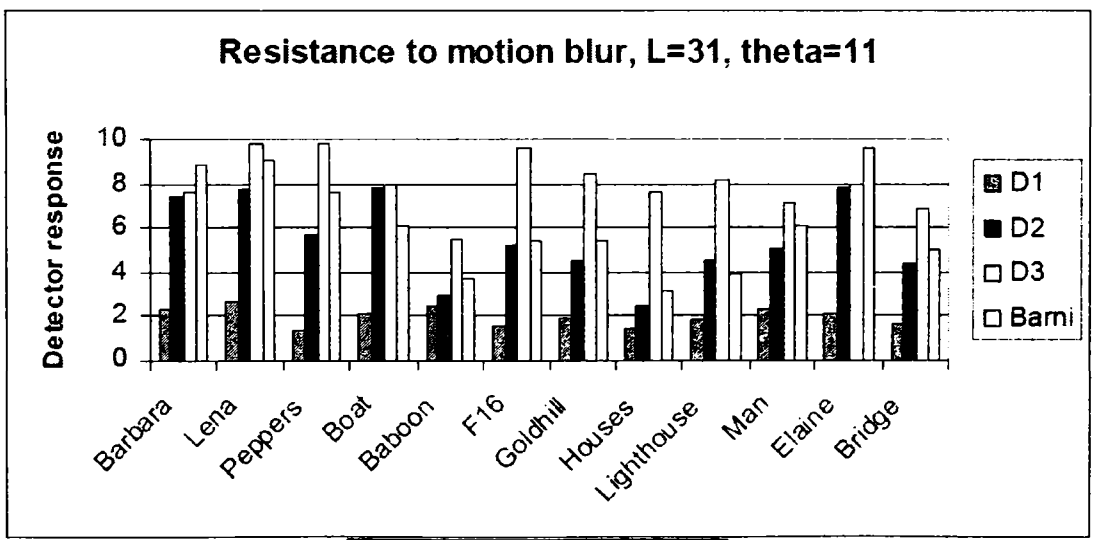
D1	D2	D3	Barni
20.32	**29.19**	**28.06**	**32.54**

Fig. 5.36: Raport corelaţie/prag, comparaţia robusteţii în cazul corecţiei de gamma, γ=2, împreună cu valorile medii pentru detectoare.

Aşa cum era de aşteptat pentru detectorul cu corelaţie normalizată, ambele metode sunt practic insensibile la corecţia de gamma [Cox05].

Tab. 5.15. Rezistenţa la blur de mişcare, L=31, θ=11

Imagine vs. Răspunsul detectorului	***Metoda propusă***			***Metoda lui Barni***
	d1	***d2***	***d3***	
Barbara	2.33	7.47	7.62	8.86
Lena	2.69	7.78	9.77	9.05
Peppers	1.35	5.74	9.80	7.62
Boat	2.12	7.83	7.94	6.14
Baboon	2.40	2.92	5.56	3.66
F16	1.56	5.23	9.62	5.42
Goldhill	1.95	4.52	8.46	5.37
Houses	1.45	2.48	7.70	3.17
Lighthouse	1.88	4.53	8.17	3.86
Man	2.37	5.07	7.11	6.11
Elaine	2.12	7.84	7.94	9.55
Bridge	1.61	4.36	6.82	4.97



D1	D2	D3	Barni
1.98	5.48	8.04	6.14

Fig. 5.37: Raport corelaţie/prag, comparaţia robusteţii în cazul blur, L=31, θ=11, împreună cu valorile medii pentru detectoare.

Pentru atacul de blur (înceţoşare) de mişcare, ambele metode au detectat cu succes marcajul. Al treilea detector are rezultate uşor mai bune decât celelalte.

Pentru primul detector, am estimat probabilitatea de fals pozitiv căutând multe marcaje diferite într-o imagine marcată, Lena. Fiecare prag $T_{\rho 1}$ a fost calculat astfel încât P_{fp} să aibă o anumită valoare. Procedeul a fost repetat pentru valori ale lui P_{fp} începând de la 10^{-1} până la 10^{-4}. In total am testat $5x10^4$ marcaje per imagine. Estimarea a fost făcută înainte de orice tip de manipulare şi după compresia JPEG, cu factor de calitate 10.

Valoarea estimată a probabilităţii de fals pozitiv, P_{fp} este prezentată în figura 5.38 în funcţie de raportul $T_{\rho 1} / \sigma_{\rho 1B}$ dintre pragurile de detecţie şi deviaţia standard a corelaţiilor din cazul B, corespunzătoare unui anumite valori teoretice a probabilităţii de fals pozitiv.

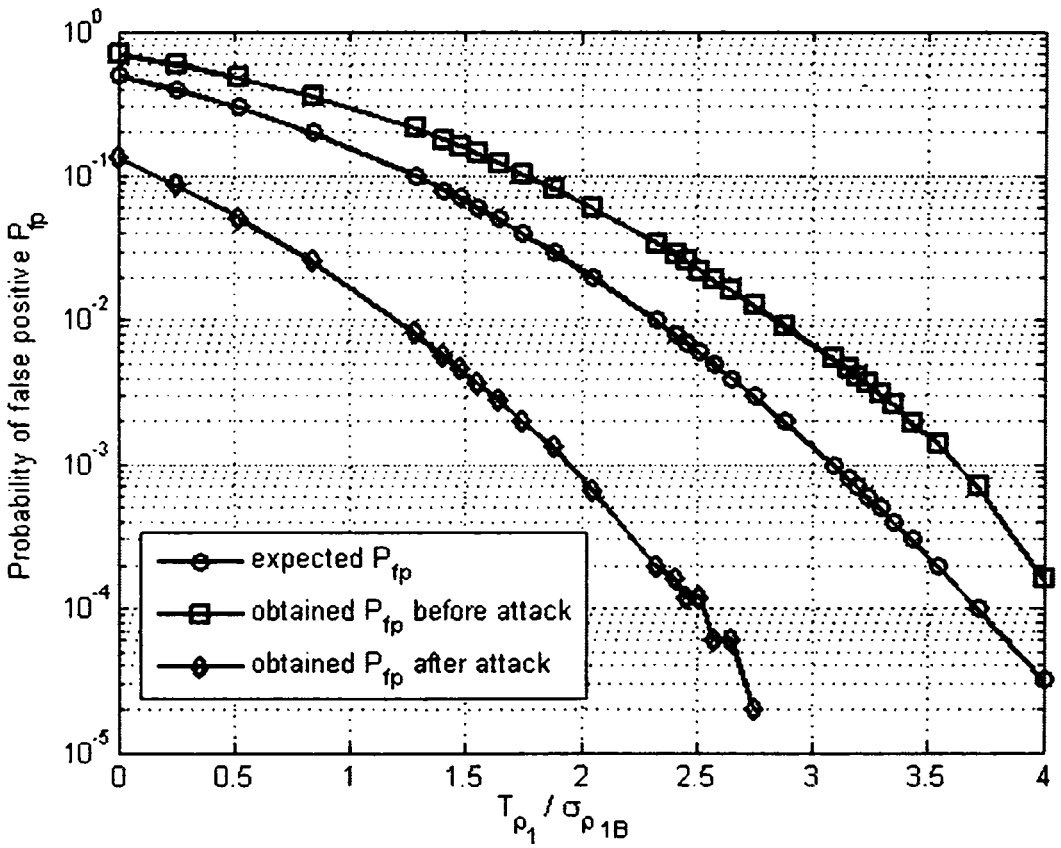


Fig. 5.38: Probabilitatea de fals pozitiv în funcţie de raportul $T_{\rho 1} / \sigma_{\rho 1B}$ dintre pragurile de detecţie şi deviaţia standard a corelaţiilor din cazul B (un alt marcaj este inserat în imagine). Valoarea teoretică este trasată cu simbolul „o". Testele au fost efectuate pe imaginea Lena, înainte şi după compresia JPEG cu factor de calitate 10, precum şi $5x10^4$ marcaje diferite.

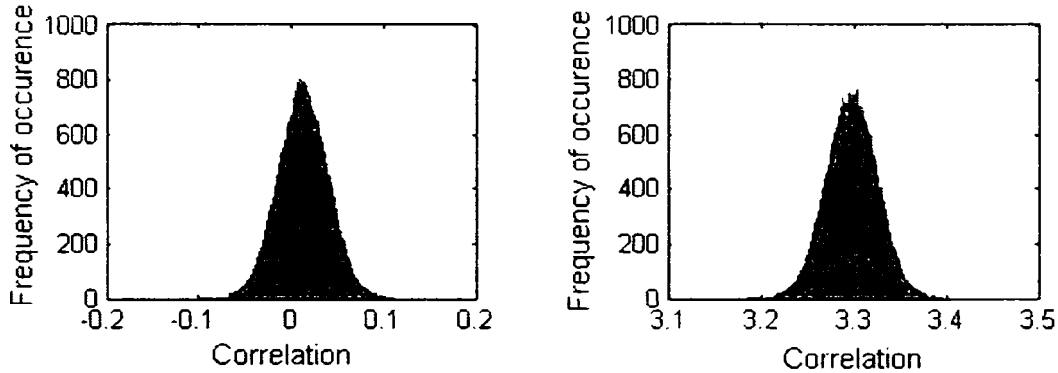


Fig. 5.39: Histogramele pentru corelaţiile din cazul B (un alt marcaj este inserat în imagine), şi cazul C (marcajul căutat este inserat în imagine), pentru imaginea Lena, înainte de atac. Au fost testate $5x10^4$ marcaje diferite.

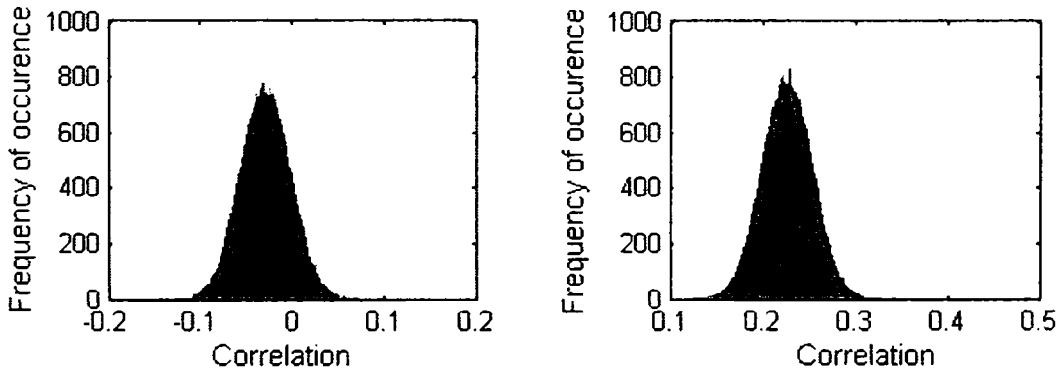


Fig. 5.40: Histogramele pentru corelaţiile din cazul B (un alt marcaj este inserat în imagine), şi cazul C (marcajul căutat este inserat în imagine), pentru imaginea Lena, după atacul prin compresie JPEG, factor de calitate 10. Au fost testate $5x10^4$ marcaje diferite.

Surprinzător, valoarea estimată a acestei probabilităţi P_{fp}, este mai mică după compresie decât înainte de orice atac pentru acelaşi prag de detecţie. Acest lucru poate fi explicat prin faptul că înainte de compresie, distribuţia empirică a corelaţiilor în cazul B (un alt marcaj este inserat în imagine), nu este gaussiană. Deşi cele două distribuţii sunt mai apropiate după atac, sunt foarte bine separate şi distribuţia empirică pentru un marcaj incorect are media sub zero, comparativ cu cazul anterior, unde era centrată pe zero (fig. 5.39 şi 5.40). Astfel pentru un prag fix, aceasta duce într-adevăr la o probabilitate de fals pozitiv mai mică după atac. Rezultate similare au fost obţinute pentru imaginea Barbara, la acelaşi atac.

Pentru primul detector, probabilitatea de fals pozitiv este apropiată de cea teoretică. Presupunerea anterioră, aceea că coeficienţii wavelet de la diverse niveluri şi subbenzi sunt variabile aleatoare statistic independente şi distribuite identic este rezonabilă şi deci detectorul va avea performanţe bune.

Concluzie. Am propus înserarea marcajului în toate nivelele de rezoluţie a imaginii; acest lucru poate fi util spre exemplu în cazul ştergerii tuturor subbenzilor

de frecvenţă înaltă care conţin marcajul în sistemul propus de Barni ş.a.[BBP01]. Detectorul neliniar cu prag fix ca raport între corelaţie şi pragul dependent de imagine este din nou folosit. Propunem şi evaluăm performanţele a trei detectoare a marcajului 1) din toate nivelele de rezoluţie, 2) separat din fiecare nivel, considerând maximul răspunsurilor de pe nivele, şi 3) separat din fiecare subbandă, considerând maximul răspunsurilor de pe subbenzi. Aceasta a fost avantajos pentru atacuri precum decupare, redimensionare şi filtrare mediană unde al treilea detector a arătat o performanţă mai bună. Am testat metoda la diverse atacuri, şi am arătat că este mai bună decât cea prezentată în [BBP01]. Comportarea metodei [Naf07b] poate fi explicată prin faptul că am folosit un estimat mai bun al măştii perceptuale, şi am folosit diversitatea transformării wavelet.

5.9 Concluzii

Am prezentat un tip nou de mascare perceptuală, construită pornind de la o metodă propusă de Barni ş.a. [BBP01]. Aceasta ascunde datele în toţi coeficienţii wavelet de detaliu, folosind o intensitate de marcare variabilă, conform unei măşti perceptuale.

Deşi tehnica propusă în [BBP01] este una performantă, îmbunătăţiri ale ei au fost propuse de mine în [NIB06a, NIB06b] exploatând superior caracteristicile sistemul vizual uman.

Într-o primă fază, tehnica din [NIB06a] estimează textura folosind o rezoluţie mai bună. Noul tip de mască perceptuală reuşeşte să ascundă datele mai bine, datorită estimării mai precise a texturii. Imaginea de textură este calculată folosind deviaţia standard locală a imaginii. Compresia wavelet a fost folosită pentru a obţine imaginea de textură de aceeaşi mărime ca şi marcajul.

O extensie a acestei metode este prezentată în [NIB06b]. În cadrul ei, marcajul se poate ascunde imperceptibil şi în subbenzile de frecvenţă mai joasă.

Acest lucru aduce un nivel crescut de robusteţe. Imaginea de luminanţă este şi ea estimată folosind o rezoluţie mai bună, pe imaginea de aproximare de frecvenţă mai înaltă. De asemenea sensibilitatea la zgomot este mărită. Această mască perceptuală permite inserarea imperceptibilă a datelor şi în nivele de rezoluţie scăzută, cum ar fi nivelul 1.

Imaginile marcate folosind masca propusă în [NIB06a, NIB06b] au fost testate la compresia JPEG. Rezultatele obţinute sunt de interes practic, în special datorită faptului că marcajul poate fi inserat în frecvenţe joase, de aici crescând şi robusteţea sistemului de marcare.

Am argumentat că nu ar trebui testată robusteţea unei metode, atâta timp cât criteriul (criteriile) de invizibilitate nu sunt satisfăcute [Naf07a]. Ca şi constrângere de invizibilitate, am folosit raportul maximal semnal-pe-zgomot, precum şi modelul de mascare spaţială din [Gir89]. Au fost testate două măşti perceptuale pe un număr mare de imagini, respectiv cele prezentate anterior, [BBP01] şi [NIB06a]. Intensitatea de marcare a fost fixată astfel încât procentajul de pixeli degradaţi din imaginea marcată să nu depăşească în medie 25%, iar valorile PSNR au fost în jur de 35 dB. Acestea ne asigură că imaginile nu au fost vizibil afectate de procesul de marcare.

Cele două seturi de imagini marcate au fost supuse la diferite tipuri de atacuri (compresie JPEG, filtrare mediană, redimensionare, decupare şi corecţie gamma).

Rezultatele simulării au arătat că impunând constrângerea de invizibilitate bazată pe modelul lui Girod [Gir89], cele două metode au fost comparabile şi au

detectat cu succes marcajul numai în cazul atacurile uşoare. Aceste rezultate au fost prezentate în [Naf07a].

În [Naf07b], am propus înserarea marcajului în toate nivelele de rezoluţie ale imaginii; acest lucru poate fi util spre exemplu în cazul ştergerii tuturor subbenzilor de frecvenţă înaltă care conţin marcajul în sistemul propus de Barni şi alţii [BBP01]. Detectorul neliniar cu prag fix ca raport între corelaţie şi pragul dependent de imagine este din nou folosit. Propunem şi evaluăm performanţele a trei detectoare ale marcajului 1) din toate nivelele de rezoluţie, 2) separat din fiecare nivel, considerând maximul răspunsurilor de pe nivele, şi 3) separat din fiecare subbandă, considerând maximul răspunsurilor de pe subbenzi. Aceasta a fost avantajos pentru atacuri precum decupare, redimensionare şi filtrare mediană unde al treilea detector a arătat o performanţă mai bună. Am testat metoda la diverse atacuri, şi am arătat că este mai bună decât cea prezentată în [BBP01]. Comportarea metodei [Naf07b] poate fi explicată prin faptul că am folosit un estimat mai bun al măştii perceptuale, şi am folosit diversitatea transformării wavelet. Trebuie menţionat că rezultatele metodei [BBP01] au fost rulate folosind codul sursă oferit de unul dintre autori, Alessandro Piva.

6. CONCLUZII ŞI CONTRIBUŢII PERSONALE

6.1 Concluzii

În **capitolul unu** am prezentat conceptele de bază ale marcării transparente şi aplicaţiile posibile. Am descris apoi etapele marcării: generarea marcajului, înglobarea şi detecţia marcajului. Proprietăţile metodelor de marcare au fost enumerate, precum şi condiţiile generale şi specifice impuse ei. Dezvoltarea unei tehnici de marcare ia în considerare mai multe aspecte, ce „împrumută" concepte din alte domenii de cercetare: steganografia, comunicaţiile cu spectru împrăştiat (Spread Spectrum - SS), modelele perceptuale umane, autentificarea şi criptarea, fuziunea datelor, transmisia semnalului în prezenţa fading-ului, estimarea canalului. Alegerea acestor elemente pentru o metodă de marcare, pentru o aplicaţie dată, este încă neclară, deoarece pentru anumite aplicaţii, trebuie făcut un compromis între imperceptibilitate, robusteţe şi complexitate. În continuare, am prezentat evaluarea performanţelor unei metode de marcare, folosind diverse criterii imperceptibilitatea, raportul dintre puterea maximă a semnalului şi puterea zgomotului PSNR, coeficientul de intercorelaţie, distanţa Hamming normalizată, probabilitatea unui fals pozitiv sau negativ, complexitatea de calcul. Am tratat problema marcării robuste şi soluţiile pentru asigurarea robusteţii.

Capitolul 2 începe cu o clasificare a tehnicilor de marcare, în funcţie de diferite criterii şi continuă cu stadiul actual al tehnicilor în funcţie de domeniul de marcare. Această a doua parte este mult mai vastă, tocmai din cauza multitudinilor abordărilor existente în literatură, care provin din domenii fundamentale ca prelucrarea semnalelor, teoria informaţiei, etc.

Astfel, cele mai multe scheme de marcare transparentă se bazează pe acelaşi principiu simplu, schimbarea redusă a valorii unor coeficienţi aleşi pseudoaleator în domeniul spaţial sau al unei transformate. Aceste schimbări sunt apoi identificate folosind un corelator sau alte tehnici asemănatoare corelaţiei. În mod normal, numărul de coeficienţi modificaţi este mult mai mare decât numărul de biţi de înserat. Aceasta poate fi considerată ca o marcare redundantă şi duce implicit la creşterea robusteţii.

Domeniul de înserare al marcajului poate influenţa semnificativ robusteţea marcajului. Metodele de marcare în domeniul spaţial sunt mai puţin robuste la atacuri de tip adăugare de zgomot, compresie JPEG. Dar marcajul poate fi recuperat uşor dacă imaginea a fost decupată sau translatată. Acest avantaj este mai puţin evident în frecvenţă. Decuparea în domeniul spaţial produce distorsiuni mari în domeniul spectral ceea ce duce de obicei la distrugerea marcajului. Acelaşi lucru este valabil şi pentru transformata DCT aplicată pe toată imaginea. Dacă sunt marcate blocuri DCT, pentru o detecţie cu succes este important să se cunoască poziţia blocurilor în care a fost înserat marcajul. Domeniul wavelet are dezavantaje asemănătoare, deoarece transformarea nu este invariantă la translaţie sau rotaţie. Cele mai multe metode plasează marcajul în domeniul spaţial, dar şi numărul metodelor în domeniul DCT este mare.

În **capitolul 3**, am făcut o prezentare a celor mai cunoscute atacuri asupra sistemelor de marcare transparentă, precum şi a soluţiilor posibile pentru diminuarea efectelor acestora. În analiza performanţelor tehnicilor de marcare transparentă, sunt folositoare benchmark-urile (Stirmark, UnZign, Certimark, etc). În paralel cu dezvoltarea tehnicilor de marcare transparentă, are loc şi dezvoltarea unor noi atacuri. Este probabilă o cooperare a criptografiei cu tehnici moderne de prelucrarea semnalelor, domenii legate de obstrucţionarea marcării transparente. Poate fi întrevăzută apariţia unor atacuri noi care să îmbine tehnici de steganaliză cu atacuri din marcare.

În **capitolul 4** am prezentat trei metode de marcare informată [NI03, NBK04, Naf04b, NB05, Naf05b, Naf05a, NIB05]. Acestea se bazează pe descompunerea multirezoluţie a imaginii cu transformata wavelet discretă. Se fac schimbări asupra unor coeficienţi wavelet, care nu vor avea un impact vizual asupra unui observator uman.

Coeficienţii au fost selectaţi folosind o detecţie cu logică de prag [NI03, NBK04, Naf04b, NB05, Naf05b]. Pragul depinde de coeficienţii wavelet ai fiecărei imagini de detaliu. Marcajul este înserat în texturi şi muchii ale imaginii folosind proprietăţile sistemului vizual uman.

Prima metodă [NI03] inserează marcajul în subbanda de detalii diagonale al primului nivel de rezoluţie, respectiv în toate subbenzile primului nivel; evident, deşi a doua abordare afectează mai mult imaginea, marcajul se dovedeşte a fi mai robust la prelucrări obişnuite de semnal (compresie JPEG, filtrare mediana, zgomot AWGN). Metoda este comparată cu cea din [KH98]. Coeficientul de intercorelaţie pentru metoda propusă este mai mare decât pentru metoda propusă în [KH98], în cazul compresiei JPEG şi zgomot alb Gaussian aditiv. Cu toate acestea, metoda propusă nu arată robusteţe împotriva filtrării mediane, comparativ cu metoda din [KH98].

A doua metodă inserează marcajul în cele trei nivele de rezoluţie, exceptând imaginea de aproximare, folosind acelaşi fel de selecţie a coeficienţilor wavelet. Detecţia se face din **(1)** toate nivele mediat, prin decizie majoritară, sau **(2)** din ultimul nivel de rezoluţie, mai puţin afectat de diverse prelucrări de semnal.

Un **set preliminar de experimente** [Naf04a] face o comparaţie a metodei cu metoda de tip cuantizare prezentată în [KH98], se dovedeşte că metoda este mai robustă. Se observă că performanţele metodei propuse [Naf04a] sunt superioare metodei din [KH98]. De asemenea, coeficientul de intercorelaţie este mai mare dacă extragerea marcajului se face numai din ultimul nivel de rezoluţie. Acest lucru se datoreşte faptului că distorsiunile obişnuite ale semnalului sunt mai semnificative pentru componentele spectrale mai înalte ale imaginii.

Un al doilea set de experimente a fost efectuat folosind patru imagini; s-a făcut o comparaţie a metodei propuse [Naf04b] cu cea de tip spread-spectrum prezentată în [CKLS97]. Aparent metoda lui Cox şi alţii este superioară în cazul atacului AWGN, comparabilă cu detectorul NC2 pentru compresia JPEG, şi inferioară pentru filtrarea mediană. Cu toate acestea, aceste teste au fost efectuate pentru imagini marcate puternic în cazul metodei [CKLS97].

Al treilea set de experimente [NB05] ia în considerare acest aspect, selectând intensitatea de marcare mai mică astfel încât imaginile să nu fie vizibil afectate de procesul de marcare pentru metoda din [CKLS97]. Imaginea Peppers este marcată cu diverse intensităţi şi apoi prelucrată cu diverse atacuri, compresie cu pierderi (JPEG şi JPEG2000), zgomot AWGN, redimensionare, filtrare mediană, ajustarea contrastului şi decupare. Metoda propusă funcţionează mai bine decât cea a lui Cox, pentru toate atacurile, cu mici excepţii, când, oricum, marca nu este detectabilă în ambele cazuri (de exemplu, pentru, α=0.1 şi β=0.01 la ajustarea contrastului). De fapt, rezultatele pentru metoda lui Cox sunt mult mai slabe şi nu detectează marca în prezenţa celor mai multe atacuri (compresie JPEG cu rata de compresie mai mare decât 10; decupare; redimensionare; filtrare mediană; ajustarea contrastului; compresie JPEG2000 cu rata de compresie mai mare de 10). Detectorul 2 are performanţe mai bune în cazul compresiei cu pierderi, filtrare mediană, rescalare, în timp ce detectorul 1 are rezultate mai bune pentru atacul AWGN.

În cazul decupării, cele două tipuri de detectoare au aceleaşi rezultate. În cazul ajustării contrastului, marcajul este detectat de ambele detectoare numai pentru α=0.3.

Răspunsurile detectoarelor, obţinute pentru imaginile comprimate cu JPEG2000, sunt mult mai mari decât cele obţinute pentru imaginile comprimate cu JPEG, evidenţiindu-se astfel robusteţea marcajului inserat în domeniul DWT.

Cu cât este mai mare intensitatea de marcare α, cu atât sunt mai bune performanţele metodei [NB05]. Cu toate acestea există un *compromis între robusteţe şi invizibilitate*, pe baza căruia intensitatea de inserare ar trebui limitată la valoarea α=0.2.

Pentru a doua metodă, s-au analizat **trei tipuri de detectoare** [NB05, Naf05b], care pot da rezultate diferite în funcţie de atacul la care a fost supusă imaginea:

- 1. din toate nivelele de rezoluţie, prin mediere, respectiv,
- 2. din ultimul nivel de rezoluţie al transformatei, care poate fi afectat mai puţin de distorsiuni obişnuite ale semnalului,
- 3. prin **corelaţie maximă** cu marcajul căutat [Naf05b].

Este evident că al treilea detector este mai bun decât primele două, deoarece estimarea marcajului se face în funcţie de marcajul original care este posibil inserat în imagine. Cu alte cuvinte, marcajul rezultat este cel mai asemănător cu cel original.

A treia metodă propune o **abordare statistică** [NIB05], unde se selectează *mai puţini coeficienţi wavelet* în care se înserează marcajul, deci numărul de repetiţii este mai mic, faţă de metoda 2. Răspunsul detectorului este mai bun faţă de metoda a doua, deoarece coeficienţii mari nu sunt atât de afectaţi de atacurile obişnuite (compresie, filtrare, etc.). Selecţia pragurilor este bazată pe proprietăţile statistice ale coeficienţilor wavelet. Aceleaşi detectoare sunt folosite ca şi mai înainte.

Se observă că detectorul 2 are rezultate mai bune pentru compresia cu pierderi, filtrare mediană, redimensionare şi ajustarea contrastului, în timp ce detectorul 1 are rezultate mai bune la atacul AWGN şi la compresia JPEG2000.

Detectorul 3 are performanţe mai bune decât detectorul 1, în cazul majorităţii atacurilor, şi performanţe comparabile cu detectorul 2, sau chiar mai bune în cazul filtrării, redimensionării, decupării, şi a ajustării contrastului. Pentru

atacul de coliziune, cu medierea a patru imagini marcate cu marcaje diferite, în cazul detectoarelor 1 şi 2, toate cele patru marcaje sunt detectate.

Performanţele metodelor propuse [NI03, NBK04, Naf04b, NB05, Naf05b, Naf05a, NIB05] au fost comparate cu cele ale metodei propuse de Cox şi alţii în [CKLS97] respectiv cu metoda propusă de Kundur şi Hatzinakos [KH98]. Metoda a demonstrat o performanţă mai bună în cazul tuturor atacurilor, în special din cauza utilizării transformatei DWT şi a analizei statistice a coeficienţilor wavelet.

În **capitolul cinci**, am prezentat un tip nou de mascare perceptuală, pornind de la o metodă propusă de Barni ş.a.[BBP01]. Aceasta ascunde datele în toţi coeficienţii wavelet de detaliu, folosind o intensitate de marcare variabilă, conform unei măşti perceptuale.

Deşi tehnica propusă de aceştia este performantă, îmbunătăţiri ale ei au fost propuse în [NIB06a, NIB06b] care ţin seama mai bine de sistemul vizual uman. Într-o primă fază, tehnica din [NIB06a] estimează textura folosind o rezoluţie mai bună.

Noul tip de mască perceptuală reuşeşte să ascundă datele mai bine, datorită estimării mai precise a texturii. Imaginea de textură este calculată folosind deviaţia standard locală a imaginii. Compresia wavelet a fost folosită pentru a obţine imaginea de textură de aceeaşi mărime ca şi marcajul. În continuare am prezentat o extensie a acestei metode [NIB06b], prin care marcajul se poate ascunde imperceptibil şi în subbenzile de frecvenţă mai joasă.
Acest lucru aduce un nivel crescut de robusteţe. Imaginea de luminanţă este şi ea estimată folosind o rezoluţie mai bună, pe imaginea de aproximare de frecvenţă mai înaltă. De asemenea sensibilitatea la zgomot este mărită. Această mască perceptuală permite inserarea imperceptibilă a datelor şi în nivele de rezoluţie scăzută, cum ar fi nivelul 1.

Imaginile marcate folosind masca propusă în [NIB06a, NIB06b] au fost testate la compresia JPEG. Rezultatele obţinute sunt de interes practic, în special datorită faptului că marcajul poate fi inserat în frecvenţe joase, de aici crescând şi robusteţea sistemului de marcare.

Am argumentat că nu ar trebui testată robusteţea unei metode, atâta timp cât criteriul (criteriile) de invizibilitate nu sunt satisfăcute [Naf07a]. Ca şi constrângere de invizibilitate, am folosit raportul maximal semnal-pe-zgomot, precum şi modelul de mascare spaţială din [Gir89]. Două măşti perceptuale au fost testate pe un număr mare de imagini, respectiv cele prezentate anterior, [BBP01] şi [NIB06a]. Intensitatea de marcare a fost fixată astfel încât procentajul de pixeli degradaţi din imaginea marcată să nu depăşească în medie 25%, iar valorile PSNR au fost în jur de 35 dB. Aceasta a indicat că imaginile nu au vizibil afectate de procesul de marcare.

Cele două seturi de imagini marcate au fost supuse la diferite tipuri de atacuri (compresie JPEG, filtrare mediană, redimensionare, decupare şi corecţie gamma).

Rezultatele simulării au arătat că impunerea constrângerii de invizibilitate bazate pe modelul lui Girod [Gir89], cele doua metode au fost comparabile şi au detectat cu succes marcajul numai în cazul atacurile uşoare. Aceste rezultate au fost prezentate în [Naf07a].

În [Naf07b], am propus înserarea marcajului în toate nivelele de rezoluţie a imaginii; acest lucru poate fi util spre exemplu în cazul ştergerii tuturor subbenzilor de frecvenţă înaltă care conţin marcajul în sistemul propus de Barni şi alţii [BBP01]. Detectorul neliniar cu prag fix ca raport între corelaţie şi pragul dependent de

imagine este din nou folosit. Propunem şi evaluăm performanţele a trei detectoare a marcajului

1) din toate nivelele de rezoluţie,

2) separat din fiecare nivel, considerând maximul răspunsurilor de pe nivele, şi

3) separat din fiecare subbandă, considerând maximul răspunsurilor de pe subbenzi.

Aceasta a fost avantajos pentru atacuri precum decupare, redimensionare şi filtrare mediană unde al treilea detector a arătat o performanţă mai bună. Am testat metoda la diverse atacuri, şi am arătăt că este mai bună decât cea prezentată în [BBP01]. Comportarea metodei [Naf07b] poate fi explicată prin faptul că am folosit un estimat mai bun al măştii perceptuale, şi am folosit diversitatea transformării wavelet.

6.2 Contribuţii personale

1. O primă contribuţie personală este legată de clasificarea şi aprecierea critică a metodelor de marcare transparentă şi a atacurilor şi este prezentată în capitolele doi şi trei. Marea diversitate a materialelor publicate în literatura de specialitate, numărul foarte mare de metode de marcare şi atac raportate în literatură au făcut analiza deosebit de dificilă. Ea se întinde pe 70 de pagini şi volumul ei este justificat de afirmaţiile precedente. Am organizat în aşa fel capitolele doi şi trei încât, în varianta electronică a tezei, cititorul poate consulta fiecare titlu bibliografic citat, pentru a-şi face o părere proprie despre cele scrise de mine. Consider că trebuie depuse în continuare eforturi, pentru "a face ordine" printre multitudinea de metode de marcare şi atac care provin din teoria semnalelor, teoria informaţiei, criptare, ş.a.

O concluzie personală, rezultată în urma analizei efectuate este faptul că marcarea în domeniul transformatei wavelet este o cale promiţătoare mai ales dacă îmbracă o forma adaptivă. Acesta este motivul pentru care în activitatea mea în domeniu am investigat mai ales o astfel de cale.

În capitolele 4 şi 5 am prezentat aproape exclusiv contribuţiile mele personale, pe care le pot numi originale. Acestea îşi propun să răspundă la câteva întrebări de interes practic pentru domeniu, cum ar fi:

(A) Unde este de preferat să se însereze marcajul (în domeniul spaţial sau în domeniul unei transformate) pentru a obţine o marcare cât mai robustă ? ;

(B) În care dintre nivelurile de descompunere ale DWT este mai bine să se însereze marcajul (în toate, în cele de rezoluţie inferioară sau în cele de rezoluţie superioară) pentru a obţine o marcare cât mai robustă ? ;

(C) În care dintre subbenzile DWT este mai bine să se însereze marcajul pentru a obţine o marcare cât mai robustă ?;

(D) Ce arhitectură de detector asigură cea mai bună extragere a marcajului? ;

(E) Cum să se facă marcarea perceptuală ?

Aceste contribuţii sunt prezentate în continuare dintr-o perspectivă istorică, care coincide în general şi cu creşterea robusteţii înserării marcajului. Ele se bazează pe simularea metodelor corespunzătoare în Matlab şi pe compararea rezultatelor obţinute astfel cu cele ale celor mai bune metode raportate în literatură.

2. *Oferă răspunsuri pentru întrebările (B), (C).* Am elaborat o primă metodă de marcare informată (capitolul 4) prezentată în [NI03] care inserează marcajul în subbanda de detalii diagonale al primului nivel de rezoluţie, respectiv în toate subbenzile primului nivel; evident, deşi a doua abordare afectează mai mult imaginea, marcajul se dovedeşte a fi mai robust la prelucrări obişnuite de semnal (compresie JPEG, filtrare mediană, zgomot AWGN). Metoda este comparată cu cea din [KH98]. Coeficientul de intercorelaţie pentru metoda propusă de mine este mai mare decât pentru metoda propusă în [KH98], în cazul atacului de tip compresie JPEG şi de tip zgomot alb gaussian aditiv. Cu toate acestea, metoda propusă de mine nu prezintă robusteţe împotriva filtrării mediane, comparativ cu metoda din [KH98].

3. *Oferă răspunsuri la întrebările (A), (B), (C), (D).* Am elaborat o a doua metoda de marcare informată (capitolul 4) care inserează marcajul în cele trei nivele de rezoluţie, exceptând imaginea de aproximare, folosind acelaşi fel de selecţie a coeficienţilor wavelet. Detecţia se face din (1) toate nivele prin decizie majoritară, sau (2) din ultimul nivel de rezoluţie, mai puţin afectat de diverse prelucrări de semnal.

3a. *Oferă răspunsuri la întrebările (B), (C) şi (D).* Un set de experimente [Naf04a] face o comparaţie a metodei propuse de mine, cu metoda de tip cuantizare prezentată în [KH98], se dovedeşte că metoda mea este mai robustă. Se observă că, în general, performanţele metodei propuse [Naf04a] sunt superioare metodei din [KH98]. De asemenea, coeficientul de intercorelaţie este mai mare dacă extragerea marcajului se face numai din ultimul nivel de rezoluţie. Acest lucru se datorează faptului că distorsiunile obişnuite ale semnalului sunt mai semnificative pentru componentele spectrale mai înalte ale imaginii.

3b. *Oferă răspunsuri la întrebarea (A).* Un al doilea set de experimente a fost efectuat folosind patru imagini; s-a făcut o comparaţie a metodei propuse de mine [Naf04b] cu cea de tip spread-spectrum prezentată în [CKLS97]. Aparent metoda lui Cox şi alţii este superioară în cazul atacului AWGN, comparabilă cu detectorul meu NC2 pentru compresia JPEG, şi inferioară pentru filtrarea mediană. Dar aceste teste au fost efectuate în cazul metodei [CKLS97] pe imagini marcate puternic.

3c. *Oferă răspunsuri la întrebările (A), (B), (C) şi (D).* Al treilea set de experimente [NB05] ia în considerare acest aspect, selectând intensitatea de marcare mai redusă, astfel încât imaginile să nu fie vizibil afectate de procesul de marcare pentru metoda din [CKLS97]. Imaginea Peppers este marcată cu diverse intensităţi şi apoi prelucrată cu diverse atacuri, compresie cu pierderi (JPEG şi JPEG2000), zgomot AWGN, redimensionare, filtrare mediană, ajustarea contrastului şi decupare. Metoda propusă de mine funcţionează mai bine decât cea a lui Cox, pentru toate atacurile, cu mici excepţii, când, oricum, marca nu este detectabilă în ambele cazuri (de exemplu, pentru $\alpha=0.1$ şi $\beta=0.01$ la ajustarea contrastului). De fapt, rezultatele pentru metoda lui Cox sunt mult mai slabe şi nu detectează marca în prezenţa celor mai multe atacuri (compresie JPEG cu rata de compresie mai mare decât 10; decupare; redimensionare; filtrare mediană; ajustarea contrastului; compresie JPEG2000 cu rata de compresie mai mare de 10). Detectorul 2 are performanţe mai bune în cazul compresiei cu pierderi, filtrare mediană, rescalare, în timp ce detectorul 1 are rezultate mai bune pentru atacul AWGN.

În cazul decupării, cele două tipuri de detectoare au aceleaşi rezultate. În cazul ajustării contrastului, marcajul este detectat de ambele detectoare numai pentru α=0.3.

Răspunsurile detectoarelor, obţinute pentru imaginile comprimate cu JPEG2000, sunt mult mai mari decât cele obţinute pentru imaginile comprimate cu JPEG, evidenţiindu-se astfel robusteţea marcajului inserat în domeniul DWT.

Cu cât este mai mare intensitatea de marcare α, cu atât sunt mai bune performanţele metodei mele [NB05]. Cu toate acestea există un *compromis între robusteţe şi invizibilitate*, pe baza căruia intensitatea de înserare ar trebui limitată la valoarea α=0.2.

4. *Răspunde la întrebările (A) şi (D).* Pentru detecţia marcajului la metoda a doua (capitolul 4) am analizat trei tipuri de detectoare, dintre care al treilea este original [NB05, Naf05b]. Aceste detectoare dau rezultate diferite în funcţie de atacul la care a fost supusă imaginea. Ele decid în funcţie de informaţia:

- 1. din toate nivelurile de rezoluţie, prin mediere,
- 2. din ultimul nivel de rezoluţie al transformatei, care poate fi afectat mai puţin de distorsiunile obişnuite ale semnalului,
- 3. obţinută prin corelaţia maximă cu marcajul căutat [Naf05b]. Acest detector este original.

Este evident că al treilea detector este îmbunătăţit faţă de primele două, deoarece estimarea marcajului se face în funcţie de marcajul original care este posibil înserat în imagine. Cu alte cuvinte, marcajul rezultat este cel mai asemănător cu cel original.

5. *Răspunde la întrebările (B), (C), (D) şi (E).* În [NIB05], (capitolul 4), am propus o abordare statistică în cadrul căreia se selectează *mai puţini coeficienţi* wavelet în care se înserează marcajul, deci numărul de repetiţii este mai mic, dar răspunsul detectorului este mai bun în al doilea caz, deoarece coeficienţii mari nu sunt atât de afectaţi de atacurile obişnuite (compresie, filtrare, etc.). Selecţia pragurilor este bazată pe proprietăţile statistice ale coeficienţilor wavelet. Se folosesc aceleaşi detectoare menţionate la contribuţia anterioară.

Se observă că detectorul 2 are rezultate mai bune pentru compresia cu pierderi, filtrare mediană, redimensionare şi ajustarea contrastului, în timp ce detectorul 1 are rezultate mai bune la atacul AWGN şi la compresia JPEG2000.

Detectorul 3 are performanţe mai bune decât detectorul 1, în cazul majorităţii atacurilor, şi performanţe comparabile cu detectorul 2, sau chiar mai bune în cazul filtrării, redimensionării, decupării, şi a ajustării contrastului. Pentru atacul de coliziune, cu medierea a patru imagini marcate cu marcaje diferite, în cazul detectoarelor 1 şi 2, sunt detectate toate cele 4 marcaje.

Performanţele metodelor propuse [NI03, NBK04, Naf04b, NB05, Naf05b, Naf05a, NIB05] au fost comparate cu cele ale metodei propuse de Cox şi alţii în [CKLS97], respectiv cu metoda propusă de Kundur şi Hatzinakos [KH98]. Metoda mea a demonstrat o performanţă mai bună în cazul tuturor atacurilor, în special din cauza utilizării transformatei DWT şi a analizei statistice a coeficienţilor wavelet.

6. *Răspunde la întrebările (B), (C), (D) şi (E).* Am prezentat (capitolul 5), un tip nou de mascare perceptuală, pornind de la o metodă propusă de Barni şi alţii [BBP01]. Aceasta ascunde datele în toţi coeficienţii wavelet de detaliu, folosind o intensitate de marcare variabilă, conform unei măşti perceptuale.

Deşi tehnica propusă de aceştia este performantă, au fost propuse de mine îmbunătăţiri ale ei în [NIB06a, NIB06b] ţinând seama mai bine de caracteristicile sistemului vizual uman. Într-o primă fază, tehnica din [NIB06a] estimează textura folosind o rezoluţie mai bună.

Noul tip de mască perceptuală reuşeşte să ascundă datele mai bine, datorită estimării mai precise a texturii. Imaginea de textură este calculată folosind deviaţia standard locală a imaginii. În acest sens metoda este una adaptivă. Compresia wavelet a fost folosită pentru a obţine imaginea de textură de aceeaşi mărime ca şi marcajul.

7. *Răspunde la întrebările (B), (C), (D) şi (E).* O extensie a acestei metode (capitolul 5), este cea din [NIB06] în care marcajul se poate ascunde imperceptibil şi în subbenzile de joasă frecvenţă. Acest lucru aduce un nivel crescut de robusteţe. Imaginea de luminanţă este şi ea estimată folosind o rezoluţie mai bună, pe imaginea de aproximare de frecvenţă mai înaltă. De asemenea sensibilitatea la zgomot este mărită. Această mască perceptuală permite inserarea imperceptibilă a datelor şi în nivele de rezoluţie scăzută, cum ar fi nivelul 1.

Imaginile marcate folosind masca propusă de mine în [NIB06a, NIB06b] au fost testate la compresia JPEG. Rezultatele obţinute sunt de interes practic, în special datorită faptului că marcajul poate fi înserat în frecvenţele joase, crescând astfel şi robusteţea sistemului de marcare.

Lucrarea citată, [NIB06b] a fost publicată în Springer-Verlag. Ca urmare a recunoaşterii faptului că am adus o contribuţie în domeniu, am fost nominalizată ca recenzor la *IEEE Transaction on Information Forensics and Security*, la *IEEE Transaction on Multimedia*, precum şi la *EURASIP Journal on Information Security*.

8. *Răspunde la întrebările (B), (C), (D) şi (E).* Am argumentat (capitolul 5), că nu ar trebui testată robusteţea unei metode, atâta timp cât nu sunt satisfăcute criteriile de invizibilitate. Ca şi constrângere de invizibilitate, am folosit raportul maxim semnal-pe-zgomot, precum şi modelul de mascare spaţială din [Gir89]. Au fost testate pe un număr mare de imagini două măşti perceptuale, respectiv cele prezentate anterior, [BBP01] şi [NIB06a]. Intensitatea de marcare a fost fixată astfel încât procentajul de pixeli degradaţi din imaginea marcată să nu depăşească în medie 25%, iar valorile PSNR au fost în jur de 35 dB. Astfel am asigurat ca imaginile să nu fie vizibil afectate de procesul de marcare.

Cele două seturi de imagini marcate au fost supuse la diferite tipuri de atacuri (compresie JPEG, filtrare mediană, redimensionare, decupare şi corecţie gamma).

Rezultatele simulării au arătat că impunând constrângerea de invizibilitate bazată pe modelul lui Girod [Gir89], cele două metode dau rezultate comparabile şi au detectat cu succes marcajul numai în cazul atacurile uşoare. Aceste rezultate au fost prezentate în [Naf07a].

9. *Răspunde la întrebările (B), (C), (D) şi (E).* În [Naf07b], (capitolul 5), am propus înserarea marcajului în toate nivelele de rezoluţie ale imaginii; acest lucru poate fi util spre exemplu în cazul ştergerii tuturor subbenzilor de frecvenţă înaltă care conţin marcajul în sistemul propus de Barni şi alţii [BBP01]. Este din nou folosit detectorul neliniar cu prag fix, ca raport între corelaţie şi pragul dependent de imagine. Am propus şi evaluat performanţele a trei detectoare ale marcajului: 1) din toate nivelele de rezoluţie, 2) separat din fiecare nivel, considerând maximul răspunsurilor de pe nivele, şi 3) separat din fiecare subbandă, considerând maximul

răspunsurilor de pe subbenzi. Aceste detectoare au fost avantajoase pentru atacuri precum decupare, redimensionare şi filtrare mediană unde al treilea detector a arătat o performanţă mai bună. Am testat metoda la diverse atacuri, şi am arătat că este mai bună decât cea prezentată în [BBP01]. Comportarea metodei [Naf07b] poate fi explicată prin faptul că am folosit un estimat mai bun al măştii perceptuale şi am folosit diversitatea transformării wavelet. Rezultatele celor trei detectoare pot fi fuzionate ameliorîndu-se în continuare procesul de extragere a marcajului.

Lucrarea citată, [Naf07b] a fost apreciată. Ea compară rezultatele mele cu cele ale echipei Barni, Bartolini şi Piva şi arăt în ea că rezultatele mele sunt superioare. În consecinţă această metodă reprezintă rezultatul final al tezei de doctorat. O recunoaştere indirectă a venit chiar de la Mauro Barni, la recomandarea căruia am devenit recenzor şi la *Institution of Engineering and Technology Information Security, IET IFS*.

Lucrarea [NBK04] a fost citată de către Bao Zheng, Zhang Jian-wei, Xia De-Shen, Dong Bing, Gao Shang-bin, în lucrarea *Image adaptive Watermarking Algorithm based on Zero Tree Structure of Wavelet Transform*, în Computer Engineering and Applications, 2006, Vol. 42, No. 32,p.72-76, Wanfang Data, China.

Dizertaţia mea de master, *Filigranage dans le domaine des ondelettes*, din 2004, [Naf04e] a fost citată în Proceedings of World Academy of Science, Engineering and Technology, vol. 17, Dec. 2006, ISSN 1307-6884, în lucrarea *A Watermarking System Using the Wavelet Technique for Satellite Images*, I. R. Farah, I. B. Ismail, M. B. Ahmed.

Lucrarea [Naf05b] a fost citată în Springer Verlag de către Xue-Quan Xu, Xian-Bin Wen, Yue-Qing Li, Jin-Juan Quan, în lucrarea *A New Watermarking Approach Based on Neural Network in Wavelet Domain*, Advanced Intelligent Computing Theories and Applications with Aspects of Artificial Intelligence, 2007, LNCS.

Mai amintesc că raportul meu "Studiul comportării la atacuri a imaginilor marcate transparent" a fost citat de revista care apare la adresa www.resursejuridice.ro care a dat şi link-ul către acesta în octombrie 2007, mai precis http://www.resursejuridice.ro/content/view/714/77/.

PUBLICAŢII PROPRII

*2007

[Naf07a] **C. Nafornita,** "Robustness Evaluation of Perceptual Watermarks", IEEE Int. Symposium on Signal, Circuits and Systems ISSCS 2007, 12-13 July 2007, Iasi, Romania.

[Naf07b] **C. Nafornita**, "A New Pixel-Wise Mask for Watermarking", Proc. of ACM Multimedia and Security Workshop 2007, Dallas, TX, USA.

[Naf07c] **C. Nafornita**, "Atacuri asupra imaginilor marcate transparent", Politehnica Publishing House, 2007, ISBN 978-973-625-414-7, 130 pag.

[ANBI07a] I. Adam, **C. Nafornita**, J.M. Boucher, A. Isar, "A New Implementation of the Hyperanalytic Wavelet Transform", IEEE Int. Symposium on Signal, Circuits and Systems ISSCS 2007, 12-13 July 2007, Iasi, Romania, in press.

[ANBI07b] I. Adam, **C. Nafornita**, J.M. Boucher, A. Isar, "A Bayesian Approach of Hyperanalytic Denoising", IEEE Int. Symposium on Intelligent Signal Processing WISP 2007, 3-5 Oct. 2007, Madrid, Spain.

*2006

[NIB06a] **C. Nafornita**, A. Isar, M. Borda, "Pixel-wise masking for watermarking using local standard deviation and wavelet compression", Scientific Bulletin of Politehnica Univ. of Timisoara, Trans. on Electronics and Communications, tom 51(65), fasc.2, pp. 146-151, ISSN 1583-3380.

[NIB06b] **C. Nafornita**, A. Isar, M. Borda, "Improved Pixel-Wise Masking for Image Watermarking", in Multimedia Content Representation, Classification and Security, September 11-13, 2006, Istanbul, Turkey, Lecture Notes in Computer Science, Springer-Verlag, 2006, pp. 90-97.

[Naf06] **C. Nafornita**, "Cresterea securitatii retelelor de comunicatii de date prin autentificare bazata pe watermarking", Research report for CNCSIS grant, type TD, code 47 no. 2930/2006.

[IMNO06] A. Isar, S. Moga, **C. Nafornita**, M. Oltean, I. Adam, "Image Denoising Using Wavelet Transforms With Enhanced Diversity", Proc. International Conference Communications 2006, Bucharest, June, 3-4, 2006, ISBN(10) 973-718-496-3, ISBN(13) 978-973-718-496-2, pp.161-164.

*2005

[Naf05a] **C. Nafornita,** "Digital Watermarking in the Wavelet Domain", Politehnica Publishing House, ISBN 973-625-236-1. 2005

[Naf05b] **C. Nafornita**, "Improved Detection for Robust Image Watermarking", Proc. of International Symposium on Signal, Circuits and Systems, ISSCS2005, Iasi, Romania, 14-15 July 2005, vol. 2, pp.473-476.

[Naf05c] **C. Nafornita**, "Stadiul actual al tehnicilor de marcare transparentă a imaginilor", Research report for CNCSIS grant, type TD, code 47 no. 34702/24.06.05

[Naf05d] **C. Nafornita**, "Studiul comportarii la atacuri a imaginilor marcate transparent", (Image Watermarking Attacks) Research Report for CNCSIS Grant, Type TD, Code 47, No. 34702/24.06.05.

[NB05] **C. Nafornita**, M. Borda, "Multiple Embedding in Wavelet Subbands for Robust Image Watermarking", Proc. of International Workshop on Spectral Methods and Multirate Signal Processing, SMMSP 2005, 200-22 June, Riga, Latvia.

[NIB05] **C. Nafornita**, A. Isar, M. Borda, "Image Watermarking Based on the Discrete Wavelet Transform Statistical Characteristics", IEEE EUROCON 2005 - The International Conference on "Computer as a Tool", Nov. 21-24, 2005, Belgrade, Serbia & Montenegro.

*2004

[NBK04] **C. Nafornita**, M. Borda, A. Kane, "A Wavelet-Based Digital Watermarking using Subband Adaptive Thresholding for Still Images", microCAD 2004, Miskolc, Hungary, 18 – 19 March 2004, pp. 87 - 92.

[Naf04a] **C. Nafornita**, "Balizarea Imaginilor Statice Folosind Transformata Wavelet Discreta", Raport de Cercetare din Cadrul Grantului CNCSIS, de tip D, cod 47, numar 33385/29.06.04.

[Naf04b] **C. Nafornita**, "A Wavelet-Based Watermarking for Still Images", Buletinul Ştiinţific al UPT tom 49(63) Electronică şi Telecomunicaţii, fascicola 2, 2004, pp. 126-131.

[Naf04c] **C. Nafornita**, "Watermarking in the wavelet domain", Research report for CNCSIS grant, type TD, code 47 no. 33385/29.06.04.

[Naf04d] **C. Nafornita**, "Algoritmi robusti de marcare transparenta a imaginilor cu turbocoduri", Research report for CNCSIS grant, type TD, code 47 no. 33385/29.06.04.

[Naf04e] **Nafornita Corina.** "Filigranage dans le domaine des ondelettes". Mémoire de diplôme pour obtenir le degré de M.Sc. Université Politechnica Timisora, Faculté d'Electronique et Télécommunication. TIMISOARA-2004.

*2003

[NI03] **C. Nafornita**, A. Isar, "Digital Watermarking of Still Images Using the Discrete Wavelet Transform," Scientific Bulletin of Politehnica University of Timisoara, Electronics and Telecommunications Trans., Tom 48(62), Fascicola 1, 2003, pp. 73-78.

BIBLIOGRAFIE

[AGP02] N. Abdulaziz, A. Glass, K.K.Pang, "Embedding Data in Images Using Turbo-Coding", 6th Symposium on DSP for Communication Systems, 28-31 Jan. 2002, Univ. Of Wollongong, Australia.

[AM03] F. Arnia, K. Munadi, "Improving Invisibility in DCT Domain Watermarking System Using Wavelet Based Image Fusion", Proc. of IECI Japan Workshop 2003, ISSN 1344-7491.

[AM05] C. Adsumilli, S. K. Mitra, "Error Concealment in Video Communications Using DPCM Bit Stream Embedding", ICASSP 2005.

[AP00] N.K.Abdulaziz, K.K. Pang, "Robust Data Hiding for Images", Proc. IEEE Communication Technology, ICCT 2000.

[AP98] R. J. Anderson and F. Petitcolas, "On the limits of steganography," IEEE J. Select. Areas Commun. (Special Issue on Copyright and Privacy Protection), vol. 16, pp. 474–481, May 1998.

[ASS02] I. Avcibas, B. Sankur, K. Sayood, "Statistical evaluation of image quality measures", Journal of Electronic Imaging / April 2002 / Vol. 11(2).

[AWS01] A. Ambroze, G. Wade, C. Serdean, M. Tomlinson, Y. Stander, M. Borda, "Turbo Code Protection of Video Watermark Channel", IEE Proceedings Vision Image, *Signal Processing*, Vol. 148, No. 1, Feb. 2001, pp. 54-58.

[BA99] A.P.Bradley, "A Wavelet Visible Difference Predictor", IEEE, Trans. On Image Processing, Vol.8, No.5, May 1999.

[Bar03a] M.Barni et al., "What is the Future for Watermarking? (Part I)", IEEE Signal Processing Magazine, Sept. 2003, pp. 55-60.

[Bar03b] M.Barni et al., "What is the Future for Watermarking? (Part II)", IEEE Signal Processing Magazine, Nov. 2003, pp. 53-57.

[BB01] T. Băjenescu, M. Borda, "Securitatea în Informatică şi Telecomunicaţii", editura Dacia, Cluj-Napoca, 2001.

[BBC03] P. Bas, N. Le Bihan, J.-M. Chassery, "Color Image Watermarking Using Quaternion Fourier Transform", ICASSP 2003, April 2003, pp.III - 521-4, vol.3.

[BBCL99] M. Barni, F. Bartolini, V.Capellini , A. Lippi, A. Piva, "A DWT-based Technique for Spatio-Frequency Masking of Digital Signatures", Security and Watermarking of Multimedia Contents, SPIE, Vol. 3657, pp. 31-39, San Jose, California, 23-29 Jan. 1999.

[BBCP98a] M Barni, F. Bartolini, V. Cappelini and A. Piva, "A DCT Domain System for Robust Image Watermarking", Signal Processing (Special Issue on Watermarking), vol. 66, no.3, 1998.

[BBCP98b] F. Bartolini, M. Barni, V. Cappellini, and A. Piva, "Mask Building for Perceptually Hiding Frequency Embedded Watermarks," Proc. 5th IEEE Int. Conf. Image Processing ICIP'98, vol. I, Chicago, IL, Oct. 4-7, 1998, pp. 450-454.

[BBCP98c] M. Barni, F. Bartolini, V. Cappellini, A. Piva, and F. Rigacci, "A M.A.P. identification criterion for DCT-based watermarking," in Proc. Europ. Signal Processing Conf. (EUSIPCO '98), Rhodes, Greece, Sept. 1998.

[BBGH00] W. Bender, W. Butera, D. Gruhl, R. Hwang, F.J. Paiz, S. Pogreb, "Applications for Data Hiding", IBM Systems Journal, 39, 3&4, 2000, pp. 547-568.

[BBP01] M. Barni, F. Bartolini, A.Piva; "Improved Wavelet-Based Watermarking through Pixel-Wise Masking," IEEE Transactions on Image Processing, Volume 10, Issue 5, May 2001, pp.783 - 791.

[BBPS02] M. Barni, F. Bartolini, A.Piva, F. Salucco, "Robust Watermarking for Cartographic Images", EURASIP Journal on Applied Signal Processing, 2002:2, pp.197-208.

[BCD98] P. Bas, J.-M. Chassery, F. Davoine, "Using fractal code to watermark images," in Proc. Int. Conf. Image Processing (ICIP), vol. 1, Chicago, IL, 1998.

[BCHL05] Poza Bill Clinton & Hillary, înlocuită cu Monica Levinsky, în varianta falsificată, autor C.-Y. Lin (originalul a apărut în ziarul Newsweek).

[BGM95] W. Bender, D. Gruhl, and N. Morimoto, "Techniques for Data Hiding", Proc. SPIE, Storage and Retrieval for Image and Video Databases III, vol. 2420, San Jose, CA, Feb. 9-10, 1995, pp. 165-173.

[BGML96] W. Bender, D. Gruhl, and N. Morimoto, A. Lu, "Techniques for Data Hiding", IBM Systems Journal, 35, 3&4, 1996, pp. 313-336.

[BKZ98] Burgett, S.; Koch, E.; Zhao, J., "Copyright labeling of digitized image data", IEEE Communications Magazine, Vol. 36, Issue 3, March 1998, pp. 94 - 100.

[BMM96] G.W. Braudaway, K.A. Magerlein, F. Mintzer, "Protecting publicly available images with a visible watermark," Proc. SPIE - Int. Soc.Opt. Eng., vol. 2659, pp.126 - 133, 1996.

[BMM96b] G. W. Braudaway, K. A. Magerlein, and F. C. Mintzer, "Color correct digital watermarking of images," U.S. Patent 5 530 759, June 1996.

[BMYY97] D. Benham, N. Memon, B.-L. Yeo, and M. Yeung, "Fast watermarking of DCT-based compressed images," in Proc. Int. Conf. Image Science, Systems, and Technology (CISST '97), Las Vegas, NV, June 1997, pp. 243–253

[BN04] M.Borda, I. Nafornita, "Digital Watermarking - Principles and Applications", Proc. of Int. Conf. Communications 2004, Bucharest, pp.41-54.

[BP96a] A. Bors and I. Pitas, "Embedding parametric digital signatures in images," in EUSIPCO-96, Trieste, Italy, Sept. 1996.

[BP96b] A.G. Bors, I. Pitas, "Image Watermarking Using DCT Domain Constraints", International Conference on Image Processing, ICIP 96.

[BP98] A.G. Bors, I. Pitas, "Image Watermarking Using Block Site Selection and DCT Domain Constraints", Optics Express, Vol. 3, No. 12, pp. 512-522, Dec. 1998

[BPGS01] F. Balado, F. Pérez-González, and S. Scalise, "Turbo Coding for Sample-Level Watermarking in the DCT Domain", Proc. of the IEEE Int. Conf. on Image Processing (ICIP), pp. 1003-1006, Thessaloniki, Greece, Oct. 2001.

[BQM95] O. Bruyndonckx, J.-J. Quisquater, B. Macq, "Spatial method for copyright labeling of digital images", Proc. IEEE Nonlinear Signal Processing Workshop, 1995, pp.456-459

[Bra97] G.W. Braudaway, "Protecting Publicly-Available Images with an Invisible Watermark," in Proc. ICIP 97, IEEE Int. Conf. on Image Processing, Santa Barbara, CA, Oct. 1997, pp. 524-531.

[BRD95] F. Boland, J. O'Ruanaidh, C. Dautzenberg, "Watermarking digital images for copyright protection", Proc. of IEE Int. Conf. on Image Proc. and Its Applications, Edinburgh, 1995

[BS95] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," in Advances in Cryptology—Proc. CRYPTO '95 (Lecture Notes in Computer Science), vol. 963, Don Coppersmith, Ed. Berlin, Germany: Springer, 1995, pp. 452–465

[BS98] Boneh, Dan and James Shaw, "Collusion-Secure Fingerprinting for Digital Data", IEEE Trans. on Information Theory, vol. 44, no. 5, pp. 1897-1905, Sept. 1998.

[BTS05] A. Briassouli, P. Tsakalides, A. Stouraitis, "Hidden Messages in Heavy-Tails: DCT-Domain Watermark Detection Using Alpha-Stable Models", IEEE Trans. on Multimedia, Vol. 7, No. 4, August 2005, pp.700-715.

[Car95] G. Caronni, "Assuring ownership rights for digital images," in Proc. VIS 95, Session "Reliable IT Systems," Vieweg, Germany, 1995.

[CB01] D. Coltman, A.G. Bors, "Hierarchical Watermarking Depending on Local Constraints", IEEE, Int. Conf. on Image Processing, Thessaloniki, Greece,7-10, Oct. 2001.

[CBD98] J.-M. Chassery, P. Bas, and F. Davoine, "Self-similarity based image watermarking," in Proc. Europ. Signal Processing Conf.(EUSIPCO '98), Rhodes, Greece, Sept. 1998

[Cha02] D.V.S. Chandra, "Digital Image Watermarking Using Singular Value Decomposition," Proc. of 45th IEEE Midwest Symposium on Circuits and Systems, Tulsa, OK, August 2002, pp. 264-267.

[Cha03] D.V.S. Chandra, On Block-based Image Watermarking, Proceeding (399) Signal and Image Processing – 2003.

[CHOS98] T.-Y. Chung, M.-S. Hong, Y.-N. Oh, D.-H. Shin, S.-H. Park, "Digital Watermarking for Copyright Protection of MPEG2 Compressed Video", IEEE, 1998, pp.895-901.

[CKLS95] I.J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", NEC Res. Instit., Princeton, NJ, Tech. Rep. 95-10, 1995.

[CKLS96] I.J. Cox, J. Killian, T. Leighton and T. Shamoon, "Secure Spread Spectrum Watermarking for Images, Audio and Video", Proc. of ICIP, vol. 3, pp.243-246, 1996.

[CKLS97] I. Cox, J. Killian, T. Leighton, T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", IEEE Trans. on Image Processing, Vol.6, No.12, pp.1673-1687, 1997.

[CKN04] P. Campisi, D. Kundur, A.Neri, "Robust Digital Watermarking in the Ridgelet Domain", IEEE, Signal Processing Letters, Vol. 11, No. 10, Oct. 2004, pp. 826-830.

[CL02] A. Cohen, A. Lapidoth, "The Gaussian Watermarking Game", IEEE Trans. on Information Theory, Vol.48, No.6, 2002, pp. 1639-1667.

[CL97] I. Cox, J.-P. M.G. Linnartz, "Public watermarks and Resistance to Tampering", Proc. IEEE, Int. Conf. on Image Processing, 1997.

[CM02] I. Cox, M. Miller, "The first 50 years of electronic watermarking", Journal of Applied Signal Processing, 2002, 2, 126-132, 2002.

[CM03] R. Chandramouli, N. Memon, "On Sequential Watermark Detection", Special Issue on Signal Processing for Data Hiding in Digital Media and Secure Content Delivery, IEEE Trans. on Signal Processing, 2003.

[CM97] I. Cox, M. Miller, "A Review of Watermarking and the Importance of Perceptual Modeling", Proc. SPIE Human Vision and Elect. Imaging II, vol. SPIE, vol. 3016, Feb. 1997.

[CM98] J.J. Chae, B.S. Manjunath, "A Robust Embedded Data from Wavelet Coefficients", Proceedings of the SPIE EI'98, vol. 3312, pp.308-317, San Jose, Feb. 1998.

[CMB02] I. Cox, M. Miller, J. Bloom, "Digital Watermarking", Morgan Kaufmann Publishers, 2002.

[CMM98] J. J. Chae, D. Mukherjee, and B. S. Manjunath, "A robust data hiding technique using multidimensional lattices," Proc. Forum on Advances in Digital Libraries, Santa Barbara, California, pp. 319-26, 1998.

[CMM99] I.J.Cox, M.L.Miller, A.L.MCKellips, "Watermarking as Communications with Side Information", Proc. of IEEE, vol. 87, No. 7, July 1999, pp. 1127-1141

[CMYY98] S. Craver, N. Memon, B. Yeo, M. Yeung, "Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks, and Implications", IEEE Journal On Selected Areas In Communications, Vol. 16, No. 4, May 1998.

[Cos83] M. Costa, "Writing on Dirty-Paper" (Corresp.), IEEE Trans. on Information Theory, vol.29, no.3, May 1983, pp. 439- 441.

[Cox05] I. Cox, "Robust Watermarking", ECRYPT Summer School on Multimedia Security, Salzburg, Austria, Sept. 22, 2005.

[CPR01] J.Chou, S.S.Pradhan, K.Ramchandran, "Turbo Coded Trellis Based Constructions for Data Embedding: Channel Coding with Side Information", In Proc. of Asilomar Conf. on Signals, Systems and Computers, Pacific Grove (USA), Oct. 2001

[CW01a] B. Chen, G. W. Wornell, "Quantization Index Modulation Methods for Digital Watermarking and Information Embedding of Multimedia", Journal of VLSI Signal Processing 27, 7-33, 2001.

[CW01b] B. Chen, G. W. Wornell, "Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding", IEEE Trans. on Information Theory, Vol. 47, No. 4, May 2001.

[CW98] B. Chen and G. W. Wornell, "Digital Watermarking and Information Embedding Using Dither Modulation", IEEE Second Workshop on Multimedia Signal Processing, pp. 273–278, 1998.

[CW99] B. Chen, G. W. Wornell, "Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding", 1999, ISIT: Proceedings IEEE Int. Symposium on Information Theory.

[DCP00] F. Deguillaume, G. Csurka and T. Pun, "Countermeasures for Unintentional and Intentional Video Watermarking Attacks", SPIE Electronic Imaging, San Jose, CA, January 2000.

[Del04] E. Delp, "Multimedia security: the 22nd century approach", invited talk at ACM Multimedia and Security Workshop 2004, Magdeburg, Germany, Sept.20-21, 2004.

[DH76] W. Diffie, M. Hellman, "New Directions in Cryptography", IEEE Trans. On Information Theory, vol. IT-22, No.6, November 1976.

[Dir01] European Parliament, "Directive on the harmonisation of certain aspects of copyright and related rights in the information society", http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001L0029:EN:HTML, http://europa.eu/scadplus/leg/en/lvb/l26021.htm, 2001/29/EC, 22 May 2001

[Dir04] European Parliament, "The Directive on the enforcement of intellectual and industrial property rights such as copyright and related rights, trademarks, designs or patents", http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_157/l_15720040430en00450086.pdf, 2004/48/EC, April 2004

[DKL98] G. Depovere, T. Kalker, and J.-P. Linnartz, "Improved Watermark Detection Using Filtering Before Correlation", Proc. 5th IEEE Int. Conf. Image Processing ICIP'98, vol. I, Chicago, IL, Oct. 4-7, 1998, pp. 430-434.

[DMCA98] U.S. Copyright Office Summary, "The Digital Millennium Copyright Act of 1998," December 1998: http://lcweb.loc.gov/copyright/legislation/dmca.pdf

[DRA98] R. Dugad, K. Ratakonda and N. Ahuja, "A New Wavelet-Based Scheme for Watermarking Images", ICIP 1998.

[DS96] P. Davern and M. Scott, "Fractal based image steganography," in Lecture Notes in Computer Science: Information Hiding, vol.1174. Berlin, Germany: Springer, 1996, pp. 279–294.

[EBTG02] J.J. Eggers, R. Bäuml, R. Tzschoppe and B. Girod, "Scalar Costa Scheme for Information Embedding", IEEE Transactions on Signal Processing, Special Issue on Signal Processing for Data Hiding in Digital Media and Secure Content Delivery, Vol. 51, No. 4, p. 1003-1019, 2002.

[EKK99] F. Ergun, J. Killian, R. Kumar, "A Note on the Limits of Collusion-Resistant Watermarks", Eurocrypt'99, pp. 140-149, 1999.

[EM00] Ejima, M., Miyazaki, A., "A wavelet-based watermarking for digital images and video", Proc. IEEE Int. Conf. Image Processing, 2000.

[Fau93] O. Faugeras, "Three Dimensional Computer Vision: A Geometric Viewpoint", Cambridge, MA: MIT Press, 1993

[FG99] J. Fridrich, M. Goljan, "Comparing Robustness of Watermarking Techniques", Proc. of SPIE, Vol. 3657, Security and Watermarking of Multimedia Content, San Jose, California, Jan. 25-27, 1999, pp. 214-225.

[FH97] D.J. Fleet and D.J. Heeger, "Embedding Invisible Information in Color Images", Proc. ICIP 97, IEEE Int. Conf. Image Processing, Santa Barbara, CA, Oct. 1997.

[FKK01] C. Fei, D. Kundur, R. Kwong, "The Choice of Watermarking Domain in the Presence of Compression", Proc. IEEE Int. Conf. on Information Technology: Coding and Computing, pp. 79-84, Las Vegas, Nevada, April 2001.

[FKK04] C. Fei, D. Kundur, R. Kwong, "Analysis and Design of Watermarking Algorithms for Improved Resistance to Compression", IEEE Trans. on Image Processing, Vol. 13, No. 2, Feb. 2004, pp. 126 - 144.

[Fri99] J. Fridrich, "Key-Dependent Random Image Transform and Their applications in Image Watermarking", 1999 Int. Conf. on Imaging Science, Systems and Technology, CISST'99, Las Vegas, June 28-July 1, 1999, pp. 237-243.

[Fri99b] Matlab implementation of Girod's model http://www.ws.binghamton.edu/fridrich/masking.html

[FS00] V. Fotopoulos, A.N. Skodras, "A Subband DCT Approach to Image Watermarking", X European Signal Processing Conference, Tampere, Finland, Sept.4-8, 2000.

[GE04] E. Ganic, A. M. Eskicioglu, "Robust DWT-SVD Domain Image Watermarking: Embedding Data in All Frequencies", ACM MM&SEC'04, September 20–21, 2004, Magdeburg, Germany.

[Gir89] B. Girod, "The information theoretical significance of spatial and temporal masking in video signals", Proc. SPIE Human Vision, Visual Processing, and Digital Display, vol. 1077, pp. 178–187, 1989.

[GZE03] E. Ganic, N. Zubair, A.M. Eskicioglu, "An Optimal Watermarking Scheme Based on Singular Value Decomposition", Proc. of the IASTED International Conference on Communication, Network, and Information Security (CNIS 2003), pp. 85-90, Uniondale, NY, December 10-12, 2003.

[HAPG00] J.R. Hernández, M. Amado, F. Pérez-Gonzalez, "DCT-Domain Watermarking Techniques for Still Images: Detector Performance Analysis and a New Structure", IEEE Trans. on Image Processing, vol. 9, pp. 55-68, Jan. 2000.

[HF02] L. Hua, J.E. Fowler, "A Performance Analysis of Spread-Spectrum Watermarking Based on Redundant Transform", Proc. of IEEE Int. Conf. on Multimedia and Expo, Lausanne, Switzerland, Aug. 2002,Vol. 2, pp. 553-556.

[HG96] F. Hartung, B. Girod, "Digital Watermarking of Raw and Compressed Video", Proc. SPIE 2952: Digital Compression Technologies and Systems for Video Communications, Oct. 1996, pp. 205-213.

[HG97] F. Hartung, B. Girod, "Fast Public-Key Watermarking of Compressed Video", Int. Conf. on Image Processing ICIP'97, Oct. 1997, Santa Barbara, California.

[HG97b] F. Hartung, B. Girod, "Digital Watermarking of MPEG-2 Coded Video in the Bitstream Domain", Proc. ICASSP'97, Vol. 4, pp. 2621-2624.

[HG98] F. Hartung, B. Girod, "Watermarking of Uncompressed and Compressed Video", Signal Processing 66 (1998) 283 – 301.

[Hir96] K. Hirotsugu, "An image digital signature system with zkip for the graph isomorphism", Int.Conf. Image Processing, ICIP 1996, vol.3, pp.247-250.

[HK99] F. Hartung, M. Kutter, "Multimedia Watermarking Techniques", Proc. IEEE, 87, 7, 1999, pp. 1079-1106.

[HLR00] A. Hanjalic, G.C. Langelaar, P.M.B. van Roosmalen, J. Biemond, and R.L. Lagendijk, "Image and Video Databases: Restoration, Watermarking and Retrieval", Advances in Image Communications, vol. 8, New York: Elsevier Science, 2000.

[HPG99] J.R. Hernández, F. Pérez-Gonzalez, "Statistical Analysis of Watermarking Schemes for Copyright Protection of Images", Proceedings of the IEEE, 87(7):1142-1166, July 1999. Special Issue on Identification and Protection of Multimedia Information.

[HPGA98] J.R. Hernández, F. Pérez-Gonzalez, M. Amado, "DCT-Domain Image Watermarking and Generalized Gaussian Models", Proc. of the COST #254 Int. Workshop on Intelligent Communications and Multimedia Terminals, pp. 23-26, Ljubljana, Slovenia, November 1998.

[HPGR98] J. R. Hernandez, F. Perez-Gonzalez, J. M. Rodrıguez, and G.Nieto, "Performance analysis of a 2-d multipulse amplitude modulation scheme for data hiding and watermarking still images," IEEE J. Select. Areas Commun., vol. 16, pp. 510–524, 1998.

[HPRP98] A. Herrigel, H. Petersen, J. O Ruanaidh, T. Pun, and P. Shelby, "Copyright Techniques for Digital Images Based on Asymmetric Cryptographic Techniques", Workshop on Information Hiding, Portland, Oregon, USA, Apr. 1998.

[HRPP98] A. Herrigel, J.J.K. Ó Ruanaidh, H. Petersen, S. Pereira, and T. Pun, "Secure Copyright Protection Techniques for Digital Images", Information Hiding, Lecture Notes in Computer Science, vol. 1525, D. Aucsmith, Ed. Berlin, Germany: Springer, 1998, pp. 169-190.

[HSG99] F. Hartung, J.K. Su, B. Girod, "Spread Spectrum Watermarking: Malicious Attacks and Counterattacks", Proc. SPIE, 3657, Security and Watermarking of Multimedia Contents, Jan. 1999.

[HTC00] Shen-Fu Hsiao, Yor-Chin Tai, and Kai-Hsiang Chang, "VLSI Design of an Efficient Embedded Zerotree Wavelet Coder with Function of Digital Watermarking", IEEE Trans. Consumer Electronics, Vol. 46, No. 3, pp. 628-636, Aug. 2000.

[HW00] C. Hsu, J. Wu, "Image Watermarking by Wavelet Decomposition", Academy of Information and Management Sciences Journal, Vol. 3, No.1, pp. 70-86, 2000.

[HW96] C.-T. Hsu and J.-L. Wu, "Hidden Signatures in Images", Proc. ICIP-96, IEEE Int. Conf. Image Processing, vol. III, Lausanne, Switzerland, Sept. 16-19, 1996, pp. 223-226.

[ICN02] A. Isar, A. Cubitchi, M. Nafornita, "Algorithmes et techniques de compression" , ed. Orizonturi Universitare, Timisoara ,Romania, 2002, 181, 973-8391-38-5.

[IMK99] H. Inoue, A. Miyazaki, T. Katsura, "An image Watermarking Method Based on the Wavelet-Transform", Proc. of ICIP, vol. 3, pp. 296-300, 1999.

[IML05] A. Isar, S. Moga, X. Lurton, "A Statistical Analysis of the 2D Discrete Wavelet Transform", Proc. of the International Conference AMSDA 2005, May 17-20, 2005, Brest, France, pp. 1275-1281.

[IN98] A. Isar, I. Nafornita, "Reprezentari Timp – Frecventa", Editura Politehnica, Timisoara, 1998.

[Isa02] A. Isar, "Securitatea Transmiterii Informaţiei pe INTERNET", 2002.

[Jai81] A.K. Jain, "Image Data Compression: A Review", Proc. IEEE, vol. 69, pp. 349-389, Mar. 1981,

[JSSK02] S. Joo, Y. Suh, J. Shin, H. Kikuchi, "A New Robust Watermarking Embedding into Wavelet DC Components", ETRI Journal, 24-25 Oct., 2002, pp. 401-404.

[Kal01] T. Kalker, "Considerations on Watermarking Security", IEEE 4th Workshop on Multimedia Signal Processing, Cannes, France, 2001, pp.201-206.

[Kal05] T. Kalker, "Digital Rights Management", ECRYPT Summer School on Multimedia Security, Salzburg, Austria, Sept. 22, 2005.

[KAS05] P. Kumsawat, K. Attakitmongcol, A. Srikaew, "A New Approach for Optimization in Image Watermarking by Using Genetic Algorithms", IEEE Trans. Signal Processing, Vol. 53, No. 12, Dec. 2005, pp. 4707-4719.

[Kay93] Steven M. Kay, "Fundamentals of Statistical Signal Processing: Detection Theory", Prentice Hall, 1993.

[KD00] D. Kundur, "Water-Filling for Watermarking", Proc. IEEE Int. Conf. On Multimedia and Expo, New York, pp. 1287-1290, August 2000.

[KD00b] D. Kundur, "Implications for High Capacity Data Hiding in the Presence of Lossy Compression", Proc. IEEE Int. Conf. On Info. Tech.: Coding & Comp, 2000.

[KD05] D. Kundur, "Attacks Against Watermarking Schemes", (joint work with William Luh), ECRYPT Summer School on Multimedia Security, Salzburg, Austria, Sept. 23, 2005.

[KD05b] D. Kundur, "Authentication Watermarking", (joint work with Chuhong Fei and Raymond Kwong), ECRYPT Summer School on Multimedia Security, Salzburg, Austria, Sept. 22, 2005.

[KDHM99] T. Kalker, G. Depovere, J. Haitsma, and M. Maes, "A Video Watermarking System for Broadcast Monitoring", Proc. SPIE Electronic Imaging '99, Security and Watermarking of Multimedia Contents, San Jose, CA, Jan. 1999, pp. 103-112.

[Ker01] Andrew D. Ker, "An Idea for Blind Watermarking Scheme Resistant to Stirmark", Programming Research Group Technical Report RR-01-14, Oxford University Computing Laboratory, 2001.

[KH01] D. Kundur, D. Hatzinakos, "Diversity and Attack Characterization for Improved Robust Watermarking", IEEE Transactions on Signal Processing, Vol. 49, No. 10, 2001, pp. 2383-2396.

[KH97] D. Kundur, D. Hatzinakos, "A robust digital image watermarking method using wavelet-based fusion," In International Conference on Image Processing, pp. 544-547, Santa Barbara, California, USA, Oct. 1997.

[KH98] D. Kundur, D. Hatzinakos, "Digital Watermarking using Multiresolution Wavelet Decomposition", Proc. IEEE Int. Conf. On Acoustics, Speech and Signal Processing, Seattle, Washington, Vol. 5, pp. 2969-2972, May 1998.

[KH98b] D. Kundur, D. Hatzinakos, "Towards a Telltale Watermarking Technique for Tamper-Proofing", ICIP 1998.

[KH99] D. Kundur, D. Hatzinakos, "Digital Watermarking for Telltale Tamper Proofing and Authentication", Proc. IEEE, 87, 7, July 1999.

[KH99b] D. Kundur, D. Hatzinakos, "Mismatching perceptual models for effective watermarking in the presence of compression", Proc. SPIE, Multimedia Systems and Applications II, September 1999.

[KI01] S. Kay, E. Izquierdo, "Robust Content Based Image Watermarking", Proc. of Workshop on Image Analysis For Multimedia Interactive Services, WIAMIS 2001, Tampere, Finland, May 2001.

[KJB97] M. Kutter, F. Jordan, F. Bossen, "Digital Signature of Color Images Using Amplitude Modulation", Proc. SPIE Electronic Imaging '97, Storage and Retrieval for Image and Video Databases V, San Jose, CA, Feb. 1997, pp. 518-526.

[KJB98] M. Kutter, F. Jordan, F. Bossen, "Digital signature of color images using amplitude modulation," J. Electron. Imaging, vol. 7, no. 2, pp. 326–332, Apr. 1998

[KK04] D. Kundur, K. Kannan, "Video Fingerprinting and Encryption Principles for Digital Rights Management", Proceedings of the IEEE, Vol. 92, No. 6, June 2004, pp. 918-932.

[KKK02] B. S. Kim, K. K. Kwon, S. G. Kwon, K. N. Park, K. N. Park, K. I. Song, K. I. Lee, "A Robust Wavelet-Based Digital Watermarking Using Statistical Characteristic of Image and Human Visual System", Proc. of ITC-CSCC 2002, vol 2. pp. 1019-1022.

[KLD98] T. Kalker, J.P. Linnartz and M. van Dijk, "Watermark Estimation Through Detector Analysis", ICIP-98, October 1998.

[KM99] J.R. Kim and Y.S. Moon, "A Robust Wavelet-Based Digital Watermarking Using Level-Adaptive Thresholding", Proc. of IEEE ICIP, Vol. 2, Kobe, Japan, Oct. 1999, pp. 226-230.

[KMKM00] M. Kesal, M. K. Mihcak, R. Koetter, and P. Moulin, "Iteratively Decodable Codes for Watermarking Applications", Proc. 2nd Int. Symp. on Turbo Codes and Related Topics, Sept. 2000 , Brest, France

[KMY04] D. Kirovski, H. Malvar, Y. Yacobi, "A Dual Watermark-Fingerprint System", IEEE Multimedia, 2004, pp.59-73

[KP99] M. Kutter and F.A.P. Petitcolas, "A Fair Benchmark for Image Watermarking Systems", Proc. Electronic Imaging '99, Security and Watermarking of Multimedia Contents, vol 3657, San Jose, CA, Jan. 25-27, 1999, pp. 226-239.

[KRR98] M. S. Kankanhalli, Rajmohan, and K. R. Ramakrishnan, "Content-based watermarking of images," in Proc. ACM Multimedia '98, Bristol, U.K., Sept. 1998.

[KSLR99] S.W.Kim, S.Suthaharan, H.K. Lee, K.R.Rao, "Image Watermarking Scheme Using Visual Model and BN Distribution", Electronics Letters, 4th Feb. 1999, Vol. 35, N0. 3, pp. 212-214

[Kun99] D. Kundur, "Multiresolution Digital Watermarking: Algorithms and Implications for Multimedia Signals", Ph.D. Thesis, Dept. of Electrical & Computer Engineering, University of Toronto, August 1999.

[Kut98] M. Kutter, "Watermarking resisting to translation, rotation, and scaling," in Proc. SPIE Int. Symp. on Voice, Video, and Data Communication, Nov. 1998

[KZ95] E. Koch, J. Zhao, "Towards Robust and Hidden Image Copyright Labeling", Proc. of 1995 IEEE Workshop on Nonlinear Signal and Image Processing (Neos Marmaras, Greece, June 20-22, 1995).

[LC05] Q. Li, I. Cox, "Using Perceptual Models to Improve Fidelity and Provide Invariance to Valumetric Scaling For Quantization Index Modulation Watermarking", ICASSP 2005.

[LD98] P. Linnartz and M. van Dijk, "Analysis of the sensitivity attack against electronic watermarks in images", in Proceedings of the 2nd Workshop on Information Hiding, Portland OR, April 15–17, 1998.

[LD99] E.T. Lin, E.J. Delp, "A Review of Fragile Image Watermarks", Proc. of the Multimedia and Security Workshop (ACM Multimedia '99), Orlando, pp.25-29, 1999.

[LD99b] E. T. Lin and E. J. Delp, "A Review of Data Hiding in Digital Images," Proceedings of the Image Processing, Image Quality, Image Capture

Systems Conference (PICS '99), Savannah, GA, April 25-28, 1999, pp. 274-278.

[LHL03] W-N Lie, T-L Hsu, G-S Lin, "Verification of Image Content Integrity by Using Dual Watermarking on Wavelets Domain", ICIP'2003, pp. 487-490.

[LK00] P. Loo, N.G. Kingsbury, "Watermarking Using Complex Wavelets with Resistance to Geometric Distortion", The 10th European Signal Processing Conference (Eusipco2000), 5-8 Sept. 2000, Tampere, Finland.

[LK05] W. Luh, D. Kundur, "New Paradigms for Effective Multicasting and Fingerprinting of Entertainment Media", IEEE Communications Magazine, June 2005, Vol. 43, No. 6, pp.77-84.

[LK92] A.S. Lewis, G. Knowles, "Image Compression Using the 2-D Wavelett Transform", IEEE, Trans. on Image Processing, 1,2, April, 1992, pp. 244-250.

[LL01] G.C. Langelaar, R.L. Lagendijk, "Optimal Differential Energy Watermarking of DCT Encoded Images and Video", IEEE Trans. On Image Processing, 10, 1, Jan. 2001.

[LLL97] G.C. Langelaar, J.C.A. van der Lubbe, and R.L. Lagendijk, "Robust Labeling Methods for Copy Protection of Images", Proc. SPIE Electronic Imaging '97, Storage and Retrieval for Image and Video Databases V, San Jose, CA, Feb. 1997, pp. 298-309.

[LMT00] T.-H. Lan, M. F. Mansour, A. H. Tewfik, "Robust High Capacity Data Embedding", ICIP 2000, pp. 581-584

[LOBL99] C.H. Lee, H.S.Oh, Y. Baek, H.K. Lee, "Adaptive Digital Image Watermarking Using Variable Size of Blocks in Frequency Domain", 1999 IEEE TENCON, pp. 702-705.

[LR00] T. Liang and J. Rodriguez, "Improved Watermarking Robustness Via Spectrum Equalization", Proc. IEEE ICASSP 2000, Istanbul, Turkey, June 5-9, 2000.

[LSL00] G. C. Langelaar, I. Setyawan, and R. Lagendijk, "Watermarking Digital Image and Video Data: A State-of-the-Art Overview", IEEE Signal Processing Mag., vol. 17, no. 5, pp. 20–46, Sept. 2000.

[LSL04] D.C. Lou, C.H. Sung, "Robust Watermarking Scheme for Digital Images Using Significant Coefficients and the De-Correlating Principle", Journal of CCIT, 32,2, May 2004.

[LT02] R. Liu, T. Tan, "A SVD-Based Watermarking Scheme for Protecting Rightful Ownership", IEEE, Trans. On Multimedia, 4, 121-128, 2002

[LWBC01] C. Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, M. L. Miller, Y. M. Lui, "Rotation, Scale, and Translation Resilient Watermarking for Images", IEEE Trans. On Image Processing, 10, 5, May 2001.

[LYC00] C.-Y. Lin, "Watermarking and Digital Signature Techniques for Multimedia Authentication and Copyright Protection", Ph.D. Thesis, Columbia University, 2000.

[LYKM06] Z.Liu, H. Yu, D. Kundur, M. Merabdi, "On Peer-To-Peer Multimedia Content Acces and Distribution", Proc. IEEE International Conference on Multimedia and Expo, Toronto, Canada, July 2006.

[Mal99] S. Mallat, "A Wavelet Tour of Signal Processing", Academic Press, 1999.

[MB99] M.L. Miller, J.A. Bloom, "Computing the Probability of False Watermark Detection", Proc. of Workshop in Information Hiding, Dresden, Germany, Sept. 29-Oct.1, 1999.

[MBM02] P.Moulin, A. Briassouli, H. Malvar, "Detection-Theoretic Analysis of Desynchronization Attacks in Watermarking", Proc. DSP'02, Santorini, Greece, July 2002.

[MCB00] M.L. Miller, I.J. Cox, J.A. Bloom, "Informed Embedding: Exploiting Image and Detector Information during Watermark Insertion", Int. Conf. on Image Proc., ICIP, 2000.

[MCM98] D. Mukherjee, J.J. Chae, and S.K. Mitra, "A source and channel coding approach to data hiding with application in hiding speech in video", Proceedings of the IEEE International Conference on Image Processing, Chicago, IL, October 1998.

[MDC02] M.L. Miller, G.J. Doerr, I.J. Cox, "Dirty-Paper Trellis Codes for Watermarking", IEEE Int. Conf. on Image Processing, 2, pp. 129-132, 2002.

[MF03] H. Malvar, D. Florencio, "Improved Spread Spectrum: A New Modulation Technique for Robust Watermarking", IEEE Trans. on Signal Processing, Vol. 51, No. 4, April 2003, pp. 898-905.

[MI03] P. Moulin, A. Ivanovic, "The Zero Rate Spread-Spectrum Watermarking Game", IEEE Trans. on Signal Processing, Vol. 51, No. 4, pp. 1098-1117, April 2003.

[MK03] P. Moulin, R. Koetter, "Data Hiding–Theory and Algorithms", National University of Singapore, Institute for Mathematical Sciences, Tutorial lecture notes, Dec. 1, 2003.

[MK05] P. Moulin, R. Koetter, "Data Hiding Codes", (tutorial paper), Proceedings IEEE, Vol. 93, No. 12, pp. 2083-2127, Dec. 2005.

[MM04] P. Moulin, M.K.Mihcak, "The Parallel-Gaussian Watermarking Game", IEEE, Trans. On Inf. Theory, Vol.50, No. 2, Feb. 2004.

[MN05] N. Memon, "Multimedia Fingerprinting", ECRYPT Summer School on Multimedia Security, Salzburg, Austria, Sept. 24, 2005.

[MO98] M. J. J. J. B. Maes and C. W. A. M. Overveld, "Digital watermarking by geometric warping," in Proc. Int. Conf. Image Processing (ICIP), vol. 1, Chicago, IL, 1998

[MOS03] P. Moulin, J. O'Sullivan, "Information-Theoretic Analysis of Information Hiding", IEEE Trans. on Information Theory, 49, 3, March 2003, pp.563-593.

[MP03a] P.Moulin, "Embedded-Signal Design for Channel Parameter Estimation, Part I: Linear Filtering", Proc. IEEE Workshop on Statistical Signal Processing, St Louis, MO, Sep. 2003.

[MP03b] P.Moulin, "Embedded-Signal Design for Channel Parameter Estimation, Part II: Quantization Embeddeding", Proc. IEEE Workshop on Statistical Signal Processing, St Louis, MO, Sep. 2003.

[MQ95] B.M. Macq and J.-J. Quisquater, "Cryptology for digital TV broadcasting", Proc. IEEE, vol. 83, pp. 944-957, June 1995.

[MR00] A T. Murgan, R. Radescu, "Principiile teoriei codurilor. Algoritmi si aplicatii", Ed. Tehnica, Bucuresti, 2000.

[MS99] S. Mallat, "A Wavelet Tour of Signal Processing", Academic Press, 1999.

[MT94] K. Matsui and K. Tanaka, "Video-steganography: How to Secretly Embed a Signature in a Picture," in Proc. IMA Intellectual Property Project, vol. 1, Jan. 1994, pp. 187–206.

[MU01] P. Meerwald, A. Uhl, "A Survey of Wavelet-domain Watermarking Algorithms", Proc. SPIE, Electronic Imaging, Security and Watermarking of Multimedia Contents III, San Jose, CA, USA, January 22 - 26, 2001.

[MW01] N. Memon, P. W. Wong, "A Buyer-Seller Watermarking Protocol", IEEE Trans. on Image Processing, 10, 4, April 2001.

[MW04] Pierre Moulin, Ying Wang, "New Results on Steganographic Capacity", Proc. CISS Conference, Princeton, NJ, Mar. 2004.

[MW98] N. Memon and P.W. Wong, "Protecting Digital Media Content," Comm. ACM, Vol. 41, No. 7, July 1998, pp. 35—43.

[NCH99] K.S. Ng and L.M. Cheng, "Selective block assignment approach for robust digital image watermarking", Proc.SPIE/IS&T Int. Conf. Security and Watermarking of Multimedia Contents, vol. 3657, San Jose, CA, Jan. 25-27, 1999, pp. 14-17.

[NP96] N. Nikolaidis and I. Pitas, "Copyright protection of images using robust digital signatures", Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing (ICASSP-96), vol. 4, Atlanta, GA, May 1996, pp. 2168-2171.

[NP98] N. Nikolaidis, I. Pitas, "Robust Image Watermarking in the Spatial Domain", Signal Processing, Elsevier Science, Vol. 66, No. 3, pp. 385-403, 1998.

[PAK98] F. Petitcolas, R. Anderson, M. Kuhn, "Attacks on Copyright Marking Systems", 2nd workshop on Information Hiding, 1525, Lecture Notes in Computer Science, Portland, Oregon, April 1998, pp. 218-238.

[PAK99] F. A. P. Peticolas, R. J. Anderson and M. G. Kuhn, "Information Hiding –A Survey", Proceedings of the IEEE, Special Issue on Protection of Multimedia Content, 87(7): 1062-1078, July 1999.

[PBBC97] A. Piva, M. Barni, E. Bartoloni, and V. Cappellini, "DCT-based watermarking recovering without resorting to the uncorrupted original image," in Proc. IEEE Int. Conf. Image Processing (ICIP), vol. 1, Santa Barbara, CA, 1997, p. 520

[PD01] C.Podilchuk, E. Delp, "Digital Watermarking: Algorithms and Applications", IEEE Signal Processing Magazine, July 2001, pp. 33-46.

[Pee03] C.B. Peel, "On Dirty-Paper Coding", IEEE Signal Processing Magazine, May 2003, pp. 112-113.

[PFA] F.A. Petitcolas, MATLAB implementation of a D.C.T. based watermarking algorithm by Ingemar J. Cox et al., http://www.petitcolas.net/fabien/software/

[PFA00] F.A. Petitcolas, "Watermarking Schemes Evaluation", IEEE Signal Processing Magazine, Sept.2000, pp.58-64.

[PGP99] ***, "An Introduction to Cryptography", PGP 6.5.1 documentation, 1999, online at ftp://ftp.pgpi.org/pub/pgp/6.5/docs/english/IntroToCrypto.pdf

[PH99] F. Perez–Gonzales, J.R. Hernandez, "A Tutorial on Digital Watermarking", Proc. of the 33rd IEEE Annual Carnahan Conf. on Security Technology, Madrid, Spain, October 1999.

[Pit96] I. Pitas, "A Method for Signature Casting on Digital Images", Proc. ICIP-96, IEEE Int. Conf. Image Processing, vol. III, Lausanne, Switzerland, Sept. 15-17, 1996, pp. 215-218.

[PJ96] J. Puate and F. Jordan, "Using fractal compression scheme to embed a digital signature into an image," in Proc. SPIE Photonics East'96 Symp., Boston, MA, Nov. 1996,

[PK95] I. Pitas, T. Kaskalis, "Applying signatures on digital images", Proc. IEEE Nonlinear Signal Processing workshop, 1995, pp. 460-463

[PL02] P. Loo, "Digital Watermarking using Complex Wavelets", Ph.D. Thesis., March 2002, Univ. of Cambridge,USA

[PM93] W.B. Pennebaker and J.L. Mitchell, "The JPEG Still Image Data Compression Standard", New York: Van Nostrand, 1993

[PMBA05] F. Perez – Gonzales, C. Mosquera, M. Barni, A. Abrado, "Rational Dither Modulation: A High Rate Data-Hiding Method Invariant Gain Attacks", IEEE Trans. On Signal Processing, Vol. 53, No. 10, Oct. 2005.

[PRP99] S. Pereira, J.K. O'Ruanaidh, T. Pun, "Secure Robust Digital Watermarking Using the Orthogonal Transform", In P.W.Wong and E.J.Delp eds., IS&T/SPIE 11th Annual Symposium, Electronic Imaging'99: Security and Watermarking of Multimedia Contents, Vol. 3657 of SPIE Proceedings, pp. 21-30, California, 23-29 Jan. 1999.

[PW02] A. H. Paquet, R. K. Ward, "Wavelet-Based Digital Watermarking for Image Autenthication", IEEE Canadian Conference on Acoustics Speech and Signal Processing (ICASSP) 2002.

[PZ98] C.I. Podilchuk, W. Zeng, "Image-Adaptive Watermarking Using Visual Models", IEEE, JSAC, Vol. 16, No.4,May 1998, pp.525-539.

[RAA99a] M.Ramkumar, A.N. Akansu, A. Alatan, On the Choice of Transforms for Data Hiding in Compressed Video, ICASSP-99

[RAA99b] M. Ramkumar, A.N. Akansu, A.A.Alatan, "A Robust Data Hiding Schemes for Images Using DFT", IEEE, International Conference on Image Processing, II, pp. 211-215, Oc. 1999.

[RDA98] K. Ratakonda, R. Dugad, N. Ahuja, "Digital Image Watermarking: Issues in Resolving Rightful Ownership", ICIP 1998.

[RDB96] J.J.K Ruanaidh, W.J. Dowling, F.M. Boland, "Phase watermarking of digital images", Proc. IEEE Int. Conf. Image Processing, 1996, pp. 239-242.

[RDB96b] J.J.K Ruanaidh, W.J. Dowling, F.M. Boland, "Watermarking digital images for copyright protection", IEE Proc., Vision, Image, and Signal Processing, Aug. 1996, Vol. 143, Issue 4, pp. 250-256.

[RP97] J. J. K. O'Ruanaidh and T. Pun, "Rotation, scale and translation invariant digital image watermarking," in Proc. IEEE Int. Conf. Image Processing 1997 (ICIP 97), Santa Barbara, CA, vol. 1, Oct. 1997, pp. 536–539.

[RP98] J.J.K. Ó Ruanaidh, T. Pun, "Rotation, Scale and Translation Invariant Spread Spectrum Digital Image Watermarking", Signal Processing, 66(1998), pp. 303-317.

[RPHP99] J. O'Ruanaidh, H. Petersen, A. Herrigel, S. Pereira, T. Pun, Cryptographic Copyright Protection for Digital Images based on Watermarking Techniques, Elsevier Science, Theoretical Computer

Science, Vol. 226, Issue 1-2 (Sept. 1999), Special issue: cryptography, pp. 117 - 142, 1999.

[SATW02] C.V. Serdean, M.A. Ambroze, M. Tomlinson and J.G. Wade, "DWT Based Video Watermarking for Copyright Protection, Invariant to Geometrical Attacks", Proc. 3'rd Int. Symp. Communication Systems, Networks and Digital Signal Processing - CSNDSP 2002, Stafford, UK, 15-17 July 2002.

[SC96] J. R. Smith and B. O. Comiskey, "Modulation and information hiding in images," in Lecture Notes in Computer Science: Information Hiding, vol. 1174. Berlin, Germany: Springer, 1996, pp. 207–226.

[SEG00] J.K. Su, J.J. Eggers, B. Girod, "Capacity of Digital Watermarks Subjected to an Optimal Collusion Attack", European Signal Processing Conf. (EUSIPCO 2000), 2000.

[SEG01] J. K. Su, J. J. Eggers, and B. Girod, "Analysis of Digital Watermarks Subjected to Optimum Linear Filtering and Additive Noise", Signal Processing, Special Issue on Information Theoretic Issues in Digital Watermarking, 2001.

[SG99] J. K. Su and B. Girod, "Power-Spectrum Condition for Energy-Efficient Watermarking", Proc. IEEE ICIP '99, Oct. 1999.

[Sha93] J. M. Shapiro, Embedded Image Coding Using Zerotrees of Wavelet Coefficients, IEEE Trans. on Signal Processing, 41:3445–3662, Dec. 1993

[SK01] A. Sequeira, D. Kundur, "Communications and Information Theory in Watermarking: A Survey", Multimedia Systems and Applications IV, A. G. Tescher, B. Vasudev, and V. M. Bove, eds., Proc. SPIE (vol. 4518), pp. 216-227, Denver, Colorado, August 2001.

[SKH05a] K. Su, D. Kundur and D. Hatzinakos, "Statistical Invisibility for Collusion-resistant Digital Video Watermarking", IEEE Trans. on Multimedia, vol. 7, no. 1, pp. 43-51, Feb. 2005.

[SKH05b] K. Su, D. Kundur and D. Hatzinakos, "Spatially Localized Image-Dependent Watermarking for Statistical Invisibility and Collusion Resistance", IEEE Trans. on Multimedia, vol. 7, no. 1, pp. 52-66, Feb. 2005.

[SO03] M.A. Suhail, M.S. Obaidat, "Digital Watermarking-Based DCT and JPEG Model", IEEE Trans. on Instrumentation & Measurement, Vol. 52, No. 5, Oct. 2003, pp. 1640-1647

[SO93] R.G. van Schyndel, C. Osborne, "A Two-Dimensional Watermark", Proc. DICTA, 93, pp. 378-383.

[SP01] V. Solachidis, I. Pitas, "Circularly Symmetric Watermark Embedding in 2-D DFT Domain", IEEE Trans. On Image Processing, 10, 11, Nov 2001, pp.1741-1753.

[SS02] L. Sendur, I. W. Selesnick, "Bivariate Shrinkage Functions for Wavelet-Based Denoising Exploiting Interscale Dependency", IEEE Trans. on Signal Processing, vol. 50, No.11, Nov. 2002, pp. 2744-2756.

[STHW04] L. Shao-Hui, C. Tian-Hang, Y. Hong-Xun,G. Wen, - "A variable depth LSB data hiding technique in images" in Proc. Int. Conf. Machine Learning and Cybernetics, 2004, 26-29 Aug. 2004, vol.7, pp. 3990 - 3994.

[STO94] R.G. van Schyndel, A.Z. Tirkel, C.F. Osborne, "A Digital Watermark", Proc. IEEE Int. Conf. Image Processing, vol. 2, Austin, TX, Nov.1994, pp. 86-90.

[SZT96] M. D. Swanson, B. Zhu, and A. H. Tewfik, "Transparent robust image watermarking," IEEE Proc. ICIP, 1996, 3, pp. 211–214.

[SZT97] M. Swanson, B. Zhu, and A. Tewfik, "Data Hiding for Video in Video", Proceedings of ICIP97, vol. 2, 1997.

[TD97] Bo Tao, B. Dickinson, "Adaptive Watermarking in the DCT Domain", International Conf. On Acoustics, Speech and Signal Processing, ICASSP'97, April, 1997.

[TE04] P. Tao, A.M. Eskicioglu, "A Robust Multiple Watermarking Scheme in the Discrete Wavelet Transform Domain", Optics East 2004 Symposium, Internet Multimedia Management System V Conference, Philadelphia, PA, Oct. 25-28,2004.

[TN02] V. Thilak, A. Nosratinia, "Robust Bandlimited Watermarking With Trellis Coded Modulation", ICIP 2002.

[TNM90] K. Tanaka, Y. Nakamura, K. Matsui, "Embedding secret information into a dithered multi-level image", Proc. IEEE Military Communications Conference, 1990, pp.216-220

[TP00] S. Tsekeridou, I. Pitas, "Wavelet-Based Self-Similar Watermarking for Still Images", IEEE Int. Symp. Circuits & Systems, ISCAS 2000, pp. 220-223.

[TRSH93] A. Z. Tirkel, G. A. Rankin, R. van Schyndel, W. J. Ho, N. Mee, C. F. Osborne, "Electronic Watermark", Digital Image Computing, Technology and Applications, Sydney Australia, 1993, pp. 666-672

[TSO93] A. Tirkel, R. van Schyndel, and C. Osborne, "A twodimensional watermark," in Proc. DICTA 1993.

[TSO95] A.Z. Tirkel, R. van Schyndel, C. Osborne, "A Two-Dimensional Digital Watermark", Digital Image Computing, Technology and Applications, Brisbane Australia, 1995, pp. 378-383

[USC] USC-SIPI image database, http://sipi.usc.edu/database/

[VDPP01] S. Voloshynovskiy, F. Deguillaume, S. Pereira, T. Pun, "Optimal adaptive diversity watermarking with channel state estimation", Proc. SPIE, Security Watermarking Multimedia Contents III, 2001.

[VHBP99] S. Voloshynovskiy, A. Herrigel, N. Baumgartner, T. Pun, "A Stochastic Approach to Content Adaptive Digital Image Watermarking," Intl Workshop in Information Hiding, Dresden, Germany, Oct. 1999.

[VP96a] G. Voyatzis and I. Pitas, "Applications of toral automorphisms in image watermarking," in Proc. Int. Conf. Image Processing (ICIP), vol. 3, Lausanne, Switzerland, Sept. 1996, pp. 237–240.

[VP96b] G. Voyatzis and I. Pitas, "Chaotic mixing of digital images and applications to watermarking," in Proc. Europ. Conf. Multimedia Applications, Services, and Techniques (ECMAST), Louvain-la-Neuve, Belgium, May 1996.

[VP99] G.Voyatzis, I. Pitas, "Problems and Challenges in Multimedia Networking and Content Protection", TICSP Series No. 3, editor Iaakko Astola, March 1999.

[VPPE01] S. Voloshynovskiy, S. Pereira, T. Pun, J. J. Eggers and J. K. Su, "Attacks on Digital Watermarks: Classification, Estimation-Based

Attacks, and Benchmarks", IEEE Comm. Magazine, pp.2-9, Aug.2001.

[VSA00] S. Voloshynovskiy et al., "Generalized Watermark Attack Based on Watermark Estimation and Perceptual Remodulation", IS&T/SPIE's 12th Annual Symp., Electronic Imaging 2000: Security and Watermarking of Multimedia Content II, P. W. Wong and E. J. Delp, Eds., SPIE Proc., vol. 3971, San Jose, CA, Jan. 2000.

[VSA01] S. Voloshynovskiy et al., "Attack Modeling: Towards a Second Generation Watermarking Benchmark", Signal Processing, Special Issue on Information Theoretic Issues in Digital Watermarking, 2001.

[VSA99] S. Voloshynovskiy et al., "A Stochastic Approach to Content Adaptive Digital Image Watermarking", Int'l. Wksp.Info.Hiding, vol. LNCS 1768, Lecture Notes in Comp. Sci., Springer Verlag, 29 Sept. -1 Oct. 1999, pp. 212-36.

[Wal95] S. Walton, "Information Authentication for a Slippery New Age", Dr. Dobbs Journal, vol. 20, no. 4, pp. 18-26, Apr. 1995.

[Wat93] A. B. Watson, "DCT Quantization Matrices Visually Optimized for Individual Images", Human Vision, Visual Processing, and Digital Display IV, Bernice E. Rogowitz, Editor, Proc. SPIE 1913-14, (1993), pp. 202-216.

[WD96] R.B. Wolfgang and E.J. Delp, "A Watermark for Digital Images", Proc. IEEE Int. Conf. Image Processing, vol. III, Sept. 16-19, 1996, Lausanne, Switzerland, pp. 219-222.

[WL02a] M. Wu, B.Liu, "Data Hiding in Image and Video: Part I Fundamental Issues and Solutions", Trans. on Image Processing, Vol. 12, No. 6, June 2003, pp. 685 - 695.

[WL02b] M. Wu, B.Liu, "Data Hiding in Image and Video: Part II Fundamental Issues and Solutions", Trans. on Image Processing, Vol. 12, No. 6, June 2003, pp. 685 - 695.

[WL98] M. Wu, B. Liu: "Watermarking for Image Authentication", ICIP, 1998.

[WMBC99] M. Wu, M. L. Miller, J. A. Bloom, and I. J Cox, "A rotation, scale, and translation resilient public watermark," in Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing 1999 (ICASSP '99), Phoenix, AZ, 1999.

[WPD99] R.B.Wolfgang, C.I.Podilchuk, E.Delp, "Perceptual Watermark for Digital Images and Video", Proc. of the IEEE, Vol. 87, No. 7, July 1999, pp 1108-1155.

[WPW98] P.W.Wong, "A Watermark for Image Integrity and Ownership Verification", Proc IS&T PIC, Portland, Oregon, 1998.

[WPW98b] P.W. Wong, "A Public Key Watermark for Image Verification and Authentication", ICIP 1998.

[WQF98] Wei, Z.H.; Qin, P.; Fu, Y.Q., "Perceptual digital watermark of images using wavelet transform", IEEE Trans. Consumer Electronics, Vol. 44, Issue 4, Nov. 1998, pp. 1267 - 1272

[WSAB00] G. Wade, C. Serdean and A. Ambroze, M. Borda, I. Nafornita, "Watermarking uncompressed video: an overview", invited paper, proc. Int. Symp. Electronics & Telecommunications, Timisoara, 2000.

[WSB03] Z. Wang, H.R. Sheikh, A.C. Bovik, "Objective Video Quality Assessment", Chapter 41 in The Handbook of Video Databases: Design and Applications, B. Furht and O. Marqure, ed., CRC Press, pp. 1041-1078, September 2003.

[WSK98] H.J.M. Wang, P.C. Su, C.-C.J.Kuo, "Wavelet-Based Digital Image Watermarking", Optics Express, Dec. 1998, 3, 12, pp. 491-496.

[WTWL04] M. Wu, W. Trappe, Z.J. Wang, K.J.R. Liu, "Collusion-Resistant Fingerprinting for Multimedia", IEEE Sign. Proc. Magazine, March 2004, pp.15-27.

[Wu03] M. Wu, "Joint Security and Robustness Enhancement for Quantization Based Data Embedding", IEEE, Trans. On Circuits and Systems for Video Technology, Vol.13, No. 8, Aug. 2003

[WYSV96] A. B. Watson, G. Y. Yang, J. A. Solomon, and J. Villasenor, "Visual thresholds for wavelet quantization error," in Proc. SPIE Human Vision and Electronic Imaging, 1996, vol. 2657, pp. 381–392.

[XA98] L. Xie, G. Arce, "Joint Wavelet Compression and Authentication Watermarking", IEEE International Conference on Image Processing, Chicago, IL, Oct 1998.

[XBA97] X.-G. Xia, C.G. Boncelet and G.R. Arce, "A Multiresolution Watermark for Digital Images", Proc. of International Conference on Image Processing, vol. 3, pp.48-51, 1997.

[XBA98] X. Xia, C. G. Boncelet, and G. R. Arce, "Wavelet Transform Based Watermark for Digital Images", Optics Express, Vol. 3, No. 12, 1998, pp. 497-505.

[YKL01] H.H. Yu, D. Kundur, C.-Y. Lin, "Spies, Thieves, and Lies: The Battle for Multimedia in the Digital Era", IEEE Multimedia, July-Sept. 2001.

[YLLS00] G. Yu and C. Lu and H. Liao and J. Sheu, "Mean Quantization Blind Watermarking for Image Authentication", Proc. IEEE Int. Conf. on Image Processing, Vancouver, Canada, Vol. III, pp. 706-709, 2000.

[YM97] Yeung, M., Mintzer, F. "An invisible watermarking technique for image verification", Proc. IEEE Int. Conf. Image Processing. Volume 2. (1997) 680—683.

[ZL00] Zhihui Wei, Xiao Liang, "An Evaluation Method for Watermarking Techniques," IEEE International Conference on Multimedia and Expo, 2000, pp. 373-376.

[ZL99] W. Zeng, B. Liu, A Statistical Watermark Detection Technique without using Original Images for Resolving Rightful Ownerships of Digital Images, IEEE Transactions on Image Processing, Nov. 1999, Vol. 8, No. 11, pp. 1534-1548

[ZWWL03] H. Zhao, M. Wu, Z. J. Wang, K.J.R. Liu, "Nonlinear Collusion Attacks on Independent Fingerprints for Multimedia", Proc. IEEE Int. Conf. Acoustics, Speech, Signal Processing, ICASSP 2003, Hong Kong, Apr.2003, pp.664-667.

[ZXZ98] W. Zhu, Z. Xiong, and Y.-Q. Zhang, "Multiresolution watermarking for images and video: a unified approach," in Proc. Int. Conf. on Image Processing (ICIP), Chicago, IL, 1998.

[ZXZ98] W. Zhu, Z. Xiong, and Y.-Q. Zhang, "Multiresolution watermarking for images and video," IEEE Trans. Circ. Sys. Video Tech., Vol. 9, No. 4, pp. 545-550, Jun. 1999

[ZZS03] D. Zheng, J. Zhao, A.E. Saddik, "RST Invariant Digital Image Watermarking Based on Log-Polar Mapping and Phase Correlation",

Trans. On Circuits and Systems for Video Technology,No. 8, Aug. 2003, pp. 753-765