Watermarking and Encryption Scheme to Secure Multimedia Information

Tarek FARAH, Houcemeddine Hermassi, Rhoouma Rhoouma, Safya Belghith
SYSCOM Lab. ENIT. Tunisia
National Engineering School of Tunis
Tunis, Tunisia
{frhtarek, houcemeddine.hermassi, rhoouma}@gmail.com, safyabelghith@yahoo.fr

ABSTRACT: *Thanks to the development of information technology, fraud has multiplied, and many protection techniques have emerged to improve the security of our information, such as encryption, steganography and watermarking. In this paper we will present a novel scheme to secure multimedia information. Our aim is to increase the security of transmitted signals. First we improved an encryption algorithm based on chaotic iteration of the Logistics map. Then, we developed an algorithm to watermark information by using DCT method to insert message. Simulations and discussions of our method are presented to prove the efficiency of our proposition.*

Keywords: Encryption, Watermarking, Chaos, Logistic Map

Received: 7 September 2012, Revised 10 October 2012, Accepted 16 October 2012

1. Introduction

Bearing in mind interesting properties of the chaos such as the ergodicity and sensitivity of initials conditions several algorithms are proposed. The first algorithm uses the iteration of the logistic map to crypt a message is proposed by Batista [1]. After that, many other algorithms are proposed [2-3].

Xiang Tao [4,5] proposed a new algorithm of chaotic encoding, Tao divided the message into 64 bits and uses the logistic function to code the message; the key is the initial condition and the parameter of control of the logistic map.

Farah at all in 2009 [6] shown that the latter is breakable by one attack (affects) because of the independence of the key with the clear text, which presents a weak point. Farah at all improved the version of Xiang Tao and proposed a novel key that is dependent on the clear text.

We propose an improvement of algorithm proposed by Farah at all by using different keys, these improvements increase the security and robustness of the encryption process.

Our aim is to combine two techniques to secure multimedia information, encryption and watermarking.

At first the information is watermarking by inserting a message, after that we crypt the total message.

Considering the images may suffer from attacks such as levy brand or JEPEG we used the discrete cosine transform DCT, and the insertion mark is made at the average frequency [7,8, 9, 10].

2. Presentation Of Encryption-watermarked System

The encryption algorithm is presented by the following steps: (Figure 1)

In the first step we tried to improve an chaotic algorithm for encryption and decryption of Xiang Tao to make it more resistant against cryptanalysis attacks.

In the second step we developed an algorithm to insert a cover message in a cover image.

In the third step we developed an algorithm or a procedure that allows extracting the message inserted into the cover image.

We shall present at the beginning the algorithm of Tao and Farah at all after that we propose our new algorithm.

2.1 Presentation of Xiang Tao Algorithm

Recently, Xiang Tao proposed an algorithm based on logistic map, we can recapitulate this algorithm in these steps:

Other blocks are coded one using same stages that the unchanged algorithm proposed by Tao who presented it in 6 steps **[4]:**

Step 1: We iterate logistic map presend in Equation (1)

$$\tau(x_n) = x_n + 1 = \mu x_n (1 - x_n);\ x_n \in [0, 1] \quad (1)$$

$\mu = 3.999996$.

We take $N = 70$, we note ω the results of logistic map, iteration as given in the following Equation (2):

We write ω in binary form.

$$\omega = \tau^{N_0}(x) \quad (2)$$

Step 2: We divide the binary sequence in to blocs, each block is formed by 8 bits (Equation 3)

$$m = p_0, p_1, p_2 \ldots p_{l-1}, p_l, \ldots p_{2l-1}, p_{2l} \ldots \quad (3)$$

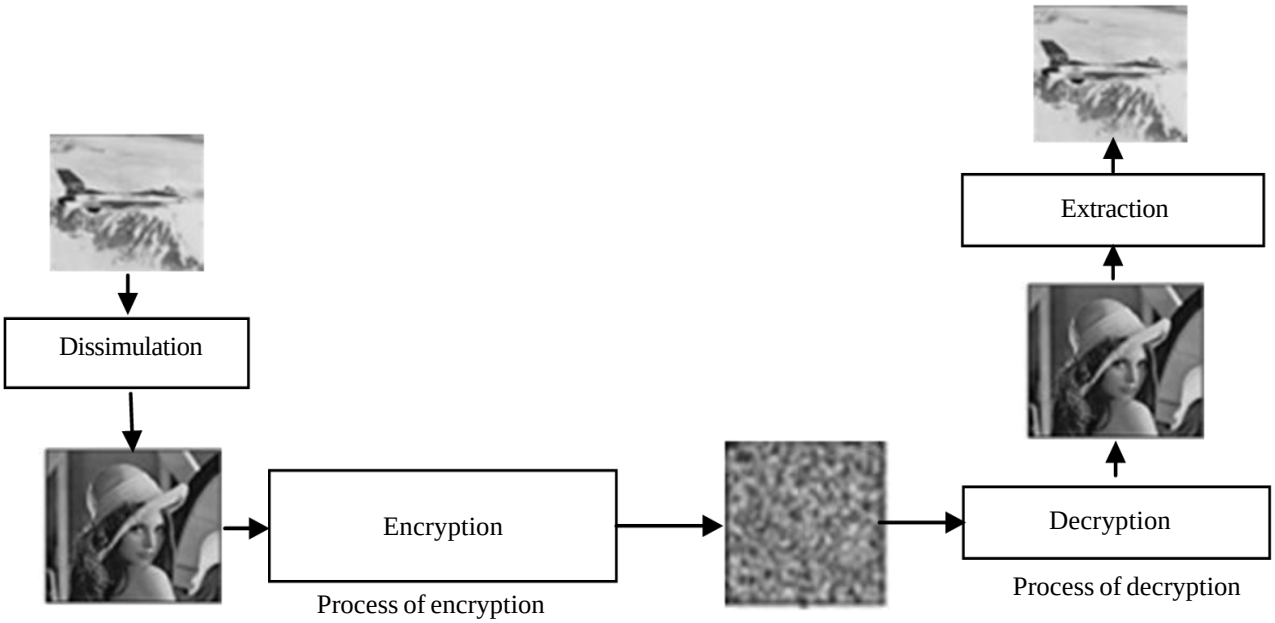

Figure1. Encryption-watermarking system

Step 3 : The binary representation of 'x' is given by this method : (Equations. 4, 5, 6 and 7)

With, $x \in [0, 1]$, $b_i(x) \in [0,1]$

$$x = 0.b_1(x)\, b_2(x) \ldots b_i(x) \tag{4}$$

$$b_i(x) = \sum_{r=1}^{2^i - 1} (-1)^{r-1}\, \Theta(r / 2^i)(x) \tag{5}$$

$$\theta_t = \begin{cases} 0 & si \quad x < t \\ 1 & si \quad x \geq t \end{cases} \tag{6}$$

$$B_i^n = \{b_i(\tau^n(x))\}_{n=0}^{\infty} \tag{7}$$

$$A_j = B_i^1\, B_i^2 \ldots\ldots\ldots\ldots B_i^{64} \quad A_j' = B_i^{65} B_i^{66} \ldots\ldots\ldots\ldots B_i^{70}$$

We take, $i = 3$, $x = 0.b_1(x)\, b_2(x)\, b_3(x)$ and we iterate 70 times. D_j is the decimal value of A_j', we will use this value to iterate the logistic map successively.

Step 4: We permute P_j and D_j by left cyclic shift.

Step 5: We applied XOR function between A_j and P_j'. (Equation (8))

$$C_j = P_j' \oplus A_j \tag{8}$$

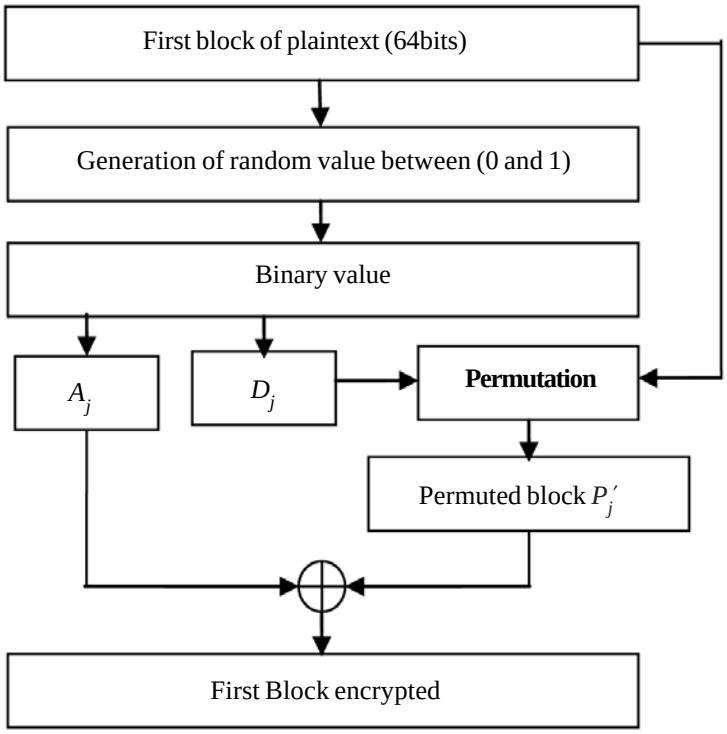

Figure 2. Farah at all algorithm

We divide C_i on 8 bits blocs.

$c_j, c_{j+1} \ldots, c_{j+7}$ and $p_j, p_{j+1}, \ldots p_{j+7}$ present respectively the blocks of plaintext.

It was noticed by the author of reference [5] that the key and the plaintext are completely independent (figure 2), this defect is corrected. This idea is to find a correction between the key and the plaintext.

It is clear that when the key and the plaintext are independent, the cryptosystem will be easily broken by using a chosen plaintext method, so the idea is to combine the key of the encryption algorithm with the message, we notice that the key depend only on the message, for this reason it is difficult to find the key.

Figure 2 presents different steps taken to encrypt the plaintext. D_j will be modified; it will depend directly on the plaintext.

It was noticed that the Tao algorithm is broken by Farah at all [6] .

Farah at all encryption algorithms is composed of two parts: an algorithm to crypt the first block of plaintext, another for the other block.

2.2 Encryption of the first block plaintext

70 random values generated are formed by two blocks. One B_J 64-bit block and the other B_j' of 6 bits.

We note :

D_j : the decimal value of the last six bits of the 70 values generate random.

The result of D_j right permutation of P_j, gives P_j' (Equation 9).

$$C_j = A_j + P_j' \tag{9}$$

To encrypt the first block text Farah considers

yy = rand (1, 70) as one key which allows to generate 70 random(unpredictable) values between 0 and 1 from which we obtain A_1 and D_1 (A_1 trained (formed) by 64 bits and D_1 of 6 dits). In other words the generation of these values will be mask. It does not depend on the iterations of the logistic map (does not depend on the initial condition and on the parameter of control of the logistic map)

Thus key becomes (*a*, *w*, *yy*)

3. Proposed Algorithm

Encryption algorithm proposed present two parts; an encryption algorithm to the first text block (the same algorithm of Farah at all [6]) and an encryption algorithm of other blocks (Figure 3)

• Encryption of the other blocks plaintext

Our algorithm is summarized by the following steps:

The steps 1, 2 and 3 are the same as the encryption algorithm of Xiang Tao in reference [4].

Step 4: we choose a new initial value x_0 and μ_2 value of control parameter of the logistic map. The logistic map is the result of this iteration (Equation 10).

$$g_2 = \tau^{64}(x_0) \tag{10}$$

Step 5: g_2 is the initial value and μ_2 the parameter control of the logistic map**.**

We iterated the logistic map ($m \times n$) times.

Step 6: The binary representation of ($m \times n$) value is given by method (see Equations 4, 5 and 6) and *z* (1, $m \times n$) is a vector line containing binary values.

Step 7: When *z* (*i*, *j*) =1 we permute P_j by D_j (see Equation 11) left cyclic bits. (see Figure 1) Otherwise unchanged.

D_1: Decimal value of 70 values generate by logistic map.

D_2: Decimal value of the first six bit of A_j.

D_3: Decimal value of the last six bit of A_j.

Eatch block to A_j is divided into two groups of eight bits.

We calculate the decimal value of each group, D_4 is the sum of these values.

$$D_j = (D_1 D_2 + D_2 D_3 + D_3 D_1) \bmod 64 \tag{11}$$

Step 8: We applied *XOR* function between A_J and P_j'. (Equation 8)

Step 9: Each block to C_j is divided into groups of 8 bits. We calculate the decimal value of each group. We note D_5 the sum of these values. After we calculate D^* by using (Equation 12)

$$D_j = (D_j D_5 + D_5 D_4 + D_4 D_j) \bmod 64 \tag{12}$$

If all blocs of plaintext are encrypted the encryption is finished, other side ω is calculated (Equation 13) and becomes the initial condition of the next block and returns to step 2.

$$\omega = \tau^{D^*}(\omega) \tag{13}$$

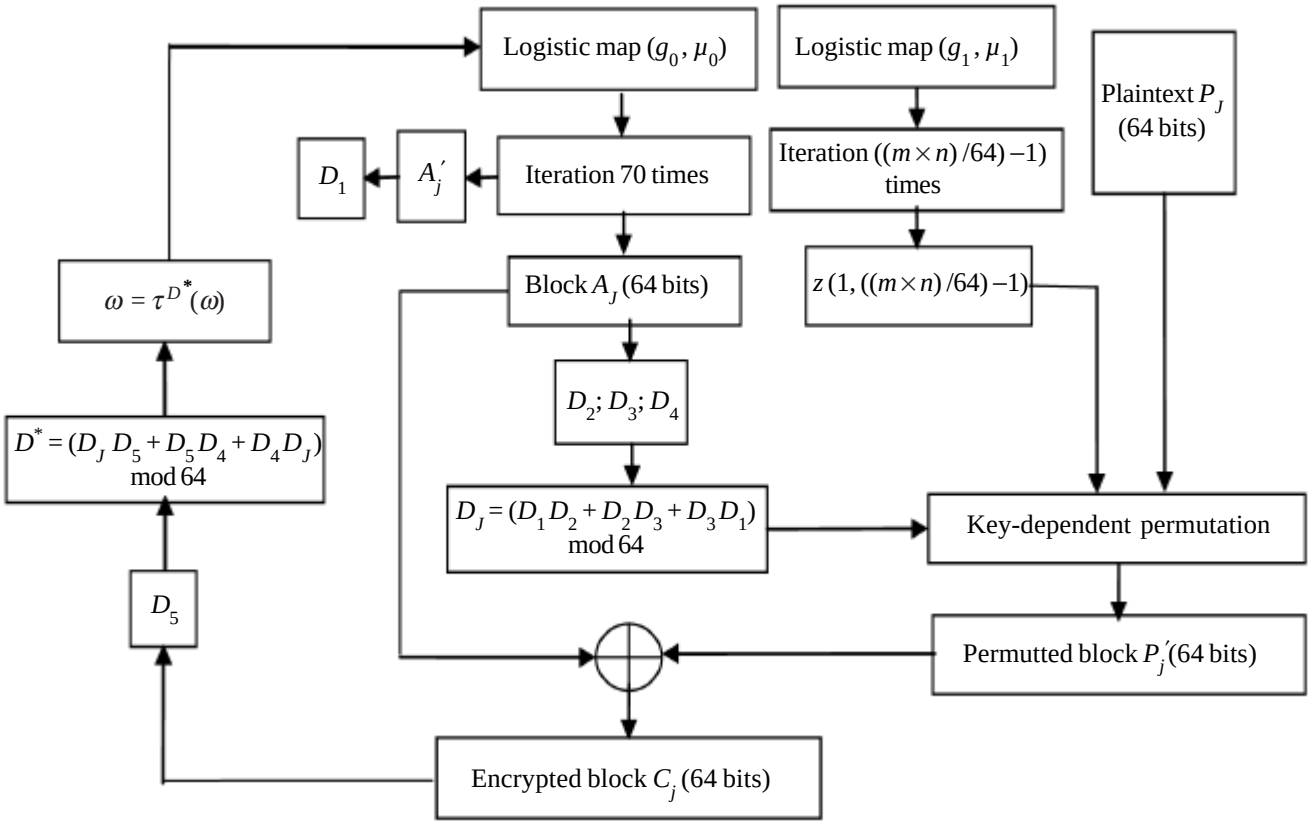

Figure 3. Proposed algorithm

From the above algorithm analysis, the attacker must possess Logistic map parameters g_0, μ_0, g_1, μ_1 and the random values *yy*, Which are totally 5 keys. The encryption algorithm improves the security and the robustness of images. The decryption algorithm process can be seen as the inverse of the encryption process. (Figures 4, 5, 6, 7)

Figure 4. Image original

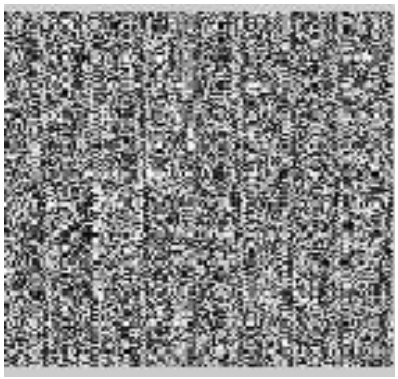

Figure 5. Encryption image

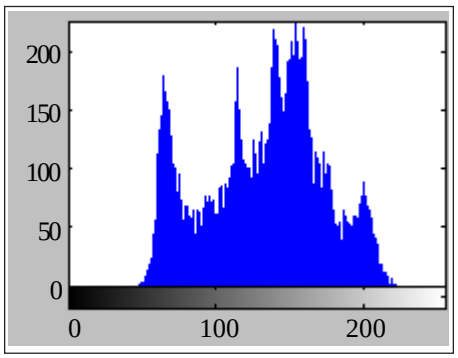

Figure 6. Histogram of original image

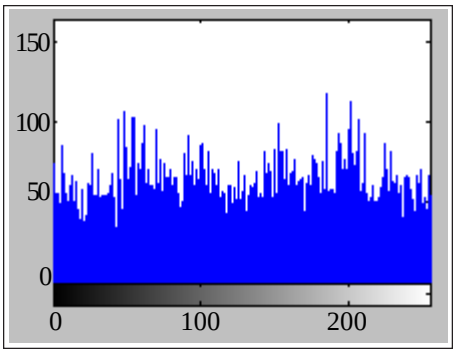

Figure 7. Histogram of encrypted image

3.1 Insertion of mark in DCT (Discrete Cosine Transform) domain

The dissimilation of information must be made in the frequency domain becaused is more robust of spatial domain.

In this area the data is inserted into very important location in the cover image, that allows the protection against attacks such as compression.

1) Choose the appropriate size of inserted image (36×36 is used in our simulation)

2) Converting gray level image to binary message.

3) Divide the message into 8×8 block.

4) Apply DCT to each block.

5) We chose two blocks to insert information in the medium frequency

6) Insertion of the secret message with modification of selected DCT coefficients.

7) Apply the DCT inverse on each block.

Let (u_1, v_1) and (u_2, v_2) are two indices chosen for the dissimilation which must belong to the medium frequency band and has the same coefficients in the standard quantification JEPEG to ensure that our message is inserted into the appropriate location ie protect it without being lost during compression or other type of attack.

Let the coefficients of the DCT transformed $(8 * 8)$ of the image carrier with the message. In the algorithm dissimilation we chose arbitrarily the two boxes and insert binary message because the last sound within the medium frequency band and presents same coefficients in the standard quantification JEPEG.

3.1.1 Extraction of the message

The algorithm of extraction of the message apply a DCT $(8 * 8)$ in the image watermarked then conducted a test on the two boxes and arbitrarily selected in the algorithm to remove dissimilation binary message.

The image inserted is shown in Figure 8.

Figure 8. Inserted image

3.2 Decryption

To get the initial image we must decrypt it with the inverse process of encryption using this equation:

$$P_j' = A_j \oplus C_j \tag{14}$$

To analyze the results obtained, it is important to develop tools to measure the error between decrypted and original image. Among these methods we find histogram analysis, key sensitivity and the degree of correlation between two images.

3.3 Histogram Analysis

A histogram is a graph representing the distribution of a continuous variable. So we can notice clearly the difference between the histogram of Lena before encryption (figure 9) and the histogram of the encrypted image of Lena shown in Figure 10, where pixels are distributed uniformly, which can resist against attacks.

So, we can say that this algorithm is efficient because it provides additional security to the hiding message which makes chaotic cryptography essential for any secure transmission of confidential information.

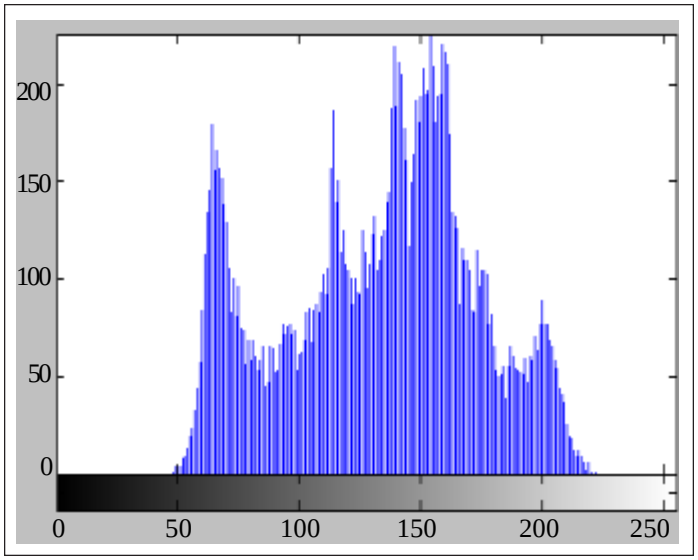

Figure 9. Histogram of original image

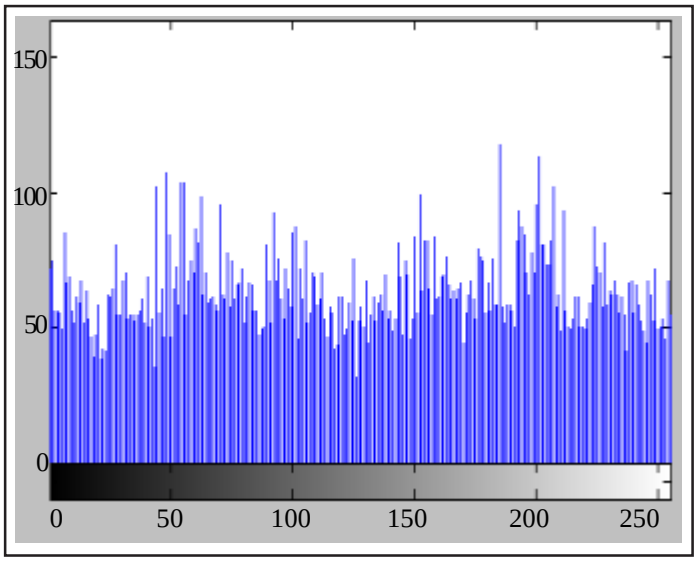

Figure 10. Histogram of encrypted image

Also, we use this technique to prove the friability of our work by comparing the original plain-image and the extracted decrypted one.

As shown in Figure 12 that represents the histogram of the decrypted image there is no difference between the two histograms

this means that the image is decrypted without any perturbation and deterioration of quality. (figures 11, 12)

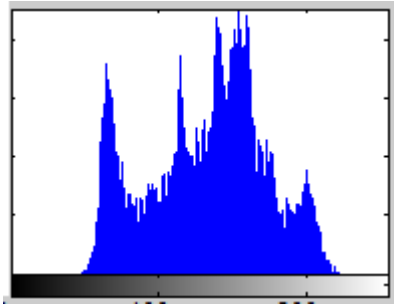

Figure 11. Histogram of the original image

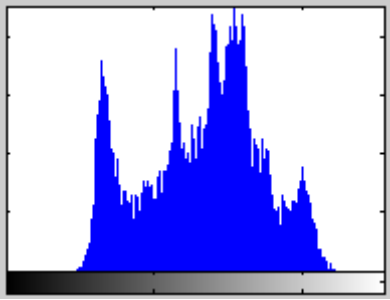

Figure 12. Histogram of decrypted image

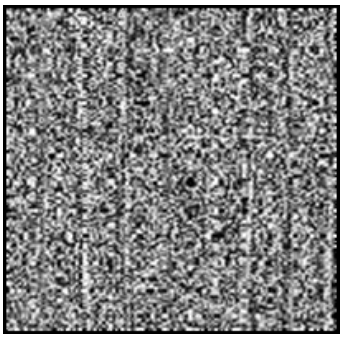

Figure 13. Encrypted Lena $\mu_0 = 3.9999995$ $g_0 = 0.778$ $\mu_1 = 3.88888888$ $g_1 = 0.666$

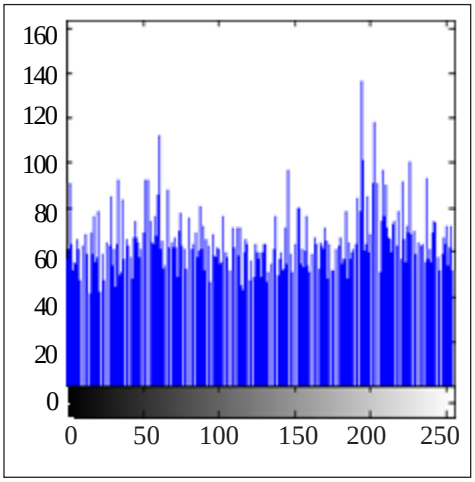

Figure 14. Histogram of Encrypted Lena $\mu_0 = 3.9999995$ $g_0 = 0.778$ $\mu_1 = 3.88888888$ $g_1 = 0.666$

3.4 Key sensitivity

To test key sensitivity, we encrypt the image with the values mentioned above and we decrypt it with different values. The result of this test shows that it is impossible to decrypt the image, if we make a small change to the initial condition "g" or the value "μ" of the logistic map. These results are illustrated in Figures 13,14,15,16.

3.5 The Correlation between two adjacent pixels

For an ordinary image each pixel is highly correlated with its adjacent pixels in the horizontal or vertical direction. An encryption algorithm should produce images ideal encrypted with the correlation between adjacent pixels is negligible. (figures 17, 18) For

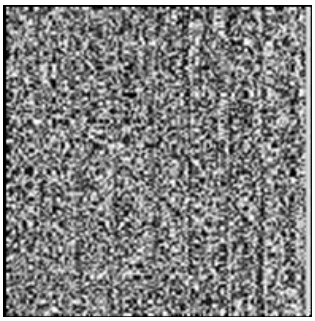

Figure 15. Encrypted Lena $\mu_0 = 3.9999996$ $g_0 = 0.778$ $\mu_1 = 3.88888888$ $g_1 = 0.666$

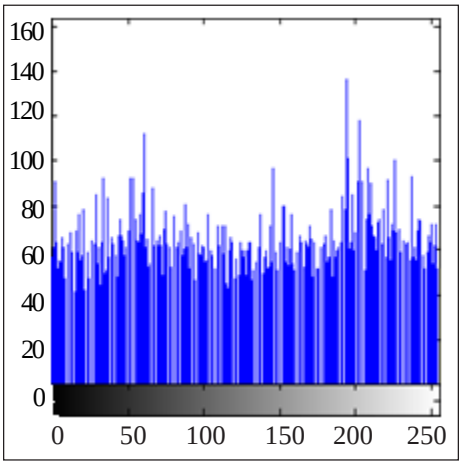

Figure 16. Histogram of Encrypted Lena $\mu_0 = 3.9999996$ $g_0 = 0.778$ $\mu_1 = 3.88888888$ $g_1 = 0.666$

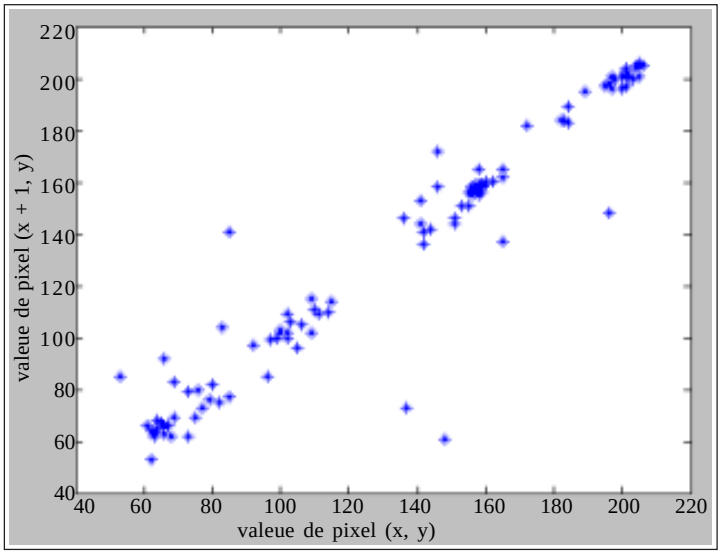

Figure 17. The correlation between two adjacent pixels vertically for the original image

an ordinary image, each pixel is highly correlated with its adjacent pixels in the horizontal or vertical direction. An ideal encryption algorithm should produce images whose numerical correlation between adjacent pixels is negligible. The following figures show the correlation tests between adjacent pixels horizontally or vertically of the original image and the encrypted one

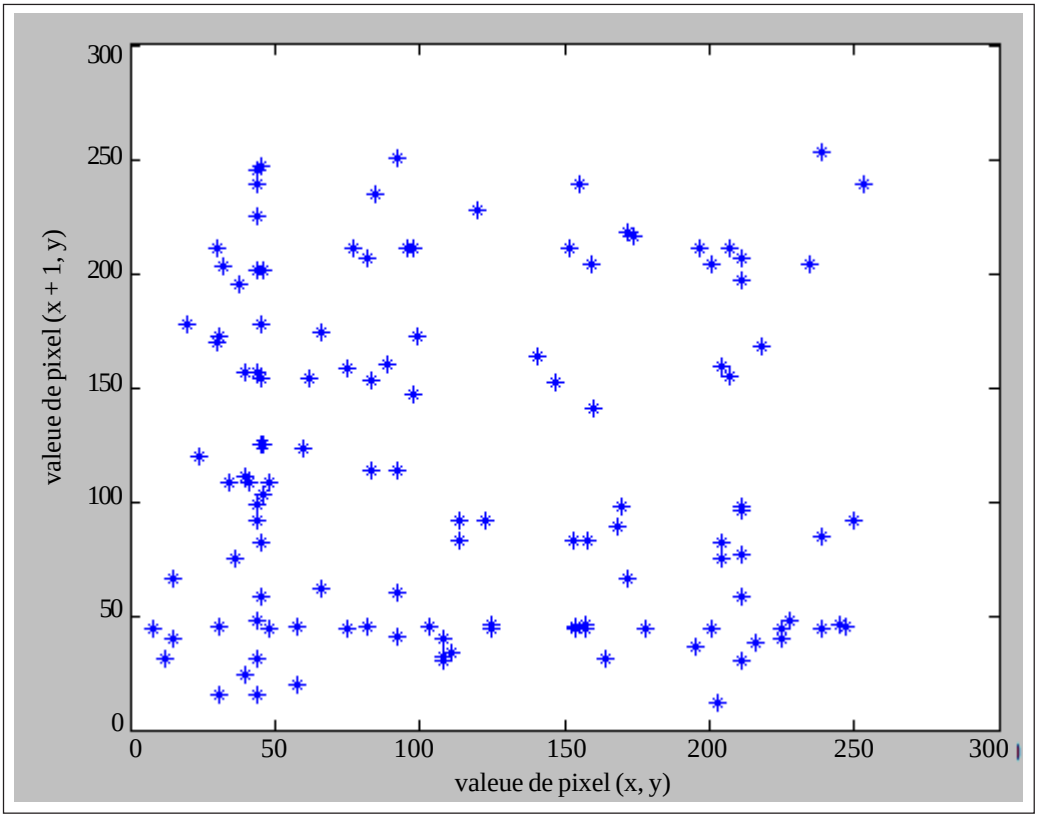

Figure 18. The correlation between two adjacent pixels horizontally for the encrypted image

It is clear that the correlation between adjacent pixels is very small in the encrypted image . This means that the proposed algorithm is efficient because the pixels of the image are distributed uniformly. And for this reason the image will be protected against attacks.

4. Conclusion

This article provides a vision of crypto-watermarking approach. First we improved an encryption algorithm based on chaotic iteration of the Logistics map. Then, we developed an algorithm to watermark information by using DCT method to insert message.

Our experimental study showed that our improved encryption algorithm is sensitive to the key and the initial condition which expresses the resistance of the latter.

In our work we will propose to improve the performance of our algorithm by reducing executing time, this step is very important in order to use our proposition in real time application. We shall compare our proposition with other encryptions schemes.

References

[1] Batista, MS. (1998). Cryptography with chaos. *Phys Lett.*

[2] Yang, T. (2004). A Survery of chaotic secure communication systems. *Int J conput*, 2 (2) 81-130.

[3] Ben Farah, M., Kachouri, A., Samet, M. (2008). Secure chaotic communication system based on active sliding mode synchronization, *In*: Prod GEI, Tunisia.

[4] Xiang, T., Liao, X., Tang, G., Chen, Y., Wong, K. (2006). A novel block cryptosystem based on iterating a chaortic map, *Phys. Lett.*

[5] Wang Y, Liao X, Xiang T, Wong K, Yang D. (2007). Cryptanalysis and improvement on a block cryptosystem based on iteration a chaotic map, *Phys Lett*.

[6] Ben Farah, M., Kachouri, A., Samet, M. (2011). Inprovement of cryptosystem based on iterating chaotic map, *Journal of Non Linear science and numerical simulation*, 16 (6) 2543-2553.

[7] Neil F. Johsen, Stefan, C., Katazenbeisser. (2000). A survey of steganographic techniques, Artech House books, ISBN 1-58053-035-4. Available on amazon .com. jannury.

[8] Tribhuwan, K.T., Vikas, S. (2007). An Improved and Robust DCT based Digital Image Watermarking Scheme. *International Journal of Computer Applications* (0975 – 8887), 3 (1), June.

[9] Zhongwei He, Wei Lu, Wei SunJiwu Huang. Digital image splicing detection based on Markov features in DCT and DWT domain, *Pattern Recognition*, 45 (12) 4292–4299, December.

[10] Zhenxing Qian, Wenwen Wang, Tong Qiao. (2012). An Edge Detection Method in DCT Domain, *Procedia Engineering*, 27, p. 344–348.