

An easy adapted image chaotic cipher to AWGN canal transmission

KHALFALLAH Ali, MBAYA Naim, BOUHLEL Mohamed Salim

Research Unit: Sciences and Technologies of Image and Telecommunications (SETIT),
Institut Supérieure de Biotechnologie
khalfallah.ali@laposte.net,
naim.mbaya@laposte.net,
medsalim.bouhlef@enis.rnu.tn

1. Introduction

Data digitization presents a great technical revolution. It allows a free and fast data processing. In fact, it is too easy to manipulate data. Moreover, transmission becomes faster. However, this flexibility in data processing menaces the intellectual propriety and confidential communication. In this paper, we are interested in safeguarding the image transmission into an AWGN canal. To ensure a safe transmission, many methods were proposed like watermarking [1-2], setganography [3] and cryptography [4-5]. We will focus on cryptography. Ciphering was the first technique of security used in the human history to ensure confidential communication [6-7]. This technique was adopted since the Roman Empire by Jules Cesar. Nowadays, cryptography is utilized in other applications. In fact, it is used for checking the integrity of transmitted data [8]. Moreover, this technique is used to know the source of transmitted data [9-11]. Now, many ciphering techniques have appeared like the RSA [12-13], the elliptic curve cipher (ECC) [14-15] and the chaotic cipher [16-17]. The cipher bloc and the decipher bloc can use the same key to encode and decode data. It's the secret key encryption. This kind of encoding is used in the chaotic cipher [18-19]. The ECC and the RSA use tow different keys: a key for encoding and another one for decoding [20]. This kind of cryptography is called public key encoding.

The cryptosystem should not be broken by crackers. An efficient cryptosystem should present a cipher text different from the plain one and should resist to cracker's attempts. On the other hand, we will utilize the cryptosystem in AWGN canal. This canal presents Gaussian noise and could yield to a failure in the deciphering bloc. Actually, the cryptography is very sensitive to perturbation. In fact, any change in the ciphered message yields to the failure of decoding level. Therefore, we need a adapted cryptosystem which ensures us robustness against crackers' attempts and noisy canal. Chaotic cipher is released through mixing a chaotic signal with a plain message [21].

2. Proposed method

2.1. The chaotic signal

The chaotic signal is based on non linear function. The chaotic generator presents also some retroactions (see fig. 1).

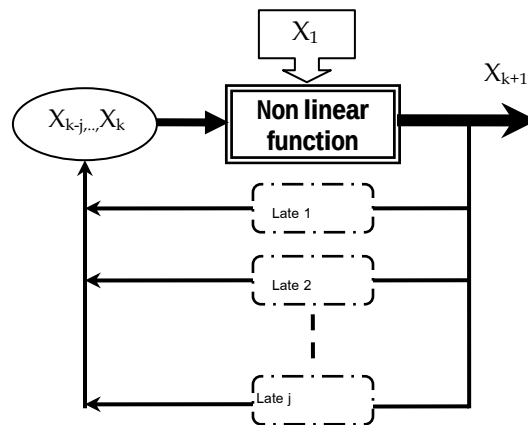


Fig. 1. Chaotic generator signal

The non linear function gives to generator a high sensitivity to the initial input. Moreover, the retroactions present in this architecture increase this sensitivity and make difficult the prediction of the future of the issued signal. It is the random feature of the chaotic signal. (See fig. 2).

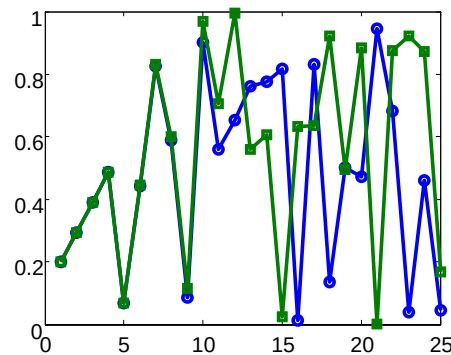


Fig. 2. Sensitivity of chaotic signal to initial input: $I_1=0.2$ (blue $-o-$) and $I_2=0.20001$ (green $-□-$)

According to figure 2, the initial input has a great effect on the evolution of the chaotic signal. In fact, the correlation rate between these two signals is equal to 0.1761 for 25 elements. This rate decreases to -0.0190 for 1000 elements signals.

Bearing in mind the configuration of the chaotic generator, we remark that the past issued values from the generator have an influence on its future behaviour. Therefore, any modifications in cipher text yields to a failed decipher text. However, knowing the chaotic generator configuration and the initial inputs this random signal could be reproduced. Consequently, the chaos signal is at the same time a random and determinist signal [22].

The chaos is used to explain various phenomena like bifurcation, weather, and it is, also, used in genetic algorithm and in the economic world. To use chaos we should ensure synchronization between utilized generators.

2.2. Chaotic cipher

Chaotic cipher is based on mixing the plain text with one or more chaotic signal(s) [23]. It is a symmetric key cryptosystem. In fact, we use the same key in the cipher bloc and the decipher bloc. The decipher key is made up of the parameters and the initial input of the chaotic generator. Consequently, using the decipher key, we could synchronize the chaotic generator of the cipher bloc and the decipher one. Thanks to this synchronization, we could reproduce the same chaotic generator in the two blocs of the cryptosystem. So, we could decipher the received message.

In classical chaotic cipher, the cipher message element depends on in the parameters of chaotic generator and the previous cipher elements.

This dependence on previous cipher elements engenders a great sensitivity of the cryptosystem to any distortion. On the one hand, this sensitivity allows a good protection against cracker's attacks. On the other hand, it presents a great problem when data are transmitted on a noisy canal.

2.3. Example of classic chaotic cipher

We present, here, an example of classic image chaotic cipher. This cryptosystem is based on the function Modulus. The cipher bloc present five retroactions used with five different real coefficients. The cipher image is obtained using the Modulus function. In fact, the plain image element is added to the five previous ciphered image elements magnified respectively with their appropriate coefficients. The cipher result is the sum Modulus 256 (see fig. 3).

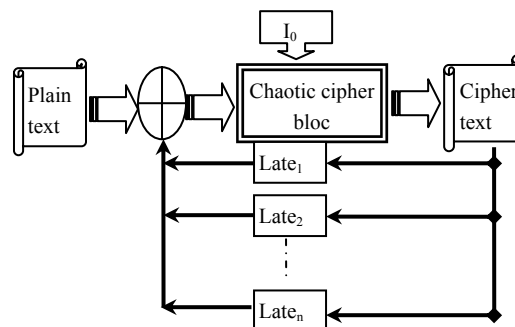


Fig. 3. Architecture of classic chaotic cipher

Looking at the plain image (see fig. 4) and the ciphered image (see fig. 5), we remark that there is a great difference between them. Moreover, they have different histograms. The histogram of the ciphered image presents an equalized histogram (see fig. 6-7). This feature presents another obstacle for crackers.



Fig. 4. Image test(A)

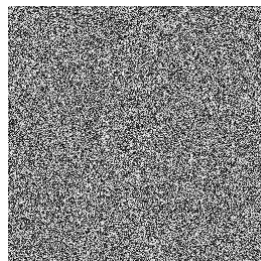


Fig. 5. image B Ciphered image(A)

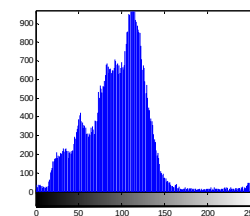


Fig. 6. Histogram of image A.

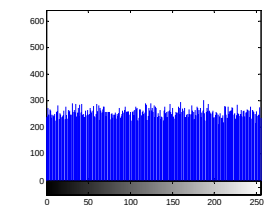


Fig. 7. Histogram of the ciphered image

The key of the cryptosystem is made up of six real which present the chaotic generator retroaction coefficients and the chaotic generator initial input. The established results are obtained with this key $K=[5 \ 1.01 \ 0.003 \ 5.1 \ 3.3 \ 2.06]$ which presents a large space key.

To study the performances of the cryptosystem we have used two other cipher keys. C is the image ciphered with the key $K_2=[5.01 \ 1.01 \ 0.003 \ 5.1 \ 3.3 \ 2.06]$. D is the image test ciphered with the key $K_3=[5 \ 1.01 \ 0.003 \ 5.1 \ 3.3 \ 2.061]$. Table 1 and table 2 summarize the comparison between ciphered images and the plain one. In fact, any modification in the ciphering key yields to a very different ciphered image.

	A	B	C	D
A	1	0.0015	0.0027	0.0001
B	0.0015	1	0.0006	0.0033
C	0.0027	0.0006	1	-0.0011
D	0.0001	0.0033	-0.0011	1

Tab. 1. Sensitivity to changing ciphering key sensitivity (correlation table)

	A	B	C	D
A	Inf	9.06	9.10	9.08
B	9.06	Inf	7.75	7.76
C	9.10	7.75	Inf	7.76
D	9.08	7.76	7.76	Inf

Tab. 2. Sensitivity to changing ciphering key sensitivity (PSNR table)

Moreover, the deciphered bloc is very sensitive to changing key. The obtained results demonstrate that using the K to decipher the image yields to successful deciphering. On the other hand, using other keys like K_2 and K_3 which present a tiny variation applied to the key K yields to a failure in on the decipher operation (see fig. 8-9).

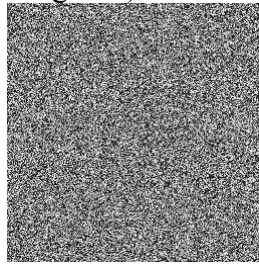


Fig. 8. Image B deciphered using K_2

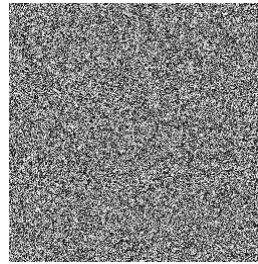


Fig. 9. Image B deciphered using K_3

These results are backed by correlation rates and PSNRs (see tab. 3-4).

	A	B	C	D
A	1	0.0015	0.0027	0.0001
B	0.0015	1	0.0006	0.0033
C	0.0027	0.0006	1	-0.0011
D	0.0001	0.0033	-0.0011	1

Tab. 3. Sensitivity to changing deciphering key sensitivity (correlation table)

	A	B	C	D
A	Inf	9.06	9.10	9.08
B	9.06	Inf	7.75	7.76
C	9.10	7.75	Inf	7.76
D	9.08	7.76	7.76	Inf

Tab. 4. Sensitivity to changing deciphering key sensitivity (PSNR table)

But to have an efficient cryptosystem it should be robust against attackers. Therefore, we tested this cryptosystem against known ciphered text attack. We suppose that we use this cipher function.

$$I_{\text{cph}} = (I_{\text{plain}} + \text{Mask}_{\text{Ch}}) \bmod 256 \quad (1)$$

Where I_{cph} is the ciphered image, I_{plain} is the plain image and Mask_{Ch} is chaotic mask. So, the chaotic mask Mask_{Ch} is computed using this equation

$$\text{Mask}_{\text{Ch}} = (I_{\text{cph}} - I_{\text{plain}}) \bmod 256 \quad (2)$$

We present in figure 10 the chaotic mask computed using the image test and its ciphered image. We try to recover the image Lena (see fig. 11).

We have the ciphered image of Lena (see figure 12). We use the chaotic mask to crack it. We remark that this attempt yield to a failure (see fig. 13).

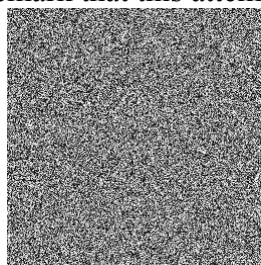


Fig. 10. Mask_{Ch}

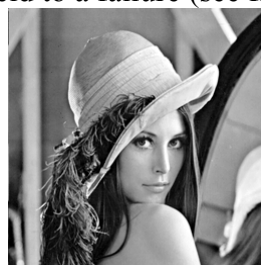


Fig. 11. Image Lena

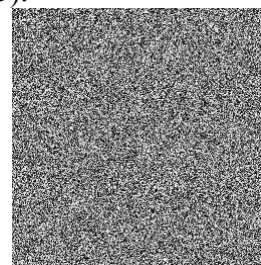


Fig.12. Ciphered image Lena

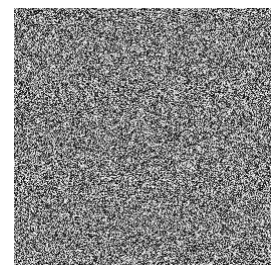


Fig. 13. Failed crack attempt

Finally, we could consider that the studied cryptosystem is efficient. We try to apply it for transmitted images on a noisy AWGN canal.

We present on figure 14, the influence of the AWGN canal SNR on transmitted images. The study was realized on 30 images for different SNR ($\text{SNR} = [0.25, 0.5, 1, 2, 4, 8]$) images are transmitted on a AWGN canal using phase shift keying modulation (PSK) using a 4 alphabet size. Color blue ($\text{—}\circ\text{—}$) refer to the plot of mean PSNR for plain image and transmitted plain images. The mean PSNR for ciphered images and transmitted cipher image is referred to by the color red ($\text{—}\text{+}\text{—}$). The SNR of the transmission canal have the same effect on ciphered images and plain ones. But, the deciphering of the noisy transmitted encoded images yields to a failure decoding step. As shown on the figure 14, the mean PSNR of deciphered transmitted images and the plain ones is too low for different SNR values (green plot $\text{—}\square\text{—}$).

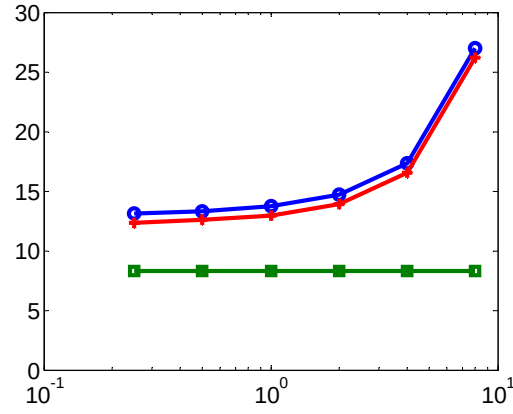


Fig. 14. Mean PSNR Vs SNR of the AWGN canal

2.4. The proposed method

To have a chaotic cryptosystem adapted to transmission canal noise, we should separate the chaotic signal and the plain image. In other words, the cipher element image should not depend on previous ciphered image elements. Therefore, we suggest that we delete retroactions on the coding bloc. So, we propose to mix chaotic signal with plain image without applying retroaction on cipher computing. In the first step, we suggest using the Modulus 256 function (Method 1).

$$I_{cph} = (I_{plain} + I_{ch}) \text{ Mod } 256 \quad (3)$$

Where, I_{ch} is chaotic signal reshaped to a matrix having the image size.

Then, we apply the known ciphered text attacks. We start by extracting the Modulus mask (see fig. 4, 15, 16). As shown in figure 17 and figure 18 the proposed ciphering method is not robust against this crack attack therefore we could not adopt it.

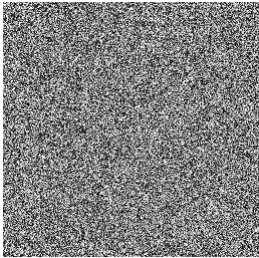


Fig. 15. Ciphered image test using Method 1

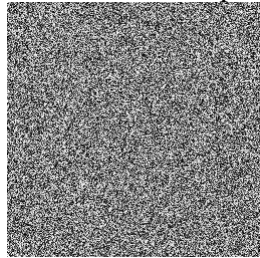


Fig. 16. Extracted Mask for Method 1

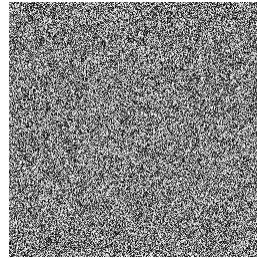


Fig. 17. Ciphered image Lena using method 1.



Fig. 18. Successful crack attack

We replace in the second method function Modulus by XOR function. The ciphering function becomes:

$$I_{cph} = I_{plain} \text{ XOR } I_{ch} \quad (4)$$

We tested it against known ciphered text attack. The obtained results (using a XOR mask) yield to a successful cracker's attempt.

After that, we tested using two different chaotic signals. We test for two ciphering equations:

$$I_{cph} = ((I_{plain} + I_{ch1}) \text{ Mod } 256 + I_{ch2}) \text{ Mod } 256 \quad (5)$$

$$I_{cph} = (I_{plain} \text{ XOR } I_{ch1}) \text{ XOR } I_{ch2} \quad (6)$$

These two approaches presented a non robust cryptosystem against known ciphered text attack.

Finally, we suggested using two different chaotic signals (I_{ch1} and I_{ch2}) mixed with the plain image using two different functions (see fig. 19). At first time, we mixed the I_{ch1} with the plain image I_{plain} using the logical function XOR. The obtained result would be added to I_{ch2} . Finally, we applied the non linear function Modulus 256 to the result. We obtain, then, the ciphered image [24].

$$M_{crp} = ((M_{clr} \text{ XOR } Ch_1) + Ch_2) \text{ Mod } 256 \quad (7)$$

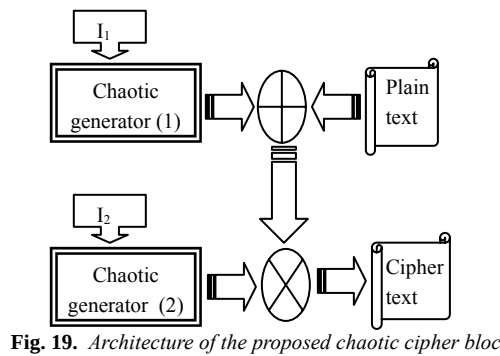


Fig. 19. Architecture of the proposed chaotic cipher bloc

To decode the encoded image, we should firstly synchronize the chaotic generators of the decipher bloc with those utilized in the cipher bloc by using the same parameters and the same initial inputs. Thus, we obtain the two chaotic signals I_{ch1} and I_{ch2} . Then, we subtract I_{ch2} from the encoded image and we apply Modulus 256 function. Finally, we mix the obtained image with I_{ch1} using the logic function XOR to have the decoded image.

3. Analysis

We test our new approach using an image test bank containing 30 different gray scale images. Each image has 256 x 256 size.

We begin by a visual analysis. Looking at the ciphered image and the plain one, we see that there is a great difference between them (see fig. 4, 20).

Moreover, the ciphered image and the plain one have two different histograms (see fig. 6, 21). In addition, the ciphered image presents an equalized histogram (see fig. 21) which makes it difficult to know the deciphering key.

After that, we apply our new encoding scheme on the whole image test bank. We see that there is a great difference between plain images and ciphered images. This difference is demonstrated, also, by the low correlation rates between plain images and their equivalent ciphered ones (see fig. 22) and the low PSNR (see fig. 23) too.

To cipher the plain image, we should produce two different chaotic signals using the chaotic generator. In fact, we use the same chaotic generator with different initial inputs and different parameters. I_{ch1} is produced by the chaotic signal with I_1 as initial input and K_{ch1} as parameters of the chaotic generator which defines $K_{MCh1} = \{I_1=21.7, K_{ch1} = [1.01 \ 0.003 \ 5.1 \ 3.3 \ 2.06]\}$. On the other hand, I_{ch2} is produced using $K_{MCh2} = \{I_2= 6.01, K_{ch2} = [3.04 \ 2.015 \ 1.204 \ 0.0026 \ 7.14]\}$; where I_2 is the initial input of the chaotic generator and K_{ch2} is its parameters}. So, the ciphering deciphering key of cryptosystem is $K = K_{MCh1} \cup K_{MCh2} = \{21.7, 1.01, 0.003, 5.1, 3.3, 2.06, 6.01, 3.04, 2.015, 1.204, 0.0026, 7.14\}$.

In the second step we test our new approach by changing the ciphering key into two keys different from K:

$$Key_1 = \{21.7000001, 1.01, 0.003, 5.1, 3.3, 2.06, 6.01, 3.04, 2.015, 1.204, 0.0026, 7.14\}.$$

$$Key_2 = \{21.7, 1.01, 0.003, 5.1, 3.3, 2.06, 6.01, 3.04, 2.015, 1.204, 0.0026, 7.1400001\}.$$

We name I_c (see fig. 20) the ciphered image of the image test I (see fig. 4) by our new approach using the key K . I_{c1} and I_{c2} are the ciphered images of the image test I using respectively the keys key_1 and key_2 (see fig. 24-25). The established results in table 5 present a low correlation rate between the plain image and the deciphered one. This rate is also low between deciphered images for different keys. Moreover, the obtained PSNR is low (see tab. 6).

These results prove that the adopted cryptosystem is very sensitive to any change in the ciphering key. On the other hand, we decipher I_c using the keys K , Key_1 and Key_2 to have I_d , I_{d1} and I_{d2} . Visually, we remark that, using a false deciphering key yields to a failure decipher (see fig. 26-28). Moreover, the correlation rate and the PSNR between deciphered images with different keys presenting a tiny variation are too low. So, our approach is very sensitive to the deciphering key.

This sensitivity to ciphering key and deciphering key explains the high large of the key space of the proposed cryptosystem. In addition our encoding scheme has a key made up of 12 real. So, its key space is too large to be broken by the brutal force attack. In reality, we use MATLAB 7.04 in our study. This mathematic tool codes real in 8 bytes. According to this coding, our space key has 96 bytes large which means 768 bits large.

After that, we test the proposed cryptosystem against the known ciphered text attack. The ciphering scheme utilizes the logic XOR function and the non linear function Modulus. Therefore, we propose to use two extracted masks. The first one named MaskXor is based on the XOR function (see fig. 30) and the second one named MaskMod is based on the Modulus function (see fig. 31). These masks are extracted from the test plain image (see fig. 4) and its equivalent ciphered image (see fig. 20). Using these masks, the crack attempts yield to a failure (see fig. 32-33).

In addition to these classic ways of attacking, we propose other equations to try breaking the suggested cryptosystem following the equations bellow:

$$IMX = (IX - \text{MaskMod}) \bmod 256 \quad (7)$$

Where, IX is the obtained image after crack attempt with MaskXor (see fig 33).

$$IXM = IM \mathbf{XOR} \text{MaskXor} \quad (8)$$

Where, IM is the obtained image after crack attempt with MaskMod (see fig. 32).

$$IMX0 = (IX - IM) \bmod 256 \quad (9)$$

$$IXM0 = IM \mathbf{XOR} IX \quad (10)$$

The established results shown in figures 34-37 demonstrate that our approach could not be broken by known ciphered text attack. Moreover, the cracked images have a low rate correlation and a low PSNR with the plain image Lena (see tab. 9-10).

Finally, we test our cryptosystem for transmitted encoded images in an AWGN canal using a PSK modulation. The cryptosystem is constituted by two blocs. The plain text is ciphered and then transmitted. The received images are noisy due to the noise presented by the canal. This noise is quantified by the SNR of the transmission canal. Finally, we decode the received image and we compare it to the transmitted plain image to study the effect of the canal noise on the proposed cipher scheme. To have an objective judgement, we study, also, the effect of this noisy transmission on the classic cryptosystem. The established results (see fig. 38-41) demonstrate that the classic coding scheme is very sensitive to noise transmission canal. In fact, transmitted images could be truly deciphered using the classic way only if it does not present any change. This condition is ensured for an AGWN canal with an SNR more than 16dB. Otherwise, the correlation rate of the received plain image and the plain image is near to the correlation rate of the plain image and the received decode image using the adapted cryptosystem. We remark, also, that the PSNRs are near too. This result High lights our contribution to cryptography.

These good performances on noisy transmission canal are due to the deletion of retroactions on the cipher bloc. In fact, this bloc separates the chaotic generators and plain text to obtain the ciphered image. So, the ciphered image element depends only to the values issued from the two chaotic generators and the plain image element. Therefore, no distorted ciphered transmitted image element could be decoded correctly. Consequently, only modified pixel will be decoded wrongly. On the other hand, the presence of retroaction in classic chaotic cipher engenders a great mistake on the decipher bloc if any pixel of the coded image is changed.

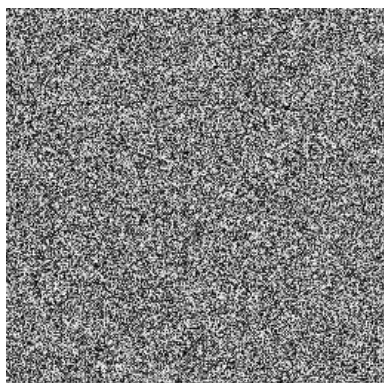


Fig. 20. Ciphered image test using the adapted chaotic cryptosystem

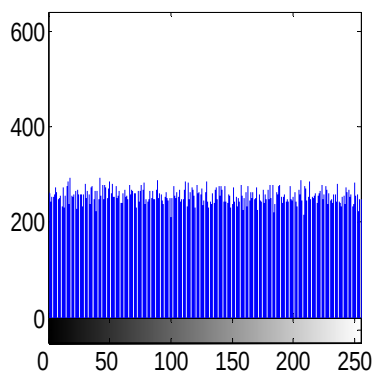


Fig. 21. Histogram of the adapted ciphered image

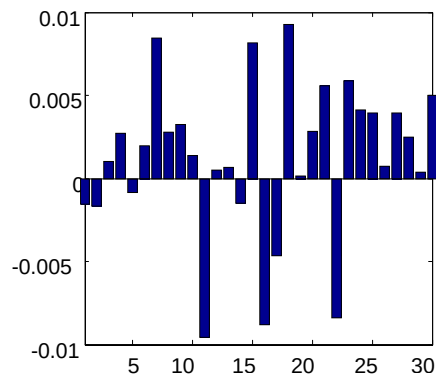


Fig. 22. Correlation rate of plain image and adapted image Vs image number

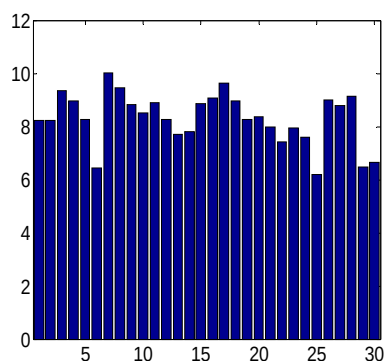


Fig. 23. PSNR (plain image, ciphered image) Vs image number using the adapted cryptosystem

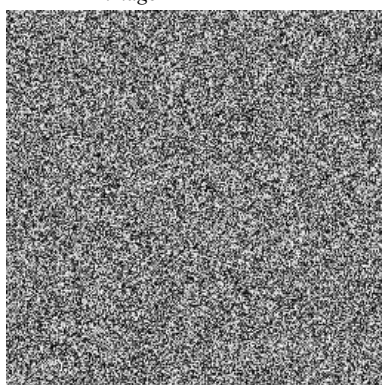


Fig. 24. Ciphered image test using the adapted chaotic cryptosystem utilizing Key₁

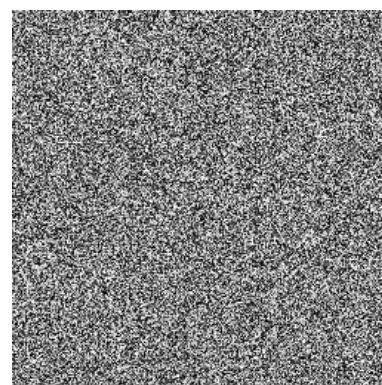


Fig. 25. Ciphered image test using the adapted chaotic cryptosystem utilizing Key₂

	lc	lc ₁	lc ₂	I
lc	1	0.0001	-0.0076	-0.0088
lc ₁	0.0001	1	0.0031	-0.0035
lc ₂	-0.0076	0.0031	1	-0.0024
I	-0.0088	-0.0035	-0.0024	1

Tab. 5. Correlation table for sensitivity to changing ciphering key on the adapted cryptosystem

	lc	lc ₁	lc ₂	I
lc	Inf	7.75	7.72	9.06
lc ₁	7.75	Inf	7.77	9.06
lc ₂	7.72	7.77	Inf	9.07
I	9.06	9.06	9.07	Inf

Tab. 6. PSNR table for sensitivity to changing ciphering key on the adapted cryptosystem

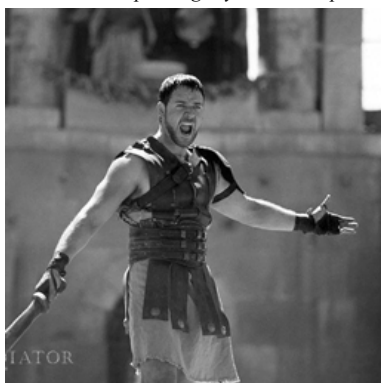


Fig. 26. lc deciphered using the key K

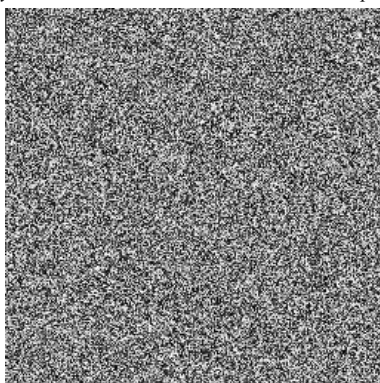


Fig. 27. lc deciphered using the key Key₁

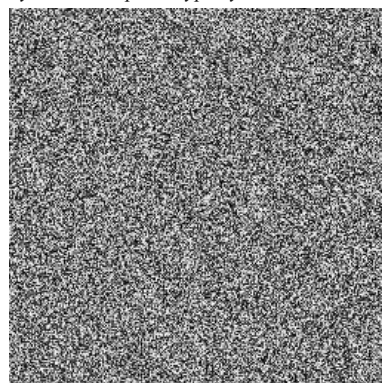


Fig. 28. lc deciphered using the key Key₂

	Id	Id ₁	Id ₂	I
Id	1	-0.0013	-0.0029	1
Id ₁	-0.0013	1	0.0010	-0.0013
Id ₂	-0.0029	0.0010	1	-0.0029
I	1	-0.0013	-0.0029	1

Tab. 7. Correlation table for sensitivity to changing deciphering key on the adapted cryptosystem

	Id	Id ₁	Id ₂	I
Id	Inf	9.07	9.08	Inf
Id ₁	9.07	Inf	7.75	9.07
Id ₂	9.08	7.75	Inf	9.08
I	Inf	9.07	9.08	Inf

Tab. 8. PSNR table for sensitivity to changing deciphering key on the adapted cryptosystem

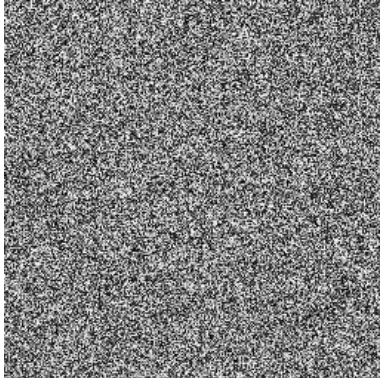


Fig. 29. Image Lena ciphered by the proposed cryptosystem

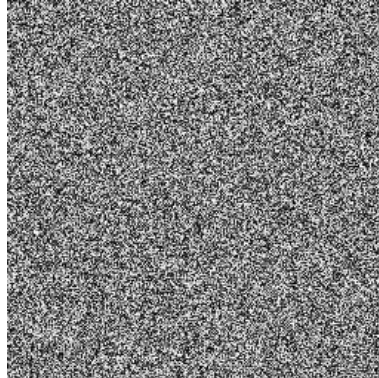


Fig. 30. Extracted MaskXOR for the proposed cryptosystem

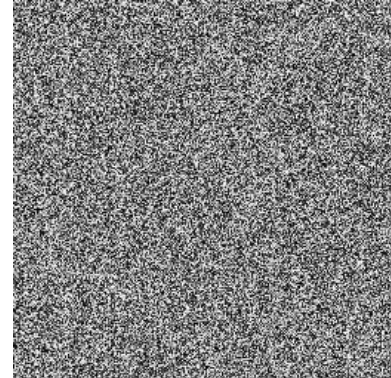


Fig. 31. Extracted MaskMod for the proposed cryptosystem



Fig.32. Failed crack attempt by MaskMod

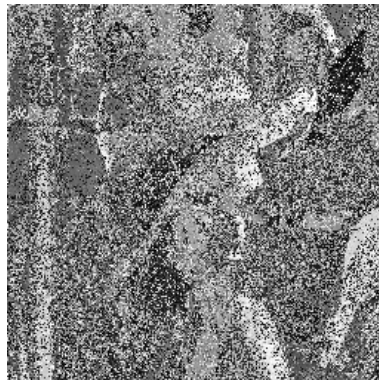


Fig. 33. Failed crack attempt by MaskXor

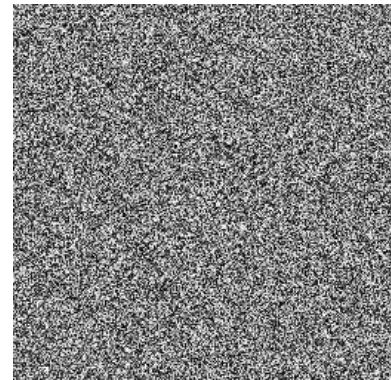


Fig. 34. Failed crack attempt using eq 7

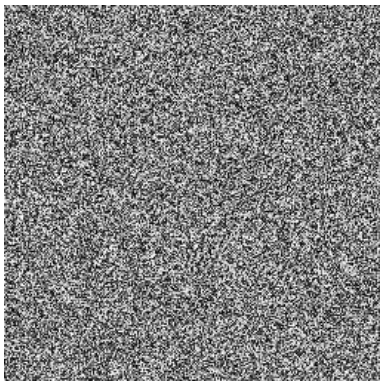


Fig. 35. Failed crack attempt using eq 8.

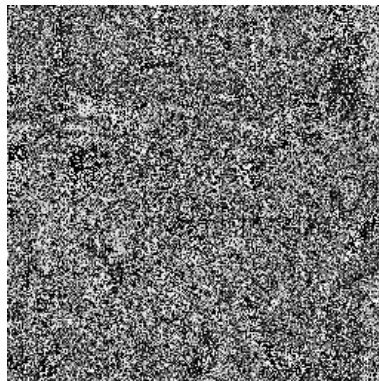


Fig. 36. Failed crack attempt using eq 9.

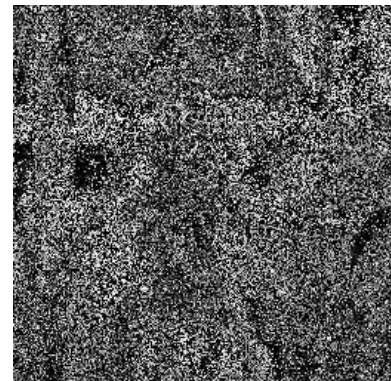


Fig. 37. Failed crack attempt using eq 10.

	IM	IX	IMX	IXM	IMX0	IXM0
Lena	0.2608	0.2732	-0.0064	0.0008	-0.0164	-0.0088

Tab. 9. Correlation table for known ciphered text attack

	IM	IX	IMX	IXM	IMX0	IXM0
Lena	9.71	9.74	8.22	8.24	6.98	7.19

Tab. 10. PSNR table for known ciphered text attack.

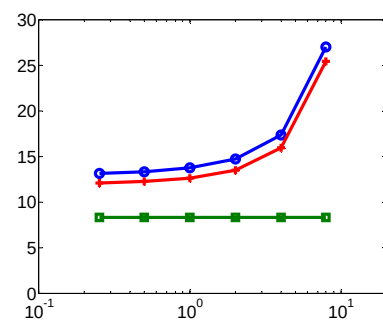


Fig. 38. Influence of the SNR Canal on transmitted image (mean PSN)

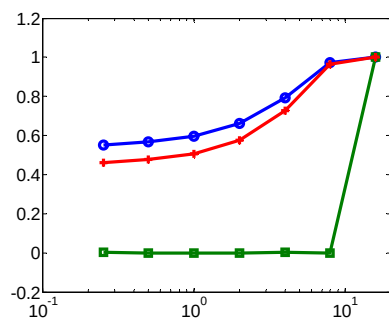
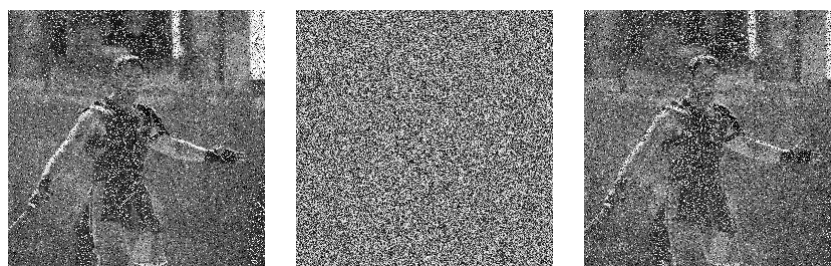
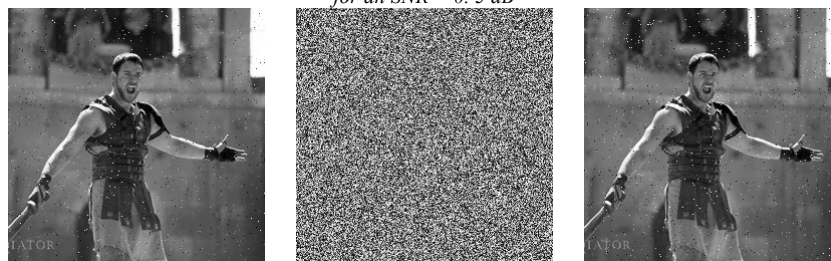


Fig. 39. Influence of the SNR Canal on transmitted image (mean correlation rate)



a. Plain image **b. Classic scheme** **c. Adapted scheme**

Fig. 40. Influence of the transmission on the plain image and decoded images for an SNR = 0.5 dB



a. Plain image **b. Classic scheme** **c. Adapted scheme**

Fig. 41. Influence of the transmission on the plain image and decoded images for an SNR = 8 dB

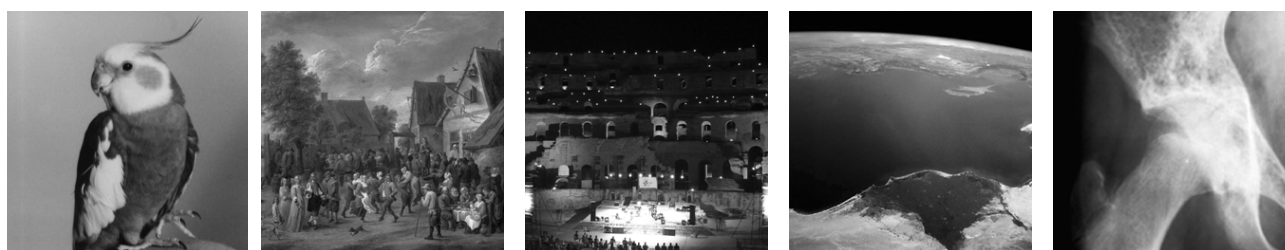


Fig. 42. Example of images belonging to the image test bank

4. Conclusion

We have studied in this paper a new scheme of cryptosystem. Our new approach is based on chaos. In fact, the cipher bloc is made up of two different chaotic generators. These two generators are based on the non linear function modulus with five retroactions. The two generators generate two different chaotic signals. Indeed, we used different parameters and initial inputs for the generators. To obtain the cipher image we mix the plain image with the first issued chaotic signal using the logic function XOR. Finally, we add the result to the second issued chaotic signal and we apply the non linear function Modulus. The ciphered images are too different from the plain ones. Unlike the plain image, ciphered images have an equalized histogram. This result makes it difficult for crackers to break the proposed cryptosystem. Moreover, this cryptosystem has a 768 bites large key space which presents a great challenge for the brutal force attack. The ciphered key is made up of the parameters and initial input of each chaotic generator used in the coding bloc. This large key space could be increased by adding other retroaction parameters in each chaotic generator. After that, we tested our approach against the known ciphered text attack. The test is based on a XOR mask or Modulus mask or both of them. The choice of these masks is argued by the use of the XOR and Modulus on the coding function. The test is established by six different attempts based on those functions. The obtained results confirm that our cryptosystem is robust against this attack.

These performances are due to random and determinist aspect of the chaos and its high sensitivity to the initial input and the parameters of the chaotic generator.

Compared to the classic chaotic cipher we have increased the key space large and ensure a good decoding for transmitted ciphered image on a noisy transmission canal. To guarantee this performance, we have deleted the retroactions joining the current ciphered image pixel to the previous ciphered pixels image. Finally, we have compared transmitted plain images to decoded transmitted ones on a noisy transmission. We have used a 4 alphabet PSK modulation on an AWGN transmission canal. The established results prove that distortion engendered by the canal transmission have nearly the same effect on plain images and ciphered images.

References:

- [1] FAHMI KAMMOUN, ALI KHALFALLAH, MOHAMED SALIM BOUHLEL. New Scheme of Digital Watermarking Using an Adaptive Embedding Strength Applied on Multiresolution Filed by 9/7 Wavelet, *Inc. International Journal of Imaging Systems and Technology*, 16, 2006, pp 249-257.
- [2] CHAW-SENG WOO, JIANG DU, AND BINH PHAM. Multiple Watermark Method for Privacy Control and Tamper Detection in Medical Images. *APRS Workshop on Digital Image Computing (WDIC 2005)*, ISBN 0-9580255-3-3, Griffith University, Southbank, Brisbane, Australia, 21 February 2005.
- [3] M. ABOLGHASEMI, H. AGHAEINIA AND K. FAEZ. Data Hiding Detection Based on DWT and Zernike Moments. *International Conference: Sciences of Electronic, Technologies of Information and Telecommunications*, March 25-29, 2007 – TUNISIA (SETIT 07).
- [4] LAURENT LARGER, JEAN-PIERRE GOEDGEBUER, Encryption using chaotic dynamics for optical telecommunications, *C.R. Physique* 5, pp. 609-611, 2004
- [5] VIPUL GUPTA, DOUGLAS STEBILA AND SHEUELING CHANG SHANTZ. Integrating Elliptic Curve Cryptography into the Web's Security Infrastructure. *the 13th international World Wide Web conference on Alternate track papers & posters*, pp 402-403, New York, NY, USA, May 19 - 21, 2004.
- [6] CONSTANTIN GROZEA, DAN LAURENTIU GRECU. Applications Of Chaos Theory In Numerical Datastreams Cryptography. Mathematical Model And Implementation Method. *International Scientific Conference Security and Protection of Information 2003*, Brno, Czech, April 28 – 30, 2003.
- [7] CRAIG GENTRY, PHILIP MACKENZIE, ZULFIKAR RAMZAN. Password Authenticated Key Exchange Using Hidden Smooth Subgroups. *12th ACM conference on Computer and communications security 2005*, pp 299-309, Alexandria, VA, USA, November 07 - 11, 2005.
- [8] RICH SCHLESINGER. A Cryptography Course for Non-Mathematicians. *the 1st annual conference on Information security curriculum development*, Kennesaw, Georgia October 08 - 08, 2004.
- [9] UELI MAURER. The Role of Cryptography in Database Security. In *proceeding of the 2004 ACM SIGMOD international conference on Management of data (SIGMOD'04)*, pp5-10, ISBN:1-58113-859-8, Paris, France June 13 - 18, 2004.
- [10] SELIM G. AKL and PETER D. TAYLOR. Cryptographic Solution to a Problem of Access Control in a Hierarchy, *ACM Transactions on Computer Systems (TOCS)*, Volume 1, Issue 3, pp293-248, ISSN: 0734-2071, New YORK, NY, USA, August 1983.
- [11] VIPUL GUPTA, DOUGLAS STEBILA AND SHEUELING CHANG SHANTZ. Integrating Elliptic Curve Cryptography into the Web's Security Infrastructure. *the 13th international World Wide Web conference on Alternate track papers & posters*, pp 402-403, New York, NY, USA, May 19 - 21, 2004.
- [12] FU-CHI CHANG AND CHIAJIU WANG. Architectural Tradeoff in Implementing RSA Processors. *ACM SIGARCH Computer Architecture News, Volume 30, Issue 1*, pp 5-11, ISSN:0163-5964, ACM Press New York, NY, USA, March 2002
- [13] CHENGHUI LU, ANDRE L. M. DOS SANTOS, FRANCISCO R. PIMENTEL. Implementation of Fast RSA Key Generation on Smart Cards. *Symposium on Applied*

Computing SAC'02, Madrid, Spain, March 11 - 14, 2002.

- [14] ZOYA DYKA AND PETER LANGENDOERFER. Area Efficient Hardware Implementation of Elliptic Curve Cryptography by Iteratively Applying Karatsuba's Method. *Conference on Design, Automation and Test in Europe (DATE'05)*, Munich, GERMANY, March 07-11, 2005.
- [15] KOSSI D. EDOH. Elliptic Curve Cryptography: Java Implementation. *the 1st annual conference on Information security curriculum development*, Kennesaw, Georgia October 08 - 08, 2004.
- [16] TZOUVELI PARASKEVI, NTALIANIS KLIMIS, KOLLIAS STEFANOS. Security of Human Video Objects by Incorporating a Chaos-Based Feedback Cryptographic Scheme. *The 12th annual ACM (Association for Computing Machinery) international conference on Multimedia*, New York, NY, USA October 10 - 16, 2004.
- [17] SHUJUN LI, XUAN ZHENG, XUANQIN MOU and YUANLONG CAI. Chaotic encryption scheme for real-time digital video. *In Real-Time Imaging VI, Proceedings of SPIE*, vol. 4666, pages 149-160, 2002.
- [18] ALI KHALFALLAH, FAHMI KAMMOUN, CHRISTIAN OLIVIER & MOHAMED SALIM BOUHLEL. Evaluation du Crypto-Tatouage Semi-Aveugle dans le Domaine Multi-résolution à Base d'Ondelette 5/3 : Notion de Signature Associée et Cryptage Chaotique. *International Conference: Sciences of Electronic, Technologies of Information and Telecommunications*, March 25-27, 2004 – TUNISIA (SETIT 07).
- [19] NADA REBHI, MOHAMED AMINE BEN FARAH, ABDENNACEUR KACHOURI and MOUNIR SAMET. Analyse De Sécurité d'une Nouvelle Méthode De Cryptage Chaotique. *International Conference: Sciences of Electronic, Technologies of Information and Telecommunications* March 25-27, 2004 – TUNISIA (SETIT 07).
- [20] A. CILARDO, A. MAZZEO, N. MAZZOCCA, L. ROMANO. A Novel Unified Architecture for Public-Key Cryptography. *conference on Design, Automation and Test in Europe (DATE'05)*, Munich, GERMANY, March 07-11, 2005.
- [21] ZBIGNIEW KOTULSKI, JANUSZ SZCZEPAŃSKI. Discrete chaotic cryptography (DCC). New method for secure communication, *the 11th Workshop on Nonlinear Evolution Equations and Dynamical Systems NEEDS'97*, OAK, Kolymbari near Chania, Crete, Greece; 18-28 June, 1997.
- [22] PAUL MANNEVILLE. Dynamique non linéaire et chaos. *Ecole d'été de physique e2phy*, Pôle Scientifique de Paris-Sud , 23 au 26 Août 2005.
- [23] KRISTINA KELBER and WOLFGANG SCHWARZ. General Design Rules for Chaos-Based Encryption Systems. *the International Symposium on Nonlinear Theory and its Applications (NOLTA2005)*, Bruges, Belgium, October 18-21, 2005.
- [24] ALI KHALFALLAH1, KHALED BRAHIM AND CHRISTIAN OLIVIER,. A New Approach To Encrypted Semi-Blind Watermarking in Multiresolution Field by 9/7 Wavelet. *In proceedings of the International Conference on E-Medical Systems*, Fez, Morocco, October 24 -26, 2007, pp 52-60

About Authors



Ali KHALFALLAH

was born in Rouen (France) in January 1980. He received the Diploma of Engineer on Electricity from the National Engineering School of Sfax-TUNISIA (ENIS) in 2003. He obtained the Diploma of Master on Electronics from the National Engineering School of Sfax-TUNISIA (ENIS) in 2004, where, he is currently pursuing the Doctorate. Currently, he is a Research member in the Research Unit of Sciences and Technologies of Image and Telecommunications (SETIT). He is an assistant teacher in the Higher Institute of Biotechnology Sfax –TUNISIA (ISBS). His research interests include digital Watermarking, Cryptography and image processing. He is member of the organization committee in the international conference: Sciences of Electronic, Technologies of Information and Telecommunication SETIT'05 and the organization Chairman of the international conference: Sciences of Electronic, Technologies of Information and Telecommunication SETIT'07.



Naim MBAYA

was born in Chebba (TUNISIA) in August 1981. He received the Diploma of Engineer on Electricity from the National Engineering School of Sfax-TUNISIA (ENIS) in 2007. He is a Research member in the Research Unit of Sciences and Technologies of Image and Telecommunications (SETIT). He is member of the organization committee in the international conference: Sciences of Electronic, Technologies of Information and Telecommunication SETIT'07.



Pr. Mohamed Salim BOUHLEL

is a professor and Head of Biomedical imagery Department in the Higher Institute of Biotechnology Sfax (ISBS).He received in 1999 the golden medal with the special mention of jury in the first International Meeting of Invention, Innovation and Technology (Dubai). He is the Chairman of the international conference: Sciences of Electronic, Technologies of Information and Telecommunication: (SETIT 2003, SETIT 2004, SETIT 2005, SETIT 2007 and SETIT 2009), the Chairman of the international conference: the International Conference on E-Medical Systems (E-MediSys 2007 and E-MediSys 2008) and member of the program committee of a lot of international conferences.