Combining Chaotic Encryption and Frequency Watermarking for Prior and Ahead Image Securing

Hassen Seddik
ESSTT, 5 Av. Taha Hussein, 1008, Tunis, Tunisia

Ben Braiek Ezzeddine
ESSTT, 5 Av. Taha Hussein, 1008, Tunis, Tunisia

ABSTRACT
Applying cryptographic techniques in the field of 2D signal processing is an attractive approach in recent years. Different methods are proposed to ensure prior data protection. Symmetric block encryption schemes, designed on two-dimensional chaotic maps, are efficient and secure for real-time image encryption. In the case of numeric data, the encrypted information can be easily intercepted in order to be revealed. This creates a need to offer a posterior protection. In this paper a method combining chaotic encryption system with frequency watermarking is presented. The proposed technique is divided in two steps. In the first step, it consists in applying a modified Tao algorithm based chaotic map with higher complexity and applicable for all images sizes. The encrypted data is then hidden by coding it in the frequencies DCT coefficients of a transformed second image. The proposed approach presents more security and reliability for any kind of image data.

Keywords
Encryption, watermarking, security, image

1. INTRODUCTION
Encryption is used to securely transmit data in open networks. Each type of data presents a relative importance and specially images; therefore different techniques should be used to protect confidential image data from unauthorized access or modification [6]. Even after enforcing the protection of personal information in April 2005, many cases of information leakages have been reported. Among those cases paper based-media is still listed as the major source of information leakage [5]. Most of the available encryption algorithms are mainly used for textual data and may not be suitable for multimedia data such as images. In real 2D signal many constraints are considered. In most of the natural images, the values of the neighboring pixels are strongly correlated (i.e. the value of any given pixel can be reasonably predicted from the values of its neighbors) [7]. In order to disperse this correlation and break the relation between pixels we choose to apply a modified Tao algorithm based chaotic map to introduce a non deterministic behavior to the processed data. The encrypted data is then watermarked and hidden by spreading it on the frequency coefficient of a DCT transformed 2D support [8]. The Tao algorithm id modified to be able to be applied to all images sizes and its complexity is also increased. Combined with watermarking [11] to offer an ahead protection to the prior encrypted data, maximizes the security to the proposed scheme [13]. When the image holding the encrypted data is transmitted, the inverse process is applied by extracting the encrypted data and decrypting it to obtain the original image without any loss [12]. In the following section the proposed algorithm is presented and the results are commented and detailed.

2. PROPOSED TECHNIQUE BASED MODIFIED TAO ALGORITHM

2.1 The logistic map
This algorithm presents a block-crypto system based on chaotic map iteration [2]. This map uses a polynomial iteration that diverges iteratively to a chaos behavior through dynamic non linear equations [1]. The mathematical recurrence is introduced using the following equation:

$$\tau(x_n) = x_{n+1} = a x_n (1 - x_n) \ with \ x_n \in [0,1] \quad (1)$$

Where a is a parameter that controls the map behavior. It is chosen such as it introduces the chaotic activity to the equation (1). In this work the choice of this parameter is as follows: $(3.57 < a < 4)$. A preliminary study of the logistic map permit to deduce that the chaos appears for this range of variation of a. x is a real that belongs to the range $[0\ 1]$, and x_0 represents the initial value such as $0 < x_0 < 1$ [1].

2.2 Generation of a chaotic signal by iterating the Logistic-Map
After iterating the equation (1) 70 times we deduce that the map diverges and presents a chaotic behavior. The values of a and x_0 are fixed as follows:

$x_0 = 0.1775$ and $a = 3.9999995$. Figure 1 illustrates the map variation within 70 iterations and the chaotic divergence of the system after its bifurcation. This variation is supervised by a very important mathematical characteristic which is the sensitivity to initial conditions. In fact if x_0 or a are changed by a 10^{-7} variation, the results of the map changes entirely. The generated sequence is in a range of [0 1], the values are randomly produced which introduces a random behavior to the encryption system used.

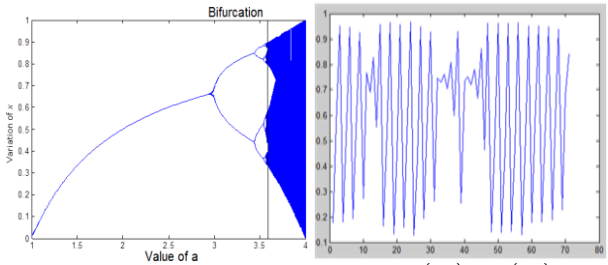

Fig 1: Logistic map after 70 iterations $\tau(x_n) = f(x_n)$ and bifurcation behavior for $x_0 = 0.1775$ and $a = 3.9999995$

2.3 Tao block crypto-system:
This crypto-system is applied in six successive steps for encryption and decryption process, presented as follows [3].
The first step consists in applying a number of iterations *N* times by the logistic map as described by the equation (1).

Such as $N = 70$ and $\tau^{70}(x_n)$ represents the output of the map in the 70th iteration.

The encryption process begins in the second step where the clear sequence m (in this paper the sequence is an image transformed in concatenate vectors) is divided in K blocks of length L= 64 bits per block as presented by the following equations.

$$m = p_0, p_1, \ldots p_{l-1}, p_l, \ldots p_{2l-1}, p_{2l}, \ldots, p_{kl-1} \quad (2)$$

And $\omega_0 = p_0, p_1, p_2 \ldots\ldots\ldots p_{l-1}$ represents the first block with L=64 bits.

In this step the outputs generated by the logistic map are transformed to binary elements. After 70 iterations we obtain two binary sequences A_j and $A_j^{'}$ .The first is composed by 64 bits and the second by 6 bits only.

The following equations describe the binary function. The general form of the sequence x is presented as follows

$$x = 0.b_1(x)b_2(x)..b_i(x) \quad (3)$$

Such as $x_n \in [0,1]$ *a*nd $b_i \in \{0,1\}$.

$$b_i(x) = \sum_{r=1}^{2^i-1} (-1)^{r-1} \Theta_{\frac{r}{2^i}}(x) \quad (4)$$

Where $b_i(x)$: is the i^{th} bit.

$$\Theta = \begin{cases} 0 \ if \ \ x < t \\ 1 \ if \ \ x \geq t \end{cases} \quad (5)$$

Θ is a majorant function

$$B_i^n = \left\{ b_i\left(\tau^n(x)\right) \right\}_{n=0}^{\infty} \quad (6)$$

B_i^n Is the binary value of the n^{th} iteration, n is the sequence length and $\tau^n(x)$ is the output of the iteration of order n.

$$A_j = B_i^1, B_i^2, \ldots\ldots B_i^{64} \quad (7)$$

$$A_j^{'} = B_i^{65}, B_i^{66}, \ldots\ldots B_i^{70} \quad (8)$$

Once the different blocks corresponding to the original message are generated, their position is non-randomly changed with cyclic translation of value T . The message block P_j is transformed to obtain $P_j^{'}(x) = T.P_j(x)$. We note by D_j the decimal value of $A_j^{'}$ that is composed by 6 bits.

If we consider $A_j^{'} = [M(65), M(66), \ldots, M(70)]$ (9)

With $M(i) \in \{0,1\}$ *and* $65 \leq i \geq 70$

$M(i)$ are the binary values of the outputs generated by the « Logistic Map » corresponding to the iterations 65, 66, 67, 68, 69, and 70.

$$D_J = \sum_{i=5}^{0} 2^i M(70-i) \quad (10)$$

In the fifth step, the encrypted message is obtained by applying the **Xor** function between $P_j^{'}$ and A_j as presented by equation (11):

$$C_j^{'} = P_j^{'} \oplus A_j \quad (11)$$

In the last step a control test is applied. If all the message is encrypted then the encryption procedure is over, otherwise $\omega_j = \tau^{70+D_j}(\omega_{j-1})$ is computed. ω represents the last iteration of (70+D_j)generated by the logistic map that will be considered as the initial value in the second step. Figures (2) and (3) illustrate the bits permutation and the encryption process.

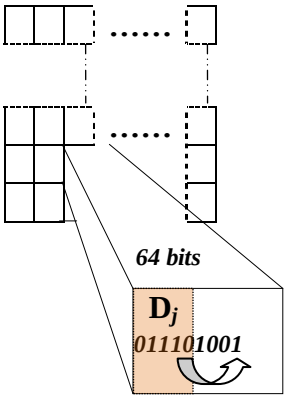

Fig 2 : Bits permutation scheme

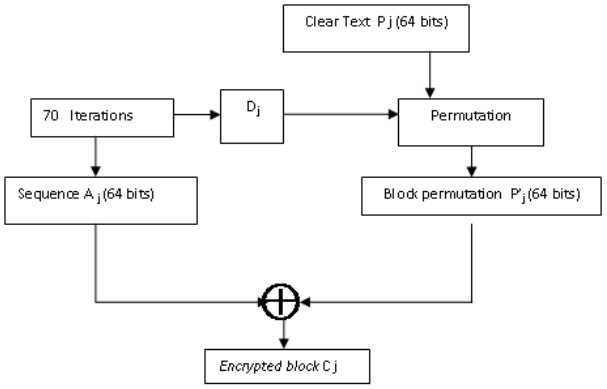

Fig 3: Encryption algorithm

2.4 Encryption algorithm weakness

Despite the efficiency of this technique proved by its security and sensitivity face to initial conditions, it presents some serious disadvantages. In fact, the number of iterations *N* is fixed to 70 which impose that the image size must be a multiple of 8!! The applied permutation is based on shift cipher techniques described by equations (12) and (13). This technique is weak and the permutation can be detected easily if the variation step *T* is revealed.

$$P_T(x) = D_j(x) + T \ [mod\ 64] \quad (12)$$

Where T the variation step and P is is the applied permutation. P-1 represents the inverse transform

$$P^{-1}{}_T(y) = y - T \ [mod\ 64] \quad (13)$$

Where y represents the permuted bit $P_T(x)$

2.5 The proposed Encryption algorithm

In this proposed algorithm we improved the complexity of the TAO encryption method and eliminate all its inconvenient. This modification makes the proposed algorithm more robust against attacks and universal with any image size.

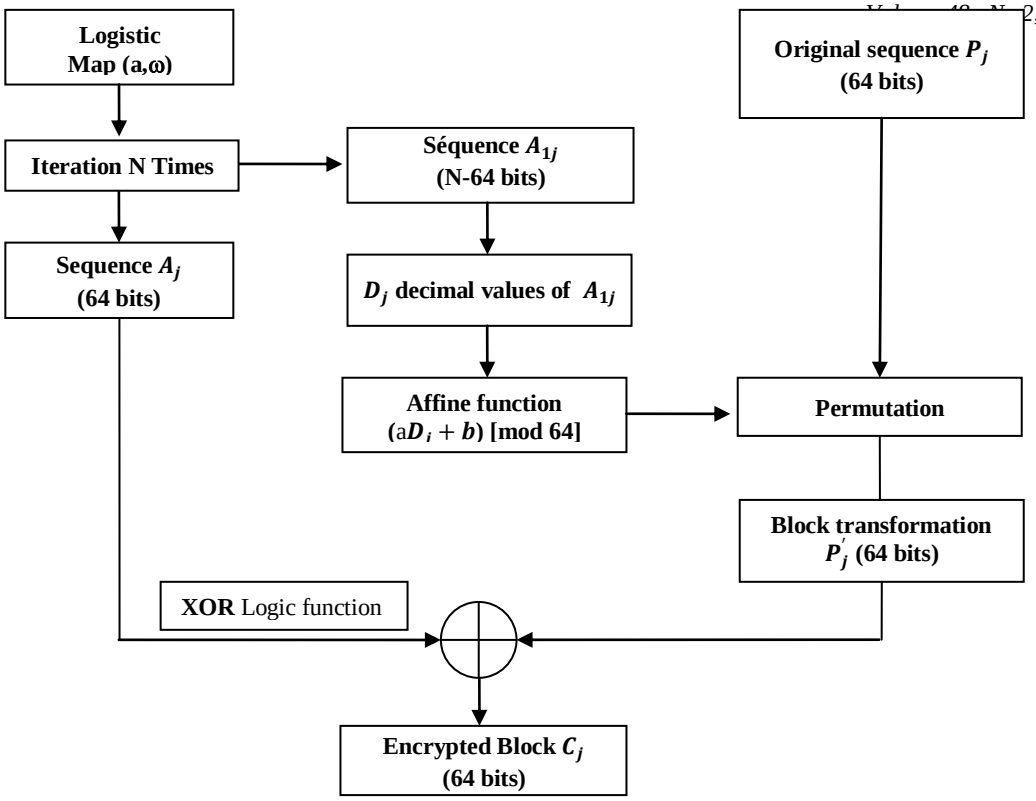

Fig 4: Proposed Encryption algorithm.

2.6 Steps of the improved algorithm

In the first step a successive iterations are generated by the « Logistic Map » as presented by equation (1). Contrarily to the TAO algorithm, the number of iterations is generalized. It can be randomized in the beginning of the Logistic map iterations or chosen by the operator as an initial condition and can be varied as he wants. The values of the initial parameters are taken as follows:

$$a = 3.9999995 \text{ and } x_0 = 0.1775;\ 0 < x_0 < 1$$

We can compute the output value of the map $\tau^{N}(x_0)$ in the N^{th} iteration. The clear message is then decomposed in blocks of 64 bits each one, as presented by equation (2).

In the following step all the N outputs of the logistics map are binarized following exactly the equation of the previous algorithm. We obtain two binary sequences A_j et A'_j. A_j is composed by 64 bits and A'_j has $(N-64)$ $bits$. The decimal value sequence Dj of A'_j is then computed as follows

$$D_J = 2^{N-65} B_i^N + 2^{N-66} B_i^{N-1} +,\ldots 2^1 B_i^{66}, 2^0 B_i^{65} \quad (14)$$

$$D_J = \sum_{n=0}^{N-65} 2^n B_i^{65+n} \quad (15)$$

In order to increase the algorithm complexity in the forth step, we replaced the shift cipher permutation by the affine permutation function represented by the following equations:

$$P_k(x) = aD_j(x) + b \left[\text{mod} 64\right] \quad (16)$$

$$P^{-1}{}_k(y) = a^{-1}(y-b)\left[\text{mod} 64\right] \quad (17)$$

Where a and b represents a couple of secret key fixed previously. The XOR operator is then applied between P'_j et $A_j$as presented by the following equation:

$$C_j = P'_j \oplus A_j \quad (18)$$

2.7 Simulation results of the proposed encryption algorithm

The proposed algorithm is tested on images. We create a database composed by 25 gray level images with different sizes. The image is encrypted and transformed into an unreadable 2D sequence as presented by figure (6). The histogram of the original image and the encrypted one are also illustrated.

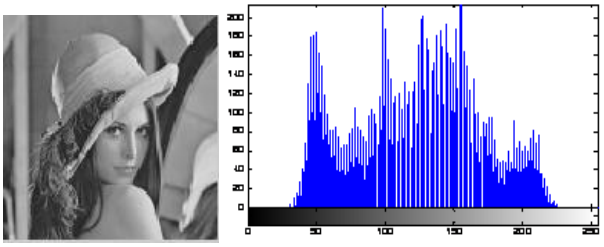

Fig 5: The original Image and its histogram

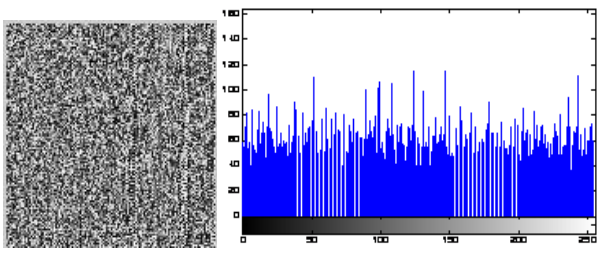

Fig 6 : The Encrypted image and its histogram

As shown by figures (5 and 6) the histogram of the encrypted image has a regular intensities distribution. This proves the efficiency of the proposed algorithm that equalizes the statistical distribution of the image in a random way making it indecipherable. The image is transformed and the information is randomly spread over the 2D sequence.

3. WATERMARKING IN THE DCT DOMAIN

3.1. Watermark presentation

The watermark database is presented as blocks with different sizes selected from the encrypted image as presented by the following figure, with $P \times P$ size described as follows:

$$W = \{ W(i, j),\ 0 \le i, j \le P \}, \quad (19)$$

W denotes the selected watermark block; Let I^h be the image used to hold the watermark in the frequency domain.

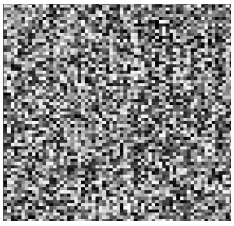

Fig 7: The embedded watermark

3.2. DCT watermark embedding

The first step of the proposed method is to use the frequency domain in which a watermark is embedded. Let I^{DCT} be the transformed image in the DCT domain presented as an (8 x 8) DCT blocks. The DCT coefficients where the watermark bits are encoded are chosen from the medium frequency band of the transformed blocks in order to provide additional resistance to lossy compression while avoiding significant modifications or distortions to the cover image. Instead of choosing arbitrarily the coefficients locations, we can increase the robustness to compression by basing our choice on the recommended JPEG table as indicated below in Fig.8. In fact, if two locations are chosen because they present identical quantization values, any scaling of the first coefficient will scale the second by the same factor preserving their relative size [8]. Furthermore, to augment survival chances of the embedded watermark against a wide range of attacks and reduces the probability of detection error; we make use of an additional gain factor denoted K in the watermark embedding process. This gain factor represents the watermark embedding strength. More this factor is high more the watermark becomes robust against attacks. Nevertheless, a constraint is applied on the choice of its value. In fact increasing this gain must not alter the image quality or introduces changes to its appearance or content. The variation of this gain must be limited by the first changes that begin to appear on the image called imperceptibility threshold. Some criteria are presented for the choice of K as shown in equation (20), but in the proposed study, a code is performed to compute the gain factor value in order to respect the imperceptibility threshold shown by the image distortion based on the Weber's law. It is found that the computed gain value is approximately equal to this introduced by the following equation:

$$A_t(u_i, v_i) - A_t(u_j, v_j) \ge K \quad (20)$$

Where A_i denotes the indexed DCT coefficient, (u_i, v_i), (uj, vj) are respectively the positions of the two selected coefficients with same quantization values and *K* is the gain factor resultant from this equation. Fig.8 proposes the quantization values used in JPEG Compression scheme. The first delimited zone represents the low frequency band; the dark zone represents the height frequency band, whereas the dashed zone represents the used medium frequency band [10].

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 8: JPEG quantization table. [8]

The embedding procedure is as follows where T^{DCT} denotes the DCT operator transform from spatial to the frequency domain:

$$T^{DCT}(I_h) = I^{DCT} \quad (21)$$

$$\alpha_x = \begin{cases} \frac{1}{\sqrt{2}} & \text{if} \quad x = 0 \\ 1 & \text{else} \end{cases} \quad (22)$$

$$I^{DCT}(u,v) = \frac{1}{\sqrt{2}} \alpha_u \alpha_v \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} I_h(i,j) \cos\left(\frac{(2i+1)\pi u}{2N}\right) \cos\left(\frac{(2i+1)\pi v}{2N}\right) \quad (23)$$

In the embedding procedure, the watermark is coded on two DCT coefficients. If many coefficients are selected to hold the watermark, two risks can occur:

- The change of a high number of DCT coefficients by coding watermarks on them can alter the watermarked image even if a low embedding strength is applied.
- More the number of coefficients used to hold the watermarks is high more the sequence is spread over the image DCT coefficients. The probability to alter and change one or more of these coefficients increase. This leads to modify and change the embedded watermarks.

The size of the watermark characterizing the amount of embedded signal changes with the image size.

After the transformation in the DCT domain, we select the DCT coefficients called I_{SL}^{DCT}. The used coefficients present identical quantization values. Let I_W^{DCT} be the watermarked image obtained as follows:

$$I_W^{DCT}(i, j) = I_{SL}^{DCT}(i, j) + K\ W(i, j);\ 0 \le i, j \le P \quad (24)$$

Where + denotes the operation of watermarks adding to the selected coefficients of the 8 x 8 blocks represented by I_{SL}^{DCT} and W is the embedded watermark.

By applying an inverse DCT transform denoted $T^{DCT^{-1}}$, as shown in equation (25), we obtain a spatial representation of a DCT watermarked image called I_W^S.

$$I_W^S = T^{DCT^{-1}}\left(I_W^{DCT}\right) \quad (25)$$

The used gain factor called K, is automatically verified based on Weber's law [10 and 11] as detailed in equation (26) to keep the watermark imperceptible.

$$\frac{|\Delta I(i,j)|}{I_w^s(i,j)} = \frac{|(I_w^s - I)(i,j)|}{I_w^s(i,j)} = CTE \quad (26)$$

Where CTE denotes a constant chosen generally equal to 2% [9] and $\Delta I(i,j)$ is the pixel variation between the watermarked and the original image. Once the gains are computed, this imperceptibility limit is also protected as shown in equation (27) by the use of a security factor that reduces the possibility to visualize some details of the embedded watermarks even though the image is zoomed many times.

$$K = K_C . S_F \quad (27)$$

Where Kc is the computed and adjusted gain factor, S_F is the used security factor. This factor is used equal to 0,9. The amount of embedded data is defined by equation (28).

$$\mathrm{Em}_c = \frac{P^2}{2.\mathrm{B}^2} \quad (28)$$

Where E_{mc} is the Embedding capacity, $P \times P$ is the message size considered as watermark and B^2 is the number of DCT blocks of the holding image.

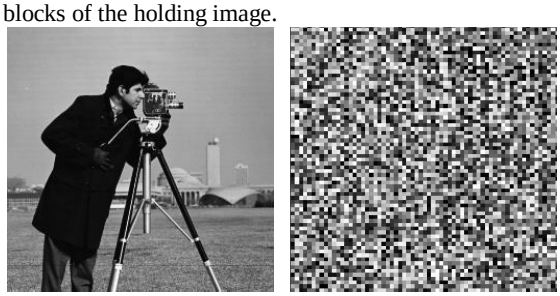

Fig.9: Clear and encrypted image "Watermark"

Fig 10: Watermarked image

In order to be sure that the embedded watermark is undetectable and does not engender any distortions to the host image, a distortion measure is associated to the psycho-visual decision. This measure based on the PSNR permit to compute the amount of noise engendered to the image by embedding the watermark. This measure is taken as a constraint for the value of the embedding gain factor K to maintain the PSNR higher than 37dB. Over this range no distortions can be detected on the watermarked image.

$$MSE = \frac{\sum_{i=1}^{n}\sum_{j=1}^{m}(I_{ij} - I_w^s)^2}{NM} \quad (29)$$

$$PSNR = 10Log_{10}\left(\frac{d^2}{MSE}\right). \quad (30)$$

Where *d*, is the dynamic of the image intensities, and I_{ij} I_w^s represent respectively the original and the watermarked image.

Fig 12: Watermarked images with different gain factors

Table 1: PSNR variation with gain factor increasing

Image	Fig.12a	Fig.12b	Fig.12c
Gain factor	K=3.2	K=5.3	K=6.8
PSNR	39.77	33.37	32.68

3.3 Watermark extraction and decryption

As the proposed technique is completely reversible, the inverse process is applied to extract the watermark from the DCT coefficients of the image [9]. In order to proceed to its decryption, the XOR logic function is applied between the encrypted watermark and the sequence A_j as shown by the equation (31).

$$P_j^{'} = A_j \oplus C_j \quad (31)$$

The following figure presents the extracted and decrypted watermark.

Fig 13: Extracted and decrypted watermark

4. RESULTS EVALUATIONS

4.1 Algorithm efficiency and rapidity

Despite the image size that generates the encryption sequences, the decryption process is considered as fast. In the following table a comparison between two decryption processes regarding two different images. The computed used is based on I.3 processor.

Tab. 21: Comparing two decryption processes for different encrypted marks

	File1	File 2
Iteration number N	100	70
File weight (Ko)	5	2,31
Decrypting time (s)	1.36	0.48

4.2 Impact of secret key variation

The couple of initial conditions (**a**, x_0) is considered as the secret key to be able to access to the decryption process and recovery the exact original image from the encrypted one. More the sensitivity to the variation of this couple of keys is higher more the efficiency and robustness of the algorithm is elevated. The following figures demonstrates that applying a very small variation of the value of these key engender a total modification of the behavior of the crypto-system outputs. The encrypted results are different; this difference is proved by the dissimilarity of their respective histograms.

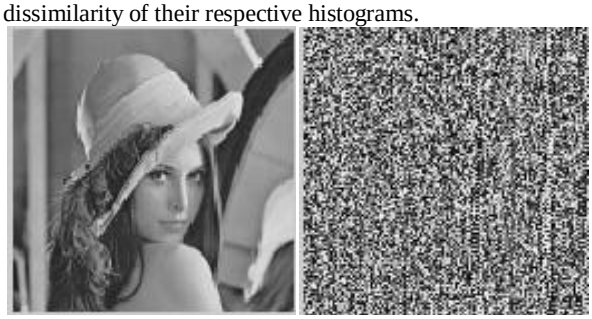

Fig 14 Original and encrypted image with: (a=3.9999995, x0=0.777)

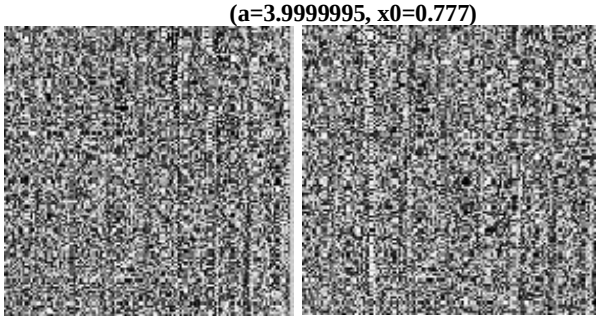

Fig 15: Encrypted image with respectively: (a=3.9999995, x0=0.778) (a=3.9999996, x0=0.777)

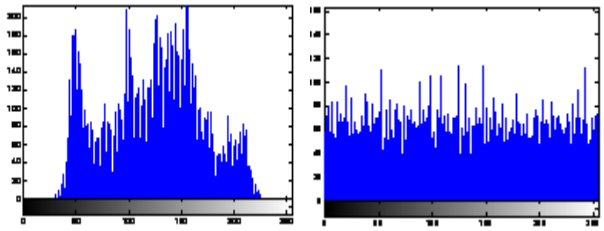

Fig 16: Histogram of the original and encrypted image with (a=3.9999995, x0=0.777)

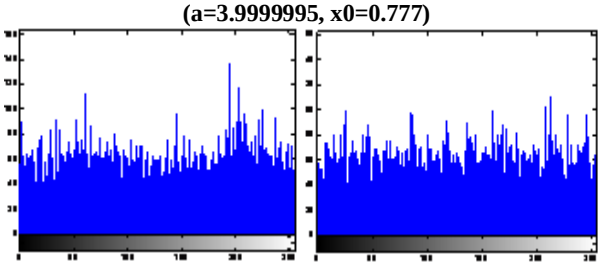

Fig 17: Histograms of the encrypted images with respectively: (a=3.9999995, x0=0.778), (a=3.9999996, x0=0.777)

4.3 Checking Dissimilarity between pixels neighbors

Any original image composed by homogeneous and textured zones presents a high correlation between the intensities of the adjacent pixels. This continuity between pixels in the image produces its forms and turn it readable. A statistical study of this cross-correlation of the encrypted image is able to reveal if this high similarity between adjacent pixels is broken. Breaking this correlation leads to an incomprehensible encrypted image. The following figures illustrate the vertical and horizontal correlation between the original image and the encrypted one.

$$Corr = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M} I(i,j)I(i-1,j)}{\sqrt{\left(\sum_{i=1}^{N}\sum_{j=1}^{M} I^2(i,j)\right)\left(\sum_{i=1}^{N}\sum_{j=1}^{M} I^2(i-1,j)\right)}} \quad (32)$$

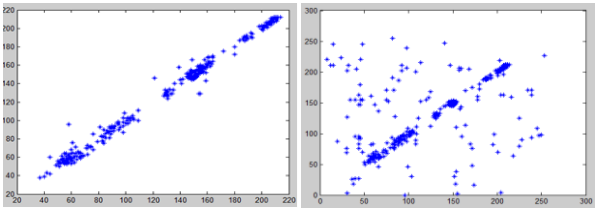

Fig 18: Correlation between vertical pixels of the original and encrypted image

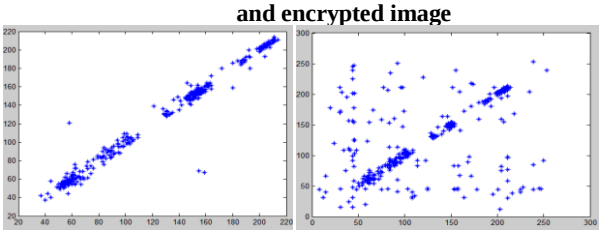

Fig 19: Correlation between horizontal pixels of the original and encrypted image

As illustrated by the above figures, the cryptosystem introduces higher dissimilarity to the adjacent pixels.

5. CONCLUSION

In this paper we presented a new method allowing ensuring image by combining encryption and watermarking technique. A modified Tao algorithm is presented. It allows encrypting gray level images with any size using chaos logistic maps and blocks encryption. The efficiency and complexity of this method is improved and tested. Once the image is encrypted a part of it is considered as a watermark and embedded in a holding image. The watermark insertion is done in the DCT domain respecting the Weber law. For better imperceptibility, a fine computing of the embedding strength avoids engendering any distortion to the watermarked image. All the process is completely reversible without any information loss. The robustness and efficiency of the proposed method is proved by statistical tests and measures.

6. REFERENCES

[1]. Schlesinger, R., "A Cryptograhy Cource for Non-Mathematicians", 1st annual conference on information security curriculum development, K ennesaw , Georgia, October 08-08,2004.

[2]. Tao, .X, Liao, .X, Guoping, T., Yong, C., Kwok-wo W., " A novel block cryptosystem based on iterating a chaotic map"; Elsevier, physics letter 15 February 2005, pp.109-115.

[3]. Maurer, .U, "The Role of cryptography in Database Security" , proceeding of the 2004ACM SIGMOD international conference on Management of data (SIGMOD'04), PP5-10, ISBN: 1-58113-859-8, Paris, France June 13- 18-2004.

[4]. Bodo, .Y, « Elaboration d'une Technique D'accès Conditionnel par Tatouage et Embrouillage Vidéo basée sur la Perturbation des Vecteurs de Mouvement », Thèse

de doctorat de L'école National supérieur des télécommunications, 2000.

[5]. Anan, .T, Kuraki. K, Takahashi. J, "Paper Encryption Technology", Fujitsu Sci, Tech j, Vol 46, No.1, pp.87-94, Yan. 2010

[6]. Y. Mao G. Chen, S. Lian, "A Novel Fast Image Encryption Scheme Based On 3D Chaoyic Baker Maps", International Journal of Bifurcation and Chaos, Vol. 14, No. 10 (2004) 3613-3624.

[7]. Ali Bani Younes, and Jantan, .A, "Image Encryption Using Block-Based Transformation Algorithm", IAENG International Journal of Computer Science, 35:1, IJCS_35_1_03.

[8]. Seddik, .H, Sayadi, .M et Fnaiech, .F "A new Multi-Domains Image Watermarking Method Based on Multi-Watermarks Embedding and Neural Network Segmentation" Applied Mathematical Sciences, Vol. 1, no. 39, pp.1927 - 1939, 2007.

[9]. H. Seddik, M. Sayadi, F. Fnaiech et M. Cheriet, "Image Watermarking Based on the Hessenberg Transform" the

International Journal of Image and Graphics, Volume: 9, Issue: 3 (July 2009).

[10]. H. Seddik and E.B.Braiek "Shaping optimal parameters selection for most favourable robustness and imperceptibility in watermarking in the DWT domain", ICGST, CSE-11 conference, 19--21 December 2011, Istanbul, Turkey.

[11]. H. Seddik, M. Sayadi et F. Fnaiech "An Accurate Estimation of Gaussian Error Function Based Scur Watermarking Algoritm", JTEA Journée tunisienne d'électricité et d'automatique, image processing track, 26-28 Mars 2010, Hammamet, Tunisie.

[12]. Xu, .X Dexter, S. and Eskicioglu, . A. M., "A hybrid scheme for encryption and watermarkin", IEEE Journal on Selected Areas in Communications 18 (2000) 850–. 860.

.