# Dynamic Chaotic Look-Up Table for MRI Medical Image Encryption

Karim Abdmouleh, Ali Khalfallah, Salim Bouhlel
Research Unit: Sciences and Technologies of Image and Telecommunications
Higher Institute of Biotechnology
Sfax, Tunisia
medkarim.abdmouleh@isggb.rnu.tn; khalfallah.ali@laposte.net; medsalim.bouhlel@enis.rnu.tn

***Abstract*—Nowadays, a variety of cryptosystem based on the chaos theory have been proposed. In this paper, we propose a new scheme encryption for Magnetic Resonance Imaging (MRI); medical images, using the chaos theory to define a dynamic chaotic Look-Up Table (LUT). Theoretic analyses and simulation results show that our scheme is secure and efficient. Also, the proposed cryptosystem is resistant to the known plaintext attack.**

***Keywords—Cryptosystem; Chaos; MRI; Look-Up-Table; Image encryption***

## I. INTRODUCTION

In modern cryptography, chaotic systems have been widely used in the development of cryptosystems [1, 2, 3, 4, 5]. Chaos has many particular properties, such as ergodicity, randomness and sensitivity to initial conditions. These proprieties are very important in cryptography. Therefore, chaotic cryptosystems have more useful and practical applications [4].

The most difficult task for the development of a cryptosystem based on chaotic aspects is the choice of the chaotic system. Most encryption algorithms using a single chaotic system are not robust against some brute-force attacks. Indeed, it is possible for a cryptanalyst to extract the characteristics of the system's chaotic trajectory [6, 7].

So, we propose a new image encryption scheme based on the combination of chaotic system based on "Logistic Map" (LM) function [8]. Indeed, the LM function ensures the properties of chaotic systems, such as sensitivity to initial values and control parameters. These properties could be exploited in cryptography.

In [4] Zhang et al. improve the properties of confusion and diffusion in terms of discrete exponential chaotic maps, and design a key scheme for the resistance to statistic attack, differential attack and grey code attack. In [9] authors suggest the introduction of a certain diffusion effect in the substitution stage by simple sequential add-and-shift operations. In the year 2010, Masmoudi et al. propose a new scheme for image encryption based on the use of a chaotic map with large key space and Engle Continued Fractions (ECF) map [10]. In [11] a new approach for image encryption based on chaotic Piecewise map, in order to meet the requirements of the secure image transfer, was proposed.

In this, the proposed cryptosystem is based on chaotic function to define a chaotic dynamic Look-Up Table (LUT) to compute the new value of the current pixel to cipher. Applying this process on each pixel of the plain image, we generate the encrypted image.

The rest of this paper is organized as follows. The proposed cryptosystem is presented in section 2. To prove the security of our proposed scheme and its robustness against various attacks, experiments results and security analysis is discussed in section 3 and 4. Finally, conclusion is drawn in section 5.

## II. THE PROPOSED APPROACH

The proposed encryption algorithm utilizes the Logistic Map. The LM function is defined by:

$$X_{n+1} = \mu X_n(1 - X_n) \quad (1)$$

Where $X$ is a floating number, which takes values in the interval [0, 1], n= 0, 1, 2,… and $\mu$ is the control parameter $0 < \mu \leq 4$.

Firstly, we must transform the image matrix size = R (N x M) pixels into a vector denoted I, with I = ($I_1$, $I_2$, ..., $I_R$). The encrypted image is also presented in a vector named E with E = ($E_1$, $E_2$, ..., $E_R$). Each element of the two vectors is shown in m bits, so the intensity of the pixel of the image is an integer between 0 and L - 1, where $L = 2^m$. For example, for a grayscale image, it is encoded in 8 bits so m = 8 and L = 256. We now proceed to present the proposed cryptosystem:

The architecture of the proposed scheme is shown in (Fig. 1, Fig. 2 and Fig. 3) and a description is given below.

**Step 1:** Initially we generate a chaotic matrix using the "Logistic Map" $LM_1$ using parameters ($x_{0XOR}$, $\mu_{0XOR}$). We mix this chaotic matrix with the plain image using the logical function XOR to obtain the initial encrypted image $I_1$.

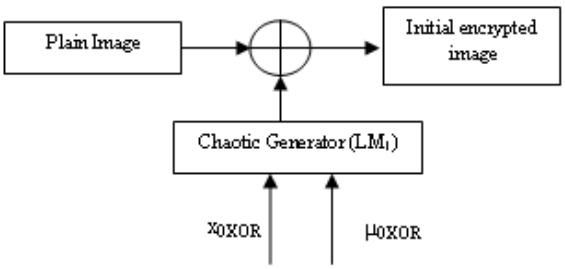



Fig. 1. XOR Chaotic encryption

⊕ : Logical function XOR

**Setp 2:** For each pixel $P_i$ of the image $I_1$, we generate a chaotic LUT (Look-Up Table) using the "Logistic Map" ($LM_2$) having as parameters $\mu_0$ and $x_0(P_c)$, with $P_c$ is the value of the previous pixel encrypted by our cryptosystem. The initial condition $x_0$ ($P_c$) depends on the previous value of the pixel $x_0$ encrypted. In addition, the values of $x_0$ ($P_c$) must be between 0.1 and 0.9.

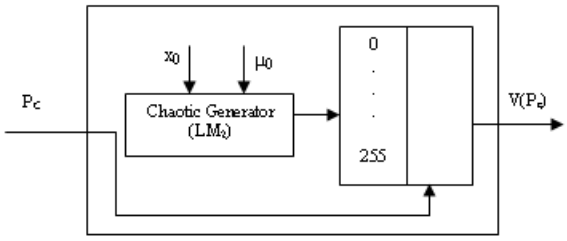



Fig. 2. Chaotic Dynamic Look-Up Table

**Step 3:** Finally, we apply this new LUT to the pixel $P_i$, we get the final pixel encrypted. This process is repeated for each pixel from the initial encrypted image to get the final encrypted one E.

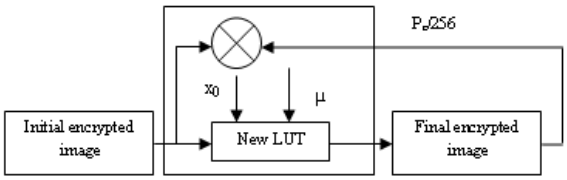



Fig. 3. Chaotic Look-Up table encryption

This stream encryption key depends on the initial condition generator LUT and the pixel value encrypted. Moreover, even if we use the same encryption key, this flow is unique for each image. Our cryptosystem is also valid for binary images and colors. Indeed, to encrypt a color image, simply extract the components of the image (RGB) and apply the algorithm to each component.

The key used in our cryptosystem is the same for encryption and decryption, and is defined by the following combination $K = (x_0, \mu_0, x_{0XOR}, \mu_{0XOR})$ where all parameters are real numbers.

## III. EXPERIMENTAL RESULTS

Simulation results of the proposed scheme are provided in this section. We used a bank of 256 grayscale MRI medical image. The different keys used in the security analysis steps are shown in Table I.

TABLE I. KEYS USED IN SECURITY ANALYSIS

| | $k_0$ | $k_1$ | $k_2$ | $k_3$ | $k_4$ |
|---|---|---|---|---|---|
| $x_0$ | 0.25 | $0.25+10^{-15}$ | 0.25 | 0.25 | 0.25 |
| $\mu_0$ | 3.8701 | 3.8701 | $3.8701+10^{-15}$ | 3.8701 | 3.8701 |
| $x_{0XOR}$ | 0.4 | 0.4 | 0.4 | $0.4+10^{-15}$ | 0.4 |
| $\mu_{0XOR}$ | 3.9 | 3.9 | 3.9 | 3.9 | $3.9+10^{-15}$ |

The improved algorithm is implemented using MATLAB 7.6 on a personnel computer (PC) with a 1.67 GHz Intel Core 2 processor, 1 Go memory and 120 Go hard disk capacity. This mathematical tool encodes a real number in 8 bytes. Thus, all the parameters are presented in 64-bit. Therefore, the proposed encryption image algorithm $\{2^{64} \times 2^{64} \times 2^{64} \times 2^{64} = 2^{256}\}$ has different combinations of the secret key.

## IV. SECURITY ANALYSIS OF THE PROPOSED CRYPTOSYSTEM

To improve the performance of the proposed encryption algorithm, we present in this section some security analysis including statistical analysis (histogram, entropy and correlation) and differential analysis (UACI and NPCR). Finally, we present the robust encryption algorithm against a type of cryptanalysis which is the known plaintext attack.

### *A. Statistical Analysis*

An image encryption algorithm should resist against statistical attacks. We present the different results obtained by statistical analysis of our cryptosystem.

#### *1) Histogram of encrypted image*

We used a database of 18 MRI medical images on 256 grayscale of size 256 x 256. We analyzed their histograms and their corresponding encrypted images.

Fig. 4.a and 4.b show respectively the original image and the encrypted image by using $k_0$. The histogram of the plain image and the encrypted image are presented in Fig 4.c and 4.d.

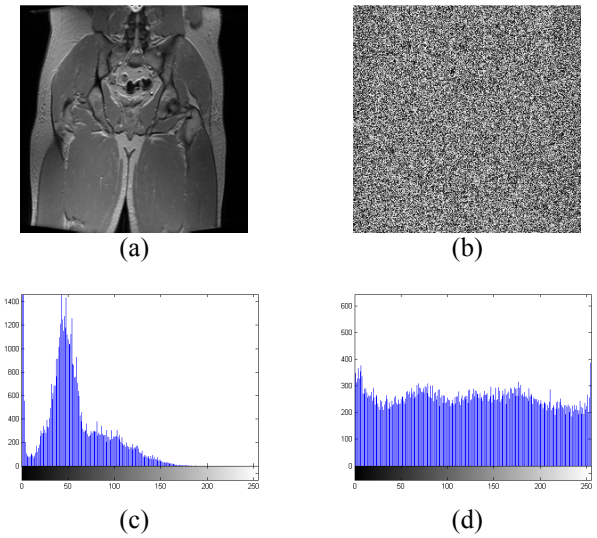


Fig. 4. Histogram analysis: (a) plain image, (b) encrypted image, (c) plain image histogram, (d) encrypted image histogram

The results show that the histograms are different; we can clearly see that the plain image Fig. 4.a differs significantly from the correspondent encrypted one Fig. 4.b. Moreover, the histogram of the encrypted image is uniform, which makes it difficult to extract the pixels statistical nature of the plain image Fig. 4.a and makes difficult any type of attack based on the analysis of the histogram of the encrypted image.

*2) Entropy of the encrypted image*

The entropy *H(m)* of a message source *m* is presented by Shannon in [12, 13] and is defined as:

$$H(m) = \sum_i P(m_i) \log_2 \frac{1}{P(m_i)} \qquad (2)$$

Where $P(m_i)$ represents the probability of symbol mi so that the entropy *H(m)* is expressed in bits.

According to Fig 4.d, the encrypted image has a uniform histogram, meaning that the gray levels have the same number of occurrences so entropy is maximum. Therefore, for a grayscale image, every pixel is represented with 8 bits, the image must have an entropy as close as possible to 8 bits / pixel [14].

The encrypted image using the key k0 shown in Fig. 4.b has an entropy equal to 7.9939 ≈8 bits/pixel which is very close to the ideal one. Also, the average entropy for 18 MRI medical images encrypted is equal to 7.9818 bits/pixel. Therefore, it is clear that our image cryptosystem is robust against the entropy attack.

*3) Correlation of two adjacent pixels*

An image is characterized by a pixel that is strongly correlated with its neighbors (in vertical, horizontal and diagonal direction). With this correlation, it is possible to deduce the value of a pixel from the knowledge of the values of neighboring pixels. For this, a cryptanalysis of the cryptosystem is complicated by the elimination of the correlation between the pixel and its neighbors [2].

To test the correlation coefficient, we select 2000 pairs of two adjacent pixels from the original image and the encrypted image respectively and randomly, and calculate the correlation coefficient using the following formula:

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \qquad (3)$$

Here, x and y are the intensity values of two adjacent pixels in the image. $r_{xy}$ is the correlation coefficient. The cov(x,y), E(x) and D(x) are given as follows:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \qquad (4)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} [x_i - E(x_i)]^2 \qquad (5)$$

$$\mathrm{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N} [(x_i - E(x_i))(y_i - E(y_i))] \qquad (6)$$

N is the number of adjacent pixels selected from the image to calculate the correlation.

The table below presents the average of the three correlation coefficients of the plain image and the corresponding ciphered images shown respectively in Fig. 4.a and Fig 4.b.

TABLE II. CORRELATION COEFFICIENTS OF TWO ADJACENT PIXELS IN THE PROPOSED METHOD

| Direction | Correlation plain image | Correlation encrypted image |
|---|---|---|
| Diagonal | 0.9307 | -8.0279e-004 |
| Horizontal | 0.9561 | 0.0041 |
| Vertical | 0.9666 | -0.0188 |

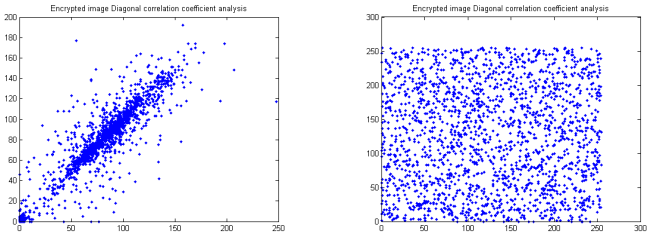



Fig. 5. Correlation between two diagonally adjacent pixels: (a) in the plain image, (b) in the encrypted image

Fig. 5 shows the correlation distributions of two diagonally adjacent pixels in the plain image and in the ciphered image. It is clear that visually neighboring pixels of a plain image are highly correlated. While this

correlation decreases significantly in encrypted images.

We see that the adjacent pixels in the original image are highly correlated, while in the encrypted image the correlation is zero. The distribution of this correlation of neighboring pixels of the encrypted image cannot prove that our cryptosystem allows the deduction of the values of neighboring pixels even with the knowledge of the value of a pixel.

We extended our study to our bank of 18 images. The results are summarized in Table III. We find the same results, which confirm the robustness of our approach.

TABLE III. AVERAGES CORRELATION COEFFICIENTS OF TWO ADJACENT PIXELS IN THE PROPOSED METHOD (18 MRI IMAGES)

| Direction | Correlation plain image | Correlation encrypted image |
|---|---|---|
| Diagonal | 0.9100 | 5.3830e-004 |
| Horizontal | 0.9376 | 0.0021 |
| Vertical | 0.9606 | -0.0394 |

*B. Differential analyzes*

Two criteria NPCR and UACI [15] are used to test the sensitivity of a single-bit change in the plain image.

The NPCR means the Number of Pixels Change Rate of ciphered image while a pixel of the plain image is changed. NPCR is defined as:

$$NPCR = \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} D(i,j)}{M \times N} \times 100 \quad (7)$$

D (i, j) is determined as follows:

$$D(i,j) = \begin{cases} 1 & if\ C_1(i,j) \neq C2(i,j) \\ 0 & else \end{cases} \quad (8)$$

The Unified Average Changing Intensity (UACI) between these two images (plain and ciphered image) is defined by the following formula:

$$UACI = \frac{1}{M \times N} \sum_{i=0}^{M-1}\sum_{j=0}^{N-1} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100 \quad (9)$$

The NPCR and UACI of the plain image shown in Fig 3.a are calculated and presented in Table IV. The objective of this analysis is to show that a small change in the image clearly introduces a major change on encrypted the image.

TABLE IV. VALUES RESULTS OF NPCR AND UACI FOR THE PLAIN IMAGE SHOWN IN FIG. 4.A

| NPCR | UACI |
|---|---|
| 99.6094 | 32.9008 |

Given the results found after our test, we can conclude that our proposed method is resistant to differential attacks.

The average of the two criteria calculated on 18 MRI medical images encrypted with key $k_0$ is shown in Table V.

TABLE V. AVERAGES VALUES RESULTS OF NPCR AND UACI (18 MRI IMAGES)

| NPCR | UACI |
|---|---|
| 99.514 | 32.5689 |

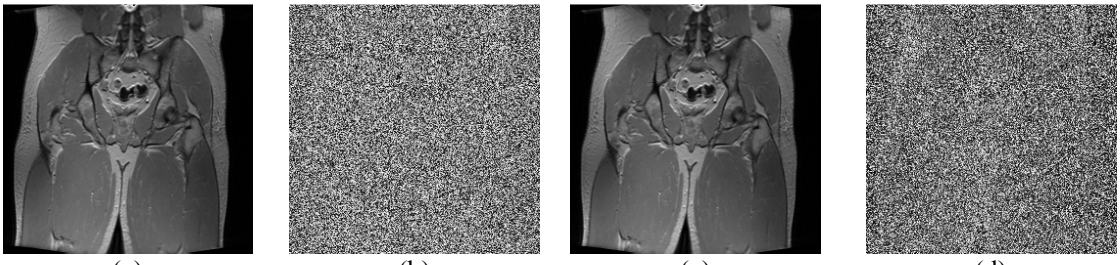
Therefore, our improved scheme is secure against Known-plaintext attack. This attack is one of the attacks where the cryptanalyst owns a plaintext image and its corresponding encrypted image. This frequently used attack utilizes the known clear image and the ciphered image to extract the decryption key or to decrypt another ciphered image.

*C. Key sensitivity*

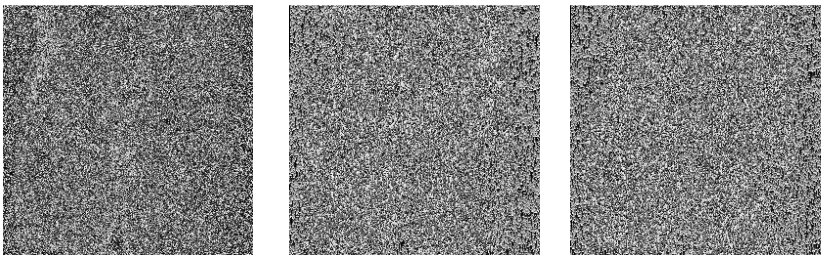
All cryptosystem should be very sensitive to every little change in the secret key [16]. In addition, we analyze the key sensitivity of our cryptosystem for encryption and decryption.

The secret key of our encryption algorithm is composed of four values $\{x_0, \mu_0, x_{0XOR}, \mu_{0XOR}\}$. These values are the parameters of the two Logistic Map functions used in our encryption algorithm.

We encrypt the original image shown in Fig 4.a with the secret key $k_0$ to analyze the sensitivity of our cryptosystem to some change in the secret key. Secondly, we propose to decrypt the cipher image encrypted with $k_0$ using keys with a difference by $10^{-15}$ on $x_0$, $\mu_0$, $x_{0XOR}$, $\mu_{0XOR}$.



(a) (b) (c) (d)



(e) (f) (g)

Fig. 6. Key sensitivity test: (a) plain image, (b) Encrypted image with k0 , (c) Decrypted image with k0 , (d) Decrypted image with k1, (e) Decrypted image with k2, (f) Decrypted image with k3, (g) Decrypted image with k4

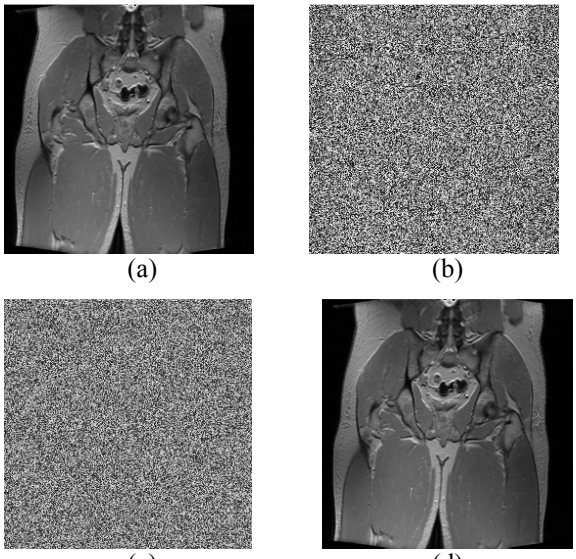
We can show in Fig. 6 that an image encrypted by the secret key k0 is not correctly decrypted by using a key with a difference by $10^{-15}$ on $x_0$, $\mu_0$, $x_{0XOR}$, $\mu_{0XOR}$.

*D. Cryptanalysis*

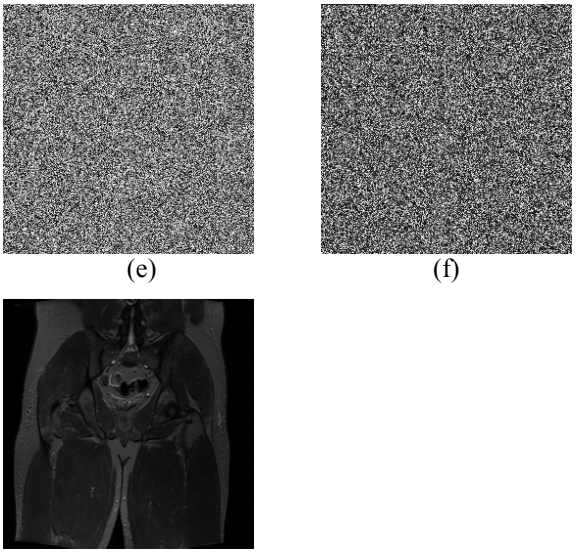
In our study, we are based on the known plaintext attack to apply the stream key attack on our cryptosystem. This attack uses clear image and encrypted image to extract the decryption key and decrypt another encrypted image.

"Fig. 7" summarizes the key stream attack applied on our cryptosystem.

Fig. 7.c represents the key stream used to decrypt encrypted image (Fig. 7.b). The result of this process is illustrated in Fig. 7.d. We note that the image obtained is equal to the clear picture (Fig. 7.a). After that, we use the key stream to decrypt the obtained image shown in Fig. 7.e, which represents the encrypted image of "MRI pelvis t2". Fig. 7.f proves the failure of the attack. Indeed, this last picture is quite different from the clear image "MRI pelvis t2" shown in Fig. 7.g.



(a) (b) (c) (d)



(e) (f) (g)

Fig. 7. Failed crack attempt: (a) plain image "MRI pelvis pd", (b) encrypted "MRI pelvis pd"image, (c) extracted key stream, (d) decrypted "MRI pelvis pd" image, (e) encrypted "MRI pelvis t2" image, (f) failed attempt to crack the cipher image of"MRI pelvis t2", (g) plain image "MRI pelvis t2"

The results in Fig. 7 show that our approach could not be broken by a known plaintext attack. This result is expected for the presence of a feedback in the cryptosystem.

## V. CONCLUSION

In this paper, we have presented a new encryption scheme based on a chaotic system called Look-Up table. This new proposal uses the "Logistic Map" to generate a dynamic LUT. This LUT depends on the previous pixel encrypted. This feedback introduced into the cryptosystem gives excellent performance. In fact, the encrypted image is very different from the plain image. This dissimilarity is due to the randomness introduced by the chaos. Finally, experimental and analytic results indicate that the proposed encryption scheme is secure and efficient.

## REFERENCES


[1] S. Li, X. Mou, and Y. Cai, "Improving Security of a Chaotic Encryption Approach," Physics Letters A, vol. 290, no. 3, 2001, pp. 127-133.

[2] X. Wu, H. Hu and B. Zhang, "Analyzing and Improving a Chaotic Encryption Method," Chaos, Solitons and Fractals, vol. 22, no. 2, 2004, pp. 367-373.

[3] T. Yang, "A Survey of Chaotic Secure Communication Systems," Int. J. Comp. Cognition, vol. 2, 2004, pp. 81-130.

[4] L. Zhang, X. Liao, and X. Wang, "An Image Encryption Approach Based on Chaotic Maps," Chaos, Solitons and Fractals, vol. 24, no. 3, May 2005, pp. 759-765.

[5] K.-W. Wong, B. S.-H. Kwok, and C.-H. Yuen, "An Efficient Diffusion Approach for Chaos-Based Image Encryption," Chaos, Solitons and Fractals, vol. 41, no. 5, 2009, pp. 2652-2663.

[6] K. M. Short, "Signal Extraction from Chaotic Communications," International Journal of Bifurcation and Chaos, vol. 7,no. 7, 1997, pp. 1579-1597.

[7] P. Li, Z. Li, W. A. Halang, and G. Chen, "A Stream Cipher Based on a Spatiotemporal Chaotic System," Chaos Solitons and Fractals, vol. 32, no. 5, 2007, pp. 1867-1876.

[8] R. L. Devaney, An Introduction to Chaotic Dynamical Systems, Westview Pr (Short Disc), 2003.

[9] K.-W. Wong, B. S.-H. Kwok, and C.-H. Yuen, "A Fast Image Encryption Scheme Based on Chaotic Standard Map," Physics Letters A, vol. 372, 2008, pp. 2645-2652.

[10] A. Masmoudi, M.S. Bouhlel and W. Puech, "A New Image Cryptosystem Based on Chaotic Map and Continued," Proc. EUSIPCO'10, 2010, pp. 1504-1508.

[11] Y. Wang and X. Liao, "A Novel Image Encryption Approach based on Chaotic Piecewise Map," Journal of Theoretical Physics and Cryptography, vol. 1, Nov. 2012, pp. 37-40.

[12] C. E. Shannon, "A Mathematical Theory of Communication," The Bell System Technical Journal, vol. 27, July 1948, pp. 379-423.

[13] C. E. Shannon, and W. Weaver, "The Theory of Communication," Illinois : University of Illinois Press, vol. 24, 1949, p. 253.

[14] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, "A Novel Algorithm for Image Encryption Based on Mixture of Chaotic Maps," Chaos, Solitons and Fractals, vol. 35, no. 2 Jan 2008, pp. 408-419.

[15] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," Chaos, Solitons and Fractals, vol. 21, no. 3, 2004, pp. 749-761.

[16] S.S. Maniccam, and N.G. Bourbakis, "Lossless image compression and encryption using SCAN," Pattern Recognition, vol. 34, no. 6, 2001, pp 1229-1245.