SELECTIVE IMAGE ENCRYPTION USING DCT WITH AES CIPHER

Belazi Akram, Benrhouma Oussama, Hermassi Houcemeddine and Belghith Safya

SysComLab, Ecole Nationale d'Ingénieurs de Tunis (ENIT), Tunis, Tunisia
belazi.akram@gmail.com

ABSTRACT

Selective encryption presents a great solution to optimize time efficiency during encryption process. In this paper a novel selective encryption scheme based on DCT transform with AES algorithm is presented. In the DCT method, the basic idea is to decompose the image into 8×8 blocks and these blocks are transformed from the spatial domain to the frequency domain by the DCT. Then, the DCT coefficients correlated to the lower frequencies of the image block are encrypted. The proposed cryptosystem is evaluated using various security and statistical analysis; results show that the proposed algorithm is strong against attacks and suitable for practical application.

KEYWORDS

DCT, Selective Encryption, AES Cipher

1. INTRODUCTION

Nowadays, multimedia content (image, audio and video) presents an enormous importance giving the fact of the rapid growth of high technologies. The rate of exchanges these types of information is growing and the need to protect it is more and more essential. However increasing number of digital documents, multimedia processing tools, and the worldwide availability of Internet access has created an ideal way to uncontrollable distribution of multimedia content [1]. To protect data, various encryption schemes has been proposed for image encryption, [2,3,4] however in these schemes (total encryption schemes) all data has to be encrypted which will generally take some time, complicated calculations and high memory occupation, which makes these schemes hard to use in real time applications.

Total encryption schemes are not necessary when we talking about most multimedia content. Given to the fact that the content is already voluminous and not all the content represents a significant importance we choose to encrypt only significant parts of the data and leave the rest to enhance time encryption and reduce memory occupation and make the encryption scheme suitable in practical application given to the fact that selective crypto-systems presents a simple architecture.

Selective encryption protects the most visually important parts of an image or video representation [5,6,7]. Encrypting only parts of the image data must be sufficient to satisfy the needed security [8,9]. There are two basic ways to encrypt digital images: in the spatial domain or in the transform domain [10]. Since wavelet based compression appeared and was adopted in the

Natarajan Meghanathan et al. (Eds) : NeTCoM, CSIT, GRAPH-HOC, SPTM - 2014
pp. 69–77, 2014. © CS & IT-CSCP 2014 DOI : 10.5121/csit.2014.41306

JPEG2000 standard, suggestions for image encryption techniques based in the wavelet domain have been abundant. However, many of these are not secure as they are based exclusively on random permutations making them vulnerable to known or chosen-plaintext attacks [11, 12, 13, 19]. For example, in DCT codec several selective encryption schemes have been proposed. Droogenbroeck and Benedett [14] selected AC coefficients from compressed images for encryption. In their method the DC coefficients are not ciphered because they carry important visible information and they are highly predictable. The compression and encryption operations are separated in this approach and this requires an additional operating cost. Jiang-Lung Liu [15] proposes to encrypt the low-frequency DCT coefficients only and leave the high-frequency ones unencrypted in the JPEG compression.

In this paper we propose a selective encryption scheme based on DCT transformation and AES algorithm to cipher digital images.

The rest of the paper is organized as follow: section 2 presents a mathematical preliminary for the DCT transform, section 3 we present our encryption, experimental results are presented in section and we conclude in section 5.

2. FREQUENCY BAND ENCRYPTION IN A DCT BLOCK

In a DCT-based codec, media data are partitioned into blocks (typically, 8 × 8 or 4 × 4), and each block is transformed by DCT, quantized and encoded with entropy coding. Generally, the DCT block is scanned in zigzag order, which generates the coefficient sequence ordered from the highest frequency to the lowest frequency. In this coefficient sequence, the first coefficient denotes the DCT block's energy, and the other coefficients denote detailed information on the image block. The DCT block is scanned from the bottom- left to the top- right, as shown in Figure 1. Thus, the first coefficient in the coefficient sequence denotes the block's energy.

In perceptual encryption, the 64 coefficients can be selected from the first one to the last one according to the quality factor Q. Thus, set N = 64 for each DCT block. Figure 2 shows the relation between n and the PSNRs of the encrypted images. As can be seen, with increase in n, the quality of the images decreases.

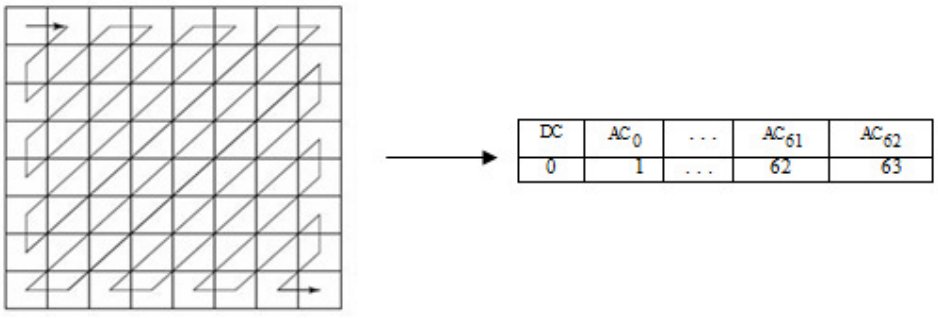

Figure 1. Coefficient sequence generation in a DCT block

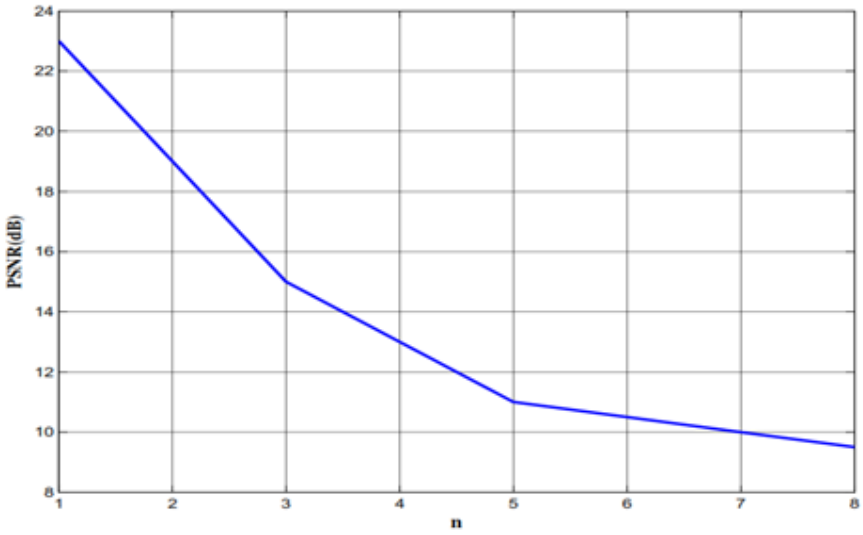

Figure 2. Relation between the quality of the encrypted images and n

For example in JPEG compressed images, there are many techniques that were developed to encrypt parts of JPEG compressed images [15,17]. One technique suggested encrypting some of the Discrete Cosine Transform (DCT) coefficients in each 8x8 blocks [15], as shown in Figure 3. The first value of the DCT coefficients matrix is called the DC coefficient, and the rest are called AC coefficients [16]. The unencrypted high-frequency coefficients provide little information about the original 8 x 8 blocks. However, when the image blocks are considered together, the unencrypted high frequency coefficients often show outlines of objects in the image [15]. An alternative technique is to encrypt the bits that indicate the sign and magnitude of nonzero AC coefficients [17]. Since they are highly predictable, the DC coefficients are left unencrypted.

DC	AC	AC	AC	AC	AC	AC	
AC	AC	AC	AC	AC	AC		
AC	AC	AC	AC	AC			
AC	AC	AC	AC				
AC	AC	AC					
AC	AC						
AC							

Figure 3. The DCT coefficients matrix and the encrypted coefficients

3. THE PROPOSED ENCRYPTION SCHEME

The proposed method based on the idea of decomposing the image into 8x8 blocks, these blocks are transformed from the spatial domain to frequency domain by the DCT. Then, the DCT coefficients related to the higher frequencies of the image block are encrypted using the AES cipher. The concept behind encrypting only some selective DCT coefficients based on the fact that the image details are situated in the higher frequencies, In fact the image encryption

algorithm obtains higher security when DCT coefficients related to the lower frequencies are encrypted than those related to higher frequencies. Fig. 4 shows the general block diagram of the proposed method of selective image encryption. We propose a secure encryption scheme:

(i) Block 1: All coefficients are encrypted.

(ii) Blocks 2, 3. . . n: The 24 most significant bit-planes are encrypted.

Where n is the number of block.

The general block diagram of the proposed method of selective image encryption is shown in Figure 4, which combines encryption process with DCT codec, and is composed of data encoding, parameter encryption and data decoding. Here, P, K and C are the plaintext, key and ciphertext, respectively. X and Y are the parameters in the data stream, among which, X is encrypted into Z according to Z = E(X, K) while Y is left unchanged. Without losing the generality, the data stream composed of two parameters is investigated. If the data steam is composed of more parameters, the similar results can be obtained.

4. EXPERIMENTAL RESULTS

In this section, the performance of the proposed image encryption scheme is analyzed in detail. It is well known that statistical analysis is of crucial importance. Indeed, an ideal cipher should be robust against any statistical attack. In order to prove the robustness of proposed image encryption scheme, we have performed some statistical tests which are described in the following.

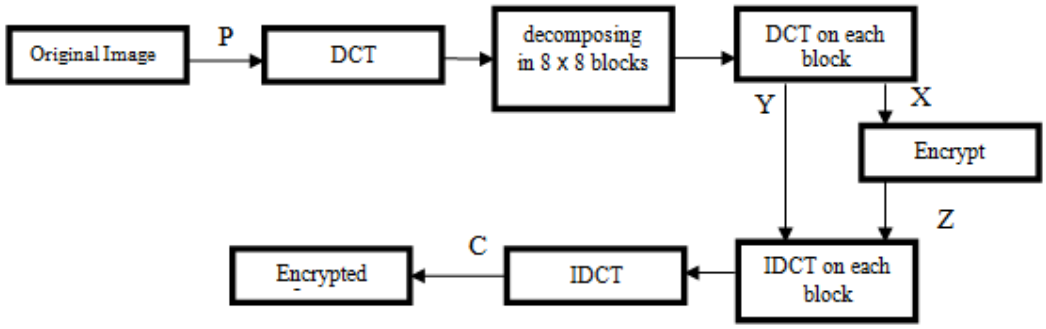

Figure 4. Block diagram of the proposed method

4.1. Histogram

To demonstrate that our proposed algorithm has strong resistance to statistical attacks, test is carried out on the histogram of enciphered image. Several gray-scale images of size 256×256 are selected for this purpose and their histograms are compared with their corresponding ciphered image. One typical example is shown below. The histogram of the original image contains large spikes as shown in Figure 5 but the histogram of the ciphered image as shown in Figure 6, is more uniform. It is clear that the histogram of the encrypted image is, significantly different from the respective histogram of the original image and bears no statistical resemblance to the plain image. Hence statistical attack on the proposed image encryption procedure is difficult.

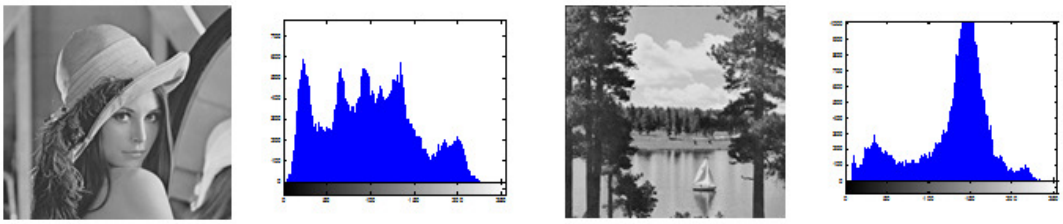

Figure 5. Histogram of Original Image

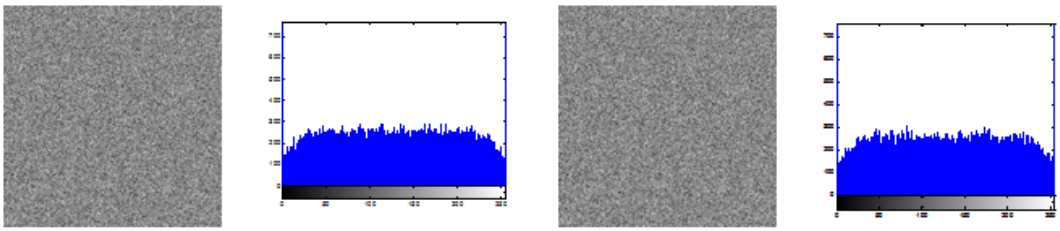

Figure 6. Histogram of Encrypted Image

4.2. Correlation of adjacent pixels

It is well known that adjacent image pixels are highly correlated either in horizontal, vertical or diagonal directions. Such high correlation property can be quantified by means of correlation coefficients which are given by:

$$r = \frac{\mathrm{cov}(p,q)}{\sqrt{D(p)}\sqrt{D(q)}} \qquad (1)$$

Where,

$$D(p) = \frac{1}{S}\sum_{i=1}^{S}(p_i - \bar{p})^2$$

$$\mathrm{cov}(p,q) = \frac{1}{S}\sum_{i=1}^{S}(p_i - \bar{p})(q_i - \bar{q})$$

q_i and p_i denote two adjacent pixels (either horizontal or vertical). S is the total number of duplets (p_i,q_i) obtained from the image; $\bar{p}$ and $\bar{q}$ are the mean values of p_i and q_i , respectively. The correlation coefficients of the plain and ciphered images of Lena and Boat are given in the Table 1. It can be observed that the encrypted images obtained from the proposed scheme have small correlation coefficients in horizontal, vertical and diagonal directions. The result are illustrated in Figure 7 and Figure 8, which presents the distribution of two adjacent pixels in the original and encrypted images of Lena and Boat for horizontal (a-b), vertical (c-d) and diagonal (e-f) directions.

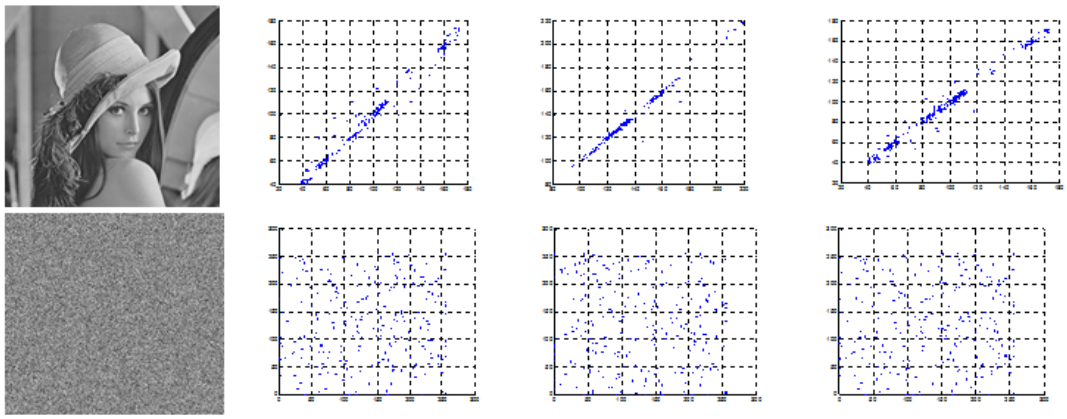

Figure 7. the distribution of two adjacent pixels in the original and encrypted lena.

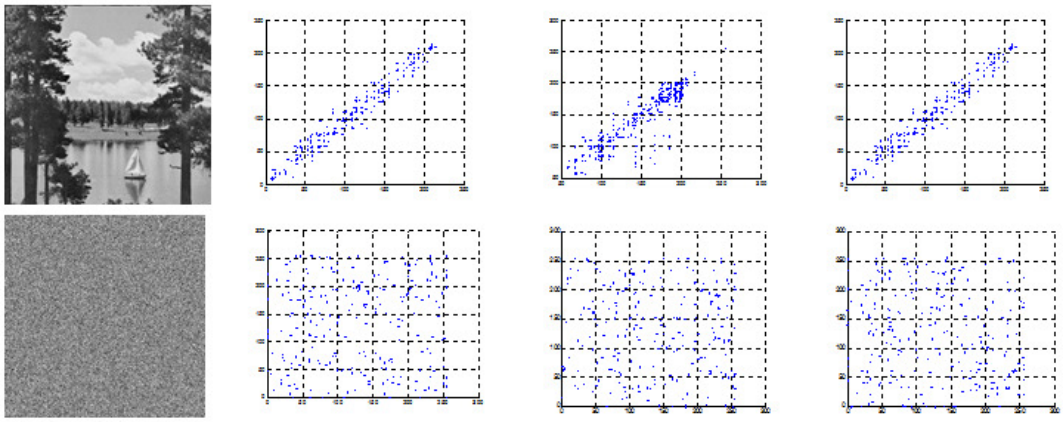

Figure 8. the distribution of two adjacent pixels in the original and encrypted boat.

Table 1. Correlation coefficients of two adjacent pixels in original and encrypted images.

Image	Horizontal		Vertical		Diagonal	
	Original	Encrypted	Original	Encrypted	Original	Encrypted
Lena	0.9888	0.0138	0.9917	-0.0383	0.9923	0.0171
Boat	0.9829	-0.0016	0.9818	-0.0682	0.9769	-0.1169

4.3. Differential attack

As a general requirement for all the image encryption schemes, the encrypted image should be greatly different from its original form. Such difference can be measured by means of two criteria namely, the NPCR (Number of Pixel Change Rate) and the UACI (Unied Average Changing Intensity) [18]. The NPCR is used to measure the number of pixels in difference between two images. Let S(i,j) and S'(i,j) be the (i,j)th pixel of two images S and S' ,respectively.

The NPCR can be defined as:

$$NPCR = \frac{\sum_{i;j} D(i,j)}{L} \times 100\% \qquad (2)$$

Where L is the total number of pixels in the image and D(i,j) is defined as :

$$D(i,j)\begin{cases}0 \; if \;\; S(i,j) = S'(i,j) \\ 1 \; if \;\; S(i,j) \neq S'(i,j)\end{cases}$$

Where S(i,j) and S'(i,j) are the pixel values of the two images, respectively. For instance, for two random images:

$$NPCR = 99.609375\%$$

The second criterion, UACI, is used to measure the average intensity difference and can be defined as:

$$UACI = \frac{1}{L}(\sum \frac{|S(i,j) - S'(i,j)|}{2^B - 1} \times 100\% \qquad (3)$$

Where B is the number of bits used to represent a grey scale pixel value. In the case of two random images, the expected value of UACI is:

$$UACI = 33.46354\%$$

The NPCR and UACI measured between the plain and ciphered images of Lena and Boat with the proposed cryptosystem are given in Table 2.

Table 2. Sensitivity to differential attacks.

Image	**NPCR%**	**UACI%**
Lena	99.5941	33.7715
Boat	99.5895	33.4626

4.4. Information entropy

Entropy is a statistical measure of randomness. Ideally, the information entropy should be 8 bits for gray scale images. Table 3 shows the entropy of different test images of size 256×256.

Table 3. Entropy results for encrypted images.

Image	**Entropy of Encrypted Image**
Lena	7.8683
Boat	7.8745

It's seen that the value of entropy for encrypted images is very close to the 8 bits, then the loss of information is negligible, and the proposed algorithm is strong against entropy attack.

5. CONCLUSIONS

Selective Image Encryption Using DCT with AES Cipher has been presented in this paper. The algorithm will not encrypt bit by bit the whole image but only selective DCT coefficients will be encrypted. Indeed the proposed encryption method uses the Selective Encryption approach where the DC coefficients and some selective AC coefficients are encrypted, hence the DC coefficients carry important visual information, and it's difficult to predict the selective AC coefficients, this give a high level of security in comparison with methods mentioned above. Several security and

statistical analysis tests are carried out in order to check the robustness of the proposed algorithm. Both simulations and analysis results prove the efficiency of the proposed cryptosystem.

REFERENCES

[1] IEEE Transactions on Circuits and Systems for Video Technology (2003) : Special Issue on Authentication, Copyright Protection, and Information Hiding, Vol. 13, No. 8.

[2] Liansheng Sui, Kuaikuai Duan, Junli Liang, Zhiqiang Zhang & Haining Meng , (2014) Asymmetric multiple-image encryption based on coupled logistic maps in fractional Fourier transform domain", Optics and Lasers in Engineering, Volume 62, Pages 139-152

[3] A. Alfalou, C. Brosseau & N. Abdallah, (2015) "Simultaneous compression and encryption of color video images", Optics Communications, Volume 338, Pages 371-379

[4] Tieyu Zhao, Qiwen Ran & Yingying Chi, (2015) "Image encryption based on nonlinear encryption system and public-key cryptography", Optics Communications, Volume 338, Pages 64-72

[5] Li-feng WANG, Wen-dong WANG, Jian MA, Chen XIAO & Kong-qiao WANG, (2008) "Perceptual video encryption scheme for mobile application based on H.264", The Journal of China Universities of Posts and Telecommunications, Volume 15, Supplement, Pages 73-78.

[6] Sukalyan Som & Sayani Sen, (2013) "A Non-adaptive Partial Encryption of Grayscale Images based on Chaos", Procedia Technology, Volume 10, Pages 663-671.

[7] Xinjun Zhang & Xingyuan Wang, (2013) "Chaos-based partial encryption of SPIHT coded color images", Signal Processing, Volume 93, Pages 2422-2431.

[8] Nidhi Taneja, Balasubramanian Raman & Indra Gupta, (2011) "Selective image encryption in fractional wavelet domain", AEU - International Journal of Electronics and Communications, Volume 65, Issue 4, Pages 338-344.

[9] Gaurav Bhatnagar & Q.M. Jonathan Wu, (2012) "Selective image encryption based on pixels of interest and singular value decomposition", Digital Signal Processing, Volume 22, Issue 4, July 2012, Pages 648-663.

[10] S. Li & G. Chen, (2004) "Chaos-Based Encryption for Digital Images and Videos", in Multimedia Security Handbook, B. Furht and D. Kirovski, CRC Press.

[11] Akram Belazi, Houcemeddine Hermassi, Rhouma Rhouma & Safya Belghith, (2014) "Algebraic analysis of a RGB image encryption algorithm based on DNA encoding and chaotic map", Nonlinear Dynamics June, Volume 76, Issue 4, pp 1989-2004.

[12] Houcemeddine Hermassi, Akram Belazi, Rhouma Rhouma & Safya Mdimegh Belghith, (2014) "Security analysis of an image encryption algorithm based on a DNA addition combining with chaotic maps", Multimedia Tools and Applications ,Volume 72, Issue 3, pp 2211-2224.

[13] Rhouma Rhouma, Ercan Solak & Safya Belghith, (2010) "Cryptanalysis of a new substitution–diffusion based image cipher, Communications in Nonlinear Science and Numerical Simulation, Volume 15, Issue 7, Pages 1887-1892.

[14] M. Van Droogenbroeck & R. Benedett, (2002) "Techniques for a Selective Encryption of Uncompressed and Compressed Images", in Proceedings of Advanced Concepts for Intelligent Vision Systems (ACIVS) 2002, Ghent, Belgium.

[15] Jiang-Lung Liu (2006) "Efficient selective encryption for JPEG 2000 images using private initial table". Pattern Recognition, Volume 39, Issue 8, Pages 1509-1517.

[16] K. Sayood, (2000) "Introduction to Data Compression", 2nd edition, USA, Morgan Kauffman Publishers.

[17] Saeed Bahrami & Majid Naderi, (2013) "Encryption of multimedia content in partial encryption scheme of DCT transform coefficients using a lightweight stream algorithm", Optik - International Journal for Light and Electron Optics, Volume 124, Issue 18, Pages 3693-3700.

[18] G. Chen, Y. Mao, & C. K Chui, (2004) "A symmetric image encryption based on 3D chaotic maps," Chaos Soliton Fractals, vol. 21, pp. 749–761.

[19] Oussama Benrhouma •Houcemeddine Hermassi & Safya Belghith, (2013) "Security analysis and improvement of a partial encryption scheme," Multimedia Tools and Applications DOI 10.1007/s11042-013-1790-4.

AUTHORS

Akram BELAZI has received his engineering diplomat in "Telecommunication & Networks" in 2011 at the National Engineering School of Gabes, ENIG Tunisia and his Master degree in "Electronic Systems and Networks Communications" in 2013 at the Polytechnic School of Tunisia, EPT. He is now a Phd student at the Syscom Laboratry, ENIT Tunisia. His researcher domain is focused on the conception of partial encryption scheme for multimedia content and cryptanalysis of chaos-based cryptosystem

Oussama Benrhouma is a PhD student in the Syscom laboratory at the ENIT Ecole Nationale d'Ingénieurs de Tunis (ENIT). His domain of interest includes cryptography, Multimedia watermarking and steganography.

Houcemeddine Hermassi has received his engineering diploma in "Telecommunications & Networks" in 2005 from the National School of Engineering Gabès ENIG, Tunisia, and his MS degree in "Communication Systems" in 2010 from the National School of Engineering Tunis ENIT, Tunisia. He is now a PhD student at the Syscom Laboratory, ENIT Tunisia. His researcher domain is focused on the cryptanalysis and the conception of the new multimedia cryptographic approaches like the chaos-based cryptography and the DNA cryptography.

Prof. Safya Belghith has received his engineering diploma in "Electricity" (1981) and his D.E.A (1982) and the PhD degree (1985) in "Automatic and Signal Processing" from the High School of Electricity, Lab Signals & Systems, University Paris XI Orsay. In 1997, she received her Status Doctorate in "Physical Sciences" from the Faculty of Sciences Tunis FST with collaboration of the Laboratory Signals & Systems, High School of Electricity University Paris XI Orsay. She is now a Professor at the National School of Engineering Tunis ENIT, Tunisia and a senior researcher at SysCom Laboratory in the ENIT, Tunisia. His research domain is focused on the analysis of nonlinear systems and chaotic communication, the generation of the pseudo random sequences from chaotic systems and studying their performance in mobile radio communications particularly in a DS/CDMA and on the Synchronization of chaotic systems and its application to secure the transmission by chaotic carrier – Cryptography.