Buletinul Ştiinţific al Universităţii "Politehnica" din Timişoara

Seria ELECTRONICĂ şi TELECOMUNICAŢII
TRANSACTIONS on ELECTRONICS and COMMUNICATIONS

Tom 49(63), Fascicola 2, 2004

Selective encryption of image with IDEA algorithm

Gabriel G. Fericean[1], Monica Borda[2]

Abstract – In this paper, a study of selective image encryption using IDEA algorithm is presented. Experimental results show a good image security using the proposed selective encryption.

Keywords: IDEA, image encryption, selective encryption, cryptography, encryption.

I. INTRODUCTION

The strongest solutions for security are offered by computational cryptography. Cryptography is used for insuring the communication confidentiality in military and diplomatic fields for a long time. During last years, cryptography has known a spectacular progress, many services and devices of security, which are used in Internet is a proof of this fact. Image encryption is among the last applications of cryptography. It looks to have in the near future many applications in Internet, taking into account that fingerprints and retina images will replace the numeric passwords.

II. IDEA ALGORITHM

Xuejia Lai and James Massey of the Swiss Federal Institute of Technology developed the International Data Encryption Algorithm (IDEA) in 1999 year. The main application for IDEA is PGP (Pretty Good Privacy). This program is the most secure and fast encryption system nowadays.

Cryptographic strength of IDEA is given by:

- Block length
- Key length – is long enough to prevent exhaustive key searches
- Confusion – the cipher text should depend on the plain text and key in a complicated way.
- Diffusion – each plaintext bit should influence every chipertext bit, and each key bit should influence every chipertext bit.

Confusion is achieved by mixing three different operations. Each operation is executed on two 16-bit inputs. These operations are:

- Exclusive–or (XOR)
- Addition by integer modulo 2^{16}, inputs and output are unsigned 16 – bit integer
- Multiplication of integers modulo $2^{16}+1$, inputs and output is unsigned 16-bit integer. In this case the blocks of all zeros is treated as representing 2^{16}.

Using this three operations we provide a complex transformation of the input, making cryptanalysis much more difficult than DES algorithm, which uses just XOR operation.

In IDEA, diffusion is provided by the basic building block of the algorithm, known as multiplication/addition (MA) structure (figure 2.). This structure has as inputs two 16-bit values derived from the plaintext and two 16-bit subkeys derived from the primary key and produces 16-bit outputs. This particular structure is repeated eight times in the algorithm (figure 1.).

IDEA uses a primary key of 128 bits long. This primary key produces 52 subkeys with 16-bit long. Encryption and decryption makes on 64-bit blocks.

Subkeys Generation

First 8 subkeys are taken directly from the primary key through segmentation in 16-bit segments. Then a circular left shift of 25 bit position is applied to the primary key and the next eight subkeys are extracted. This procedure is repeated until all 52 subkeys are generated.

Encryption

Encryption schema for IDEA has two inputs plaintext (64b) and primary key (128b). IDEA is making up for 8 rounds and one output transformation. These algorithms divide plaintext in 4 blocks of 16 bits. Output transformation achieves 4 outputs of 16 bits, which is concatenated and makes chipertext of 64 bits. Each round uses 6 subkeys of 16-bits, but output transformation uses 4 subkeys (figure 1.)

[1] Facultatea de Electronică şi Telecomunicaţii, Departamentul Comunicaţii Str. Daicoviciu Nr. 2, Cluj-Napoca, e-mail gabifericean@yahoo.com
[2] Facultatea de Electronică şi Telecomunicaţii, Departamentul Comunicaţii Str. Daicoviciu Nr. 2, Cluj-Napoca, e-mail Monica.Borda@com.utcluj.ro

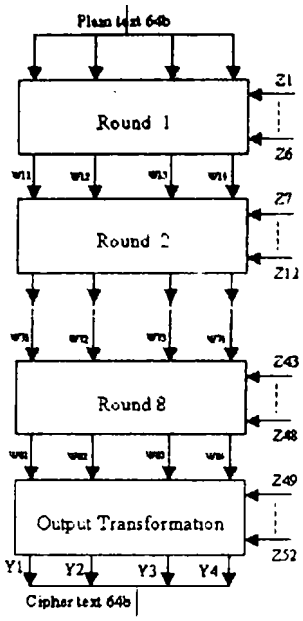

Figure 1. Idea algorithm

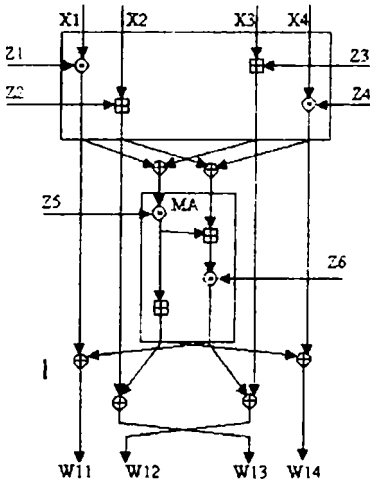

Figure 2.

Decryption

In this case the inputs is chipertext (64b) and different selection of subkeys. Decryption subkeys $U_1,...,U_{52}$ are derived from encryption subkeys as follows:

- First 4 subkeys of decryption round i are derived from the first 4 subkeys of encryption round 10-i, where the output transformation is counted as round 9. First and fourth subkey are equal to the multiplicative inverse modulo $2^{16}+1$ of the corresponding first and fourth encryption subkeys. For round 2 through 8, the second and third decryption subkeys are equal to the additive inverse modulo 2^{16} corresponding third and second encryption subkeys. For round 1 and 9, the second and third decryption subkeys are equal to the additive inverse modulo 2^{16} of corresponding second and third encryption subkeys.
- For the first 8 rounds, the last two subkeys of decryption round i are equal to last two subkeys of encryption round 9-i. [5],[6]

III. SELECTIVE ENCRYPTION

Selective encryption or partial encryption represents a good idea if we wish to reduce the volume of calculation necessary for image processing. The security of selective encryption application is always lower than using full encryption. The only reason to use selective encryption is to reduce time and computational demand.

This method can be applied to binary images or any other format as: JPEG, BMP, GIF, PNG. If applied to a binary image, the method consists in mixing image data and a message (key) that has the same size as the image. A XOR function is sufficient when the message is used only once. A generalized for gray level images, is possible: in this case the image is divided in bitplanes, which are encrypted separately and reconstruct a gray level image. The highest bitplanes exhibit some similarities with the image, but the least significant bitplanes look random, adding noise to the image.

Selective encryption can be applied with any cryptographic algorithm (IDEA, AES, DES). [14], [15], [16].

IV. EVALUATION OF SELECTIVE ENCRYPTION

In this chapter we present a study of behavior for image encryption and implementation of selective encryption for color planes (RGB), for luminance and chrominance planes and for bitplanes. The IDEA algorithm is used for encryption because it offers high security and we have experience in VHDL im lementation for IDEA al orithm.

Luminance and chrominance planes are obtain from color planes using the following formulae:

$$\begin{aligned} Y &= 0.299*R + 0.587*G + 0.114*B \\ U &= 0.493*(B-Y) \\ V &= 0.877*(R-Y) \end{aligned} \quad (1)$$

The color plains are obtain from luminance and chrominance with the relations:

$$\begin{aligned} R &= Y + 1.14*V \\ G &= Y - 0.395*U - 0.581*V \\ B &= Y + 2.032*U \end{aligned} \quad (2)$$

Difficulties were met in primary key generation because Matlab uses only 52 bits to represent a

number. For this reason the number of all zero subkeys is very high, so we looked for another solution: we generated eight subkeys with values between 1 and 2^{16}, than we transformed in binary and concatenated them. After these operations we obtained primary key with 128 bits dimension.

Next we present the results obtained for color plane encryption on different images.

For a correct function, after the program compilation, we must import an image and generate a primary key. These operations achieve on *File* menu (figure 3).

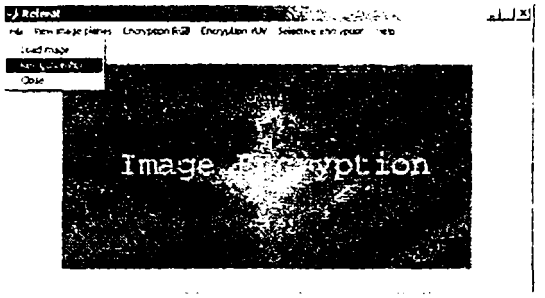

Figure 3. Image of application

Now we can achieve the image encryption. The color planes (RGB) encryption is as follows: for encrypting all planes the *Encryption RGB* menu is accessed, where the *Encryption planes RGB* option is chosen. For encrypting only one of this color planes one of next options: *Encryption plane R*, *Encryption plane G*, *Encryption plane B* are available. The next five images present results for color plane encryption.

Figure 4 Original image

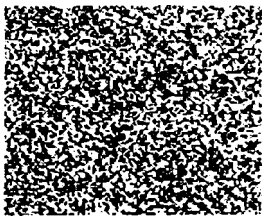

Figure 5 Encryption RGB planes

Figure 6 Encryption R plane

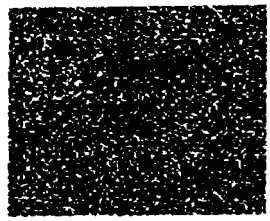

Figure 7 Encryption G plane

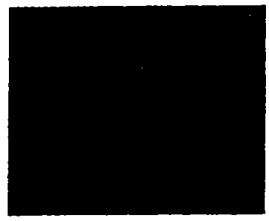

Figure 8 Encryption B plane

For color plane encryption, the encrypted image is secured only if all color planes are encrypted.

Figure 9 Image view without R plane

This fact is valid for any combination at the color planes.

Luminance and chrominance planes encryption is the same with color planes encryption. For a secure encryption we must encrypt all planes. A presentation of the luminance and chrominance planes encryption for the same image is done in figure 10.

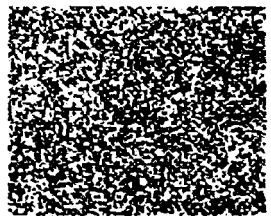

Figure10 Encryption YUV planes

The proposed method has as disadvantage the necessary time for all pixels encryption. Figures 11 to 18 present results obtained for bitplanes encryption. Each of these figures is followed by the representation of the initial image without bitplanes encryption. The most significant bit (msb) plane is considered the plane 1 and the last significant bit (lsb) plane is considered the plane 8.

Figure 11 Encryption first plane

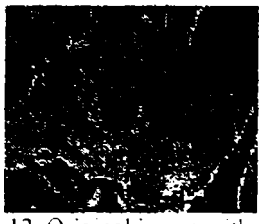

Figure 12 Original image without first plane

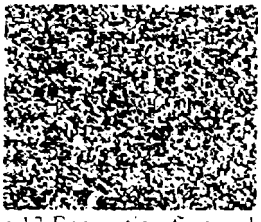

Figure 13 Encryption first and second planes

Figure 14 Original image without first and second planes

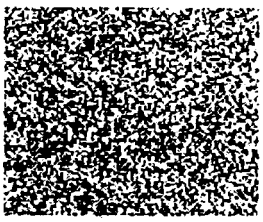

Figure 15 Encryption first, second and third planes

Figure 16 Original image without first, second and third planes

Because the security is lower for encryption of lsb planes (8 – 2) we decided to represent only encrypted images (figures 19 to 21).

Figure 19 Encryption eighth plane

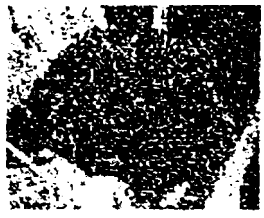

Figure 20 Encryption second, third, fourth, fifth, sixth, seventh and eighth planes

Figure 21 Original image without lsb plane

Figure 22 a.Original image

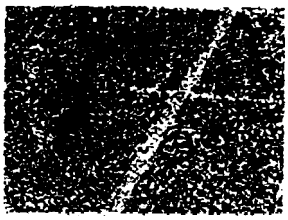

Figure 22 b. Encryption first plane (msb)

Figura 22 c. Original image without first plane

Through selective encryption we can offer more security planes, the minimum for an acceptable security being represented by the first plane encryption (msb plane). This affirmation is sustained by the experiment presented in figure 22.

V. CONCLUSIONS

Our paper had as starting point the need of transmitting safely images on Internet, images such as fingerprints, medical images, etc.

Such images must guarantee a high security rank as well as speed and all these can be obtained through cryptographic algorithm and hard implementation.

The whole paper is a study of encryption tehnics for images with experimental results.

The concluding remarks are:

- For image encryption the first step is the knowledge of needed security rank.
- If a fast connection is needed and less security, we can choose for selective encryption, encrypt only first plane (msb plane).
- To enhance the security degree, we can encrypt first and second bitplanes. In this mode we can grow image security until image security is relied only on algorithm security. Maximum security can be provided if all bitplanes are encrypted.
- For color planes encryption, image security can be obtained only for all color planes encryption.

REFERENCES

[1] http://www.byte.ro/byte95-03/vic.html [2004]

[2] Vasiu Ioana, *Criminalitatea informatică*, Editura Nemira, 2001

[3] Patriciu Victor, Monica Pietroşanu-Ene, Ion Bica, Costel Cristea, *Securitatea informatică în UNIX şi INTERNET*, Editura Tehnică, 1998

[4] Bajenescu T., Borda M. *Securitatea in informatica si telecomunicatii*, Editura Dacia, Cluj-Napoca, 2001

[5] Schneier B. *Applied Cryptography, Second Edition*, Editura John Wiley& Sons, Inc 1996

[6] Stallings W.: *Cryptography and Network Security: Principles and Practice Second Edition*, Editura Prentice Hall, New Jersey, 1999

[7] Borko Furth, Darko Kirovski, *Multimedia Security Handbook*, February 17, 2004

[8] Vlaicu A., *Curs multimedia*, 2002 (manuscris)

[9] Gibson D. Jerry, Berger T., Lookabaugh T., Lindbergh D., Baker R., *Digital compresion for multimedia: Principles and Standards*, Editura morgan Kaufmann, 1998

[10] Biryukov A., Nakahara J., Preneel B., Vandewalle, J. *New Weak Key Classes of IDEA, Advances in Cryptology, Eurocrypt 1998*

[11] Daemen J., Govaerts R., Vandewalle J.: Weak Keys for IDEA, *Advances in Cryptology, Crypto'93, LNCS 773*, D.R Stinson, Ed., Springer-Verlag, 1994

[12] Marc Van Droogenbroeck and Raphaël Benedett. Techniques for a selective encryption of uncompressed and compressed images. In Proc. Advanced Concepts for Intelligent Systems (ACIVS'02), pages 90–97, 2002.

[13] Martina Podesser, Hans-Peter Schmidt, and Andreas Uhl. Selective bitplane encryption for secure transmission of image data in mobile environments. In Proc. 5th IEEE Nordic Signal Processing Symposium (NORSIG'2002), 2002.

[14] Roland Norcen, Martina Podesser, Andreas Pommer, Hans-Peter Schmidt, and Andreas Uhl. Confidential storage and transmission of medical image data. Computers in Biology and Medicine, 33(3):277–292, 2003.