The ISC Int'l Journal of Information Security
ISeCure

January 2013, Volume 5, Number 1 (pp. 97–110)
http://www.isecure-journal.org

Image Encryption Based on Chaotic Tent Map in Time and Frequency Domains☆

Elham Hassani [1],* and Mohammad Eshghi [2]
[1] Tehran Municipality ICTO, Applied Science and Technology Center, Tehran, Iran
[2] Electrical and Computer Engineering, Shahid Beheshti University, Tehran, Iran

ARTICLE INFO.

Article history:
Received: 3 February 2012
Revised: 5 June 2013
Accepted: 21 July 2013
Published Online: 1 November 2013

Keywords:
Image Encryption, Chaotic Tent Map, Key Image, Frequency Domain, Time Domain.

ABSTRACT

The present paper is aimed at introducing a new algorithm for image encryption using chaotic tent maps and the desired key image. This algorithm consists of two parts, the first of which works in the frequency domain and the second, in the time domain. In the frequency domain, a desired key image is used, and a random number is generated, using the chaotic tent map, in order to change the phase of the plain image. This change in the frequency domain causes changes in the pixels value and shuffles the pixels location in the time domain. Finally, in the time domain, a pseudo random image is produced using a chaotic tent map, to be combined to the image generated through the first step, and thus the final encrypted image is created. A computer simulation is also utilized to evaluate the proposed algorithm and to compare its results to images encrypted by other methods. The criteria for these comparisons are chi-square test of histogram, correlation coefficients of pixels, NPCR (number of pixel change rate), UACI (unified average changing intensity), MSE (mean square error) and MAE (mean absolute error), key space, and sensitivity to initial condition. These comparisons reveal that the proposed chaotic image encryption method shows a higher performance, and is of more secure.

1 Introduction

In recent years, with the fast development of computer networks, multimedia communications and image transmission through networks, such as internet, are increased. The transmission of images through networks is of numerous applications including military, commercial or even medical applications. In any case, in order to prevent unauthorized access to images, it is essential to encrypt them, before or during transmission through networks. To protect such communications, image encryption technique has recieved its due attention by the researchers. In this respect, many image encryption schemes have been proposed. The chaos-based encryption methods are one of the methods that yield a good combination of speed and high security [1–3].

An image, as one of multimedia data, has high capacity, high redundancy, and high correlation between adjacent pixels. Eventually, applying old algorithms such as Advance Encryption Standard (AES), Data Encryption Standard (DES) and RSA, which usually encrypt binary or text data, may encounter two seri-

☆ An earlier version of the paper has been peer reviewed, accepted, and presented at the 7th Iranian Machine Vision & Image Processing Conference, Tehran, Iran, November 16-17, 2011.

* Corresponding author.

Email addresses: e.hasani@srbiau.ac.irr (E. Hassani), m-eshghi@sbu.ac.ir (M. Eshghi).

ISSN: 2008-2045 © 2013 ISC. All rights reserved.

ous problems with respect to image encryption. First, due to the high correlation between adjacent pixels in the image and its background color consistency, these algorithms do not show a good performance in creating an acceptable security level in the image. The second problem lies with real time applications, i.e the prolongation of the time for execution of these algorithms [4–6].

The chaotic functions have numerous properties such as randomness, ergodicity and sensitivity to initial conditions. These properties create a close relationship between cryptosystems and chaotic systems. Chaotic maps produce long-period, random-like chaotic sequences, which are changed significantly as a result of a small difference of the initial value or system parameters [5, 7].

In this regard, Mao *et al.* have designed a new image encryption system based on distributed Baker map in time domain [8]. Zhou *et al.* also introduced a parallel image encryption algorithm in time domain, using the kolmogrov flow map. In this algorithm, all of the pixels are permuted by this map and then encrypted by Cipher Block Chain model [9]. Xin Zhang *et al.* proposed another image encryption algorithm in time domain. In this system, first the combination of the original and the key image produces a fusion image. This image is then ciphered using the Henon chaotic map [10].

In a similar vein, Borujeni *et al.* designed an image encryption algorithm based on chaotic maps and Tompking-Paig's algorithm [11]. Khanzadi *et al.* also proposed an algorithm using a random bit sequence generator (RBSG) based on logistic and tent map. In this algorithm, a plain image is permuted and then partitioned into 8 bit maps. Bits are permuted and substituted in each bit map. Finally, the 8 bit maps are composed to produce the encrypted image [12]. In [1], we introduced an image encryption system based on chaotic function in both time and frequency domains.

In this paper, a new algorithm is proposed for image encryption using tent chaotic map and desired key image. This algorithm consists of two parts. In the first part, the encryption system works in the frequency domain while in the second part, it operates in the time domain. In the frequency domain, using the desired key image, a random number is generated by the chaotic tent map and Exclusively ORed key image pixels for changing in the phase of plain image. The result in the time domain causes a change in the pixel value and shuffles the pixel location in time domain. In the time domain, the image produced in frequency domain is Exclusively ORed so that a pseudo random image is produced through a chaotic process.

The rest of the paper is thus organized as follows. In Section 2 a literature survey is presented on chaotic image encryption system. Section 3 includes a background on chaotic systems. In Section 4, the proposed design of the chaotic image encryption scheme is discussed in details. In Section 5, this proposed image encryption scheme is evaluated. Comparisons are then drawn with other methods in Section 6 and finally the paper ends with a conclusion in Section 7 .

2 Literature Survey

2.1 Analysis on an Image Encryption Algorithm

Shubo *et al.* proposed a new image encryption scheme [13]. This paper proposes a chaos-based image encryption system, in the framework of stream cipher architecture.

Given the abovementioned method, an image is firstly converted to a binary data stream. The corresponding encrypted image is formed By masking these data with a random key stream generated by the chaos-based pseudo-random key stream generator (PRKG).

The proposed PRKG is governed by a couple of logistic maps, which depend on the values of (b, x_0, p, y_0). These values are secreted, and are then used as the cipher key. Through iterations, the first logistic map generates a hash value x_{i+1}, which is highly dependent on the input (b, x_0), obtained and used to determine the system parameters of the second logistic map.

The second logistic map also generates binary sequences y'_{i+1}, which are highly dependent on the input (p, y_0) and the first logistic map, which are obtained and used to masking the data stream of the plain image. The generator system can be briefly expressed in the following:

$$\begin{array}{ll} 1 & x_{i+1} = bx_i\left(1 - x_i\right) \\ & y_{i+1} = py_i\left(1 - y_i\right),\ i = 0, 1, 2, \ldots \\ 2 & x^{'}_{i+1} = X^{'}_{i+1} = X_1\ XOR\ X_m\ XOR\ X_h \\ & y^{'}_{i+1} = Y^{'}_{i+1} = Y_1\ XOR\ Y_m\ XOR\ Y_h \\ 3 & x^{''}_{i+1} = x^{'}_{i+1} \times 10 \\ & p = x^{''}_{i+1} \qquad (3.569945 < x^{''}_{i+1} < 4 \cap n \geq 100) \end{array} \tag{1}$$

2.2 Image Encryption Algorithm Based on Henon Chaotic System

Chen Wei-bin *et al.* proposed a new image encryption algorithm based on Henon chaotic system in order to meet the requirements of the secure image transfer [14].

This image encryption algorithm includes two steps. Firstly, the positions of the pixels of the original image are shuffled using Arnold cat map. Then the pixel values of the shuffled image are encrypted by Henon's chaotic system.

2.2.1 Encryption Using the Arnold Cat Map

The Arnold cat map is a two-dimensional invertible chaotic map. Without loss of generality, we assume the dimension of the original grayscale image I as $M * M$. Arnold cat map is described as the following:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 \; c \\ d \; cd+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod (M) \qquad (2)$$

where c and d are positive integers. (x_{n+1}, y_{n+1}) is the new position of the original image, and (x_n, y_n) is its original position, and $n = 0, 1, 2, \ldots$. After iterating N times, there exist positive integers T, such that $(x_{n+1}, y_{n+1}) = (x, y)$. The period T depends on the parameters c, d and the size M of the original image.

Thus the parameters c, d and the number of iterations N all can be used as the secret keys. Since there only exist a linear transformation and a mod function, it is very efficient to shuffle the pixel positions using the Arnold cat map. After several iterations, the correlation among the adjacent pixels can be disturbed completely.

2.2.2 Encryption by Henon Chaotic System and Arnold Cat Map

In our scheme, two variables of the Henon chaotic map are adopted to encrypt the shuffled-image. The encryption process consists of three steps of operations.

Step1: The Henon chaotic system is converted into a one-dimensional chaotic map. The one-dimensional Henon chaotic map is defined as:

$$x_{i+2} = 1 - ax_{i+1}^2 + bx_i \qquad (3)$$

Where $a = 0.3$, and $b \in [1.07, 1.4]$. Parameters a, and b ,and the initial values of x_0 and x_1 may represent the key.

Step2: After shuffling the image, we adopt Henon chaotic map to change the pixel values of the shuffled-image. First, Henon chaotic map is obtained by (3). Then, the transform matrix of pixel values is created.

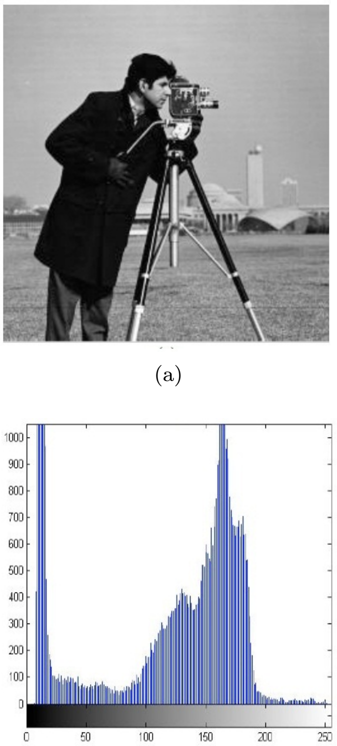
Step3: The exclusive OR operation will be completed bit-by-bit between the transform matrix of pixel values and the values of the shuffled-image. We can obtain the cipher-image.

Since the chaotic systems are deterministic, the receiver can reconstruct exactly the same shuffled-image using the same secret keys. Then the anti-process of image shuffling is defined as:

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} 1 & c \\ d & cd+1 \end{bmatrix}^{-1} \begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} \bmod (M) \qquad (4)$$

The parameter is chosen the same as the process of image shuffle. Subsequently, the original image can be obtained. At this stage, the decrypted process is completed.

The original image with the size of $256 * 256$ is shown in Figure (1a) the histogram of which is also provided in Figure (1b). Figure (2a) illustrates the cipher-image created by Henon chaotic map with its corresponding histogram displayed in Figure (2b).



(a)

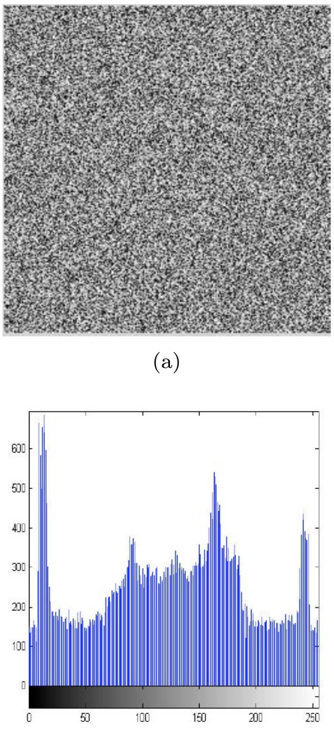
(b)

Figure 1. (a) original-image, (b) histogram of the original-image

2.3 Image Encryption Using Random Bit Sequence Based on Chaotic Maps

Khanzadi *et al.* proposed an image encryption algorithm using a random bit sequence generator (RBSG) based on logistic and tent map [12].

The encryption process consists of five major stages, namely the pixel permutation, pixel decomposition, bit map permutation, bit map substitution, and bit map composition. A brief description of each stage is being presented below.



(a)

(b)

Figure 2. (a) cipher-image, (b) histogram of the cipher-image

2.3.1 Pixel permutation Stage

The permutation stage consists of three phases. In each phase, a RNM is used to produce the required random Ergodic matrix (REM). Each pixel of the image which is obtained from the permutation stage, and is called the permuted image, has a gray level (0-255) which can be presented with 8 bits. The permutation stage is depicted in Figure 3.

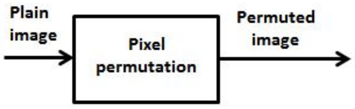


Figure 3. Block diagram of permutation stage

2.3.2 Decomposition Stage

In the decomposition stage, the permuted image is decomposed to 8 bit map images, which are called BM0 to BM7. BM0 consists of a bit map image using the least significant bit of pixel values of the permuted image. Other BMs use the other bits of the pixels of permuted image respectively. The decomposition stage is shown in Figure 4.

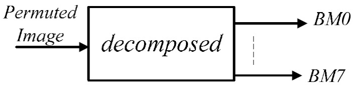


Figure 4. Block diagram of decomposition stage

2.3.3 Bit Map Permutation Stage

In the bit map permutation stage, these BMs are permuted using other 8 different REMs, with eight different initial conditions. The result of this stage is eight permuted bit maps (PBM), called PBM0 to PBM7. The block diagram of the permutation bit map stage is illustrated in Figure 5.

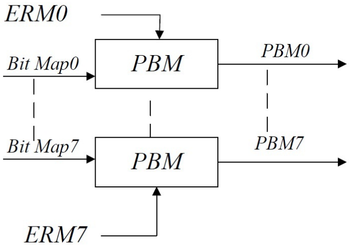


Figure 5. Block diagram of permutation in bit map stage

2.3.4 Bit Map Substitution Stage

In the substitution stage, a random generator is used to produce 8 RBMs, which have also different initial conditions. Each bit of the PBM is EX-ORed with its corresponding bit in RBMs, respectively. The EX-OR decreases the correlation between the bits. The results of this stage are eight substitute bit maps (SBM0-SBM7), called SBMs. Equation (5) expresses the formula:

$$SBM_k(i,j) = xor(RBG_k(i,j), BM_k(i,j)) \quad (5)$$

Figure 6 below displays the block diagram of substitution bit map.

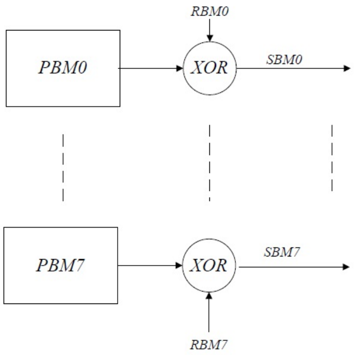
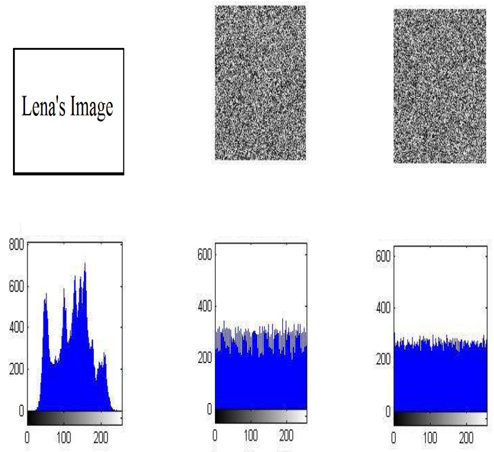


Figure 6. Block diagram of Bit Map Substitution stage

2.3.5 Bit Map Composition

In the composition stage, 8-BMs will be put together to create the image. The BM0 is the least significant bit of image pixels while BM1 is the 2nd bit of image pixels.

Similarly, BM7 is the most significant bit of image pixels. In this section, these SBMs of the substitution stage are put together and thus the encrypted image is obtained. The results of the plain image, the bit map permutation and encryption image as well as the histogram of the three images are illustrated in Figure 7.



(a) (b) (c)

Figure 7. (a) plain image and it's histogram, (b) bit map permutation and it's histogram, (c) encrypted image and it's histogram

3 Background on Chaotic System

3.1 Chaos

One of the significant fields for study in the area of non-linear dynamic systems is deterministic systems, with irregular behavior, which is also known as the“Chaotic System”. Although chaotic systems and chaotic dynamics have been known for a long time, their importance for a broad range of applications has been taken into consideration only in the recent two decades.

The word ‘Chaos” means disorder, clutter, confusion and irregularity. Theoretically speaking, it is described as regularity in irregularity. This word originates in the recognition of existing secrets and rules of nature and creation. In other words, “a chaotic system” is a dynamic system that has a predictable behavior in a short period of time, but not in a long period of time [15, 16].

3.2 Chaotic system properties

Considering the most significant chaotic system properties, the following items can be referred to:

Chaotic systems are thoroughly defined by deterministic and definite equations. They are not periodic or semi-periodic. In fact, they are very sensitive to primary conditions. Short-term predictions may be precise, yet long-term predictions are absolutely impossible. In addition, using a small control signal they can be controllable. It is also notale that accessing a chaotic system history is impossible. In other words, chaotic systems are invertible [5, 15, 16].

3.3 Chaotic Maps

Chaotic maps are divided into two categories of discrete time chaotic maps such as the tent map, and continuous time chaotic maps such as the Lorenz' Chaotic Map [17].

Yet in another classification, chaotic maps are divided into two categories of one-dimensional and multi-dimensional maps [17].

3.3.1 Logistic Map

One dimensional Logistic maps can be expressed as (6) below [15–17]:

$$f(x_n) = x_{n+1} = r.x_n.(1 - x_n) \qquad (6)$$

Where x_0 is the initial value and r is the control parameter. It has to be noted that for $x_n \in [0, 1]$, the system enters a chaotic state.

3.3.2 Tent Map

One dimensional tent mapping [5, 11, 17] is expressed through the following equation:

$$f(x_n) = x_{n+1} = \begin{cases} \frac{x(n)}{a} & 0 \leq x(n) \leq a \\ \frac{1-x(n)}{1-a} & a \leq x(n) \leq 1 \end{cases} \qquad (7)$$

Where x_0 is the initial value and $x_n \in [0, 1]$. The control parameter $a \in (0, 1)$ and when $a \neq 0.5$, the system enters a chaotic state.

3.3.3 Chebyshev Map

Chebyshev's chaotic map is a one-dimensional chaotic map and its recurrence equation is given as (8) below [5, 11, 17].

$$x_{n+1} = \cos\left(d * \cos^{-1}(x_n)\right) \ \ where\ x_n \in [-1, 1] \quad (8)$$

Where n is the time index, d is the control parameter and x_0 is the initial value. As long as $d \in (1, 5]$, the system remains chaotic.

3.3.4 Saw Tooth Map

Saw tooth chaotic map (Bernoulli's Map) is a one-dimensional chaotic map with the following recurrence equation [5, 17]:

$$x_{n+1} = (b * x_n)\, mod\ 1 \qquad where\ x_n \in [0,1] \quad (9)$$

where n is the time index and b is the control parameter and x_0 is the initial value. As long as $b \in (1,5]$, the function remains chaotic.

3.3.5 Sine Map

As another one dimensional map is the Sine map equation, as shown in (10) below [5, 16, 17].

$$f(x_n) = x_{n+1} = r * \sin(\pi * x_n) \quad -1 < x_n < 1 \quad (10)$$

3.3.6 Henon MAP

Another uni-dimensional chaotic map is the Henon chaotic map function, which can be stated as (11) [5, 16, 18].

$$x_{i+2} = 1 - ax_{i+1}^2 + bx_i \qquad (11)$$

3.3.7 Two-Dimensional CAT MAP

Arnold cat map function is a two-dimensional,map which is stated as (12) [14, 17, 18].

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = (\begin{bmatrix} 1 & c \\ d & cd+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix})\ mod\ (N) \qquad (12)$$

Where c, and d are control parameters and have positive integers.

3.3.8 Three-Dimensional Lorenz MAP

The three-dimensional Lorenz map function is stated in (13) [5, 16].

$$\frac{dx}{dt} = \sigma(x - y) \qquad (13)$$
$$\frac{dy}{dt} = rx - xz - y$$
$$\frac{dz}{dt} = xy - bz$$

Where $t, x, y, z, , r, b \in R$ and $, r, b$ are positive constants.

4 The Proposed Chaotic Image Encryption Scheme

In this section, a new algorithm is proposed for image encryption using tent chaotic map and desired key image. This algorithm works in both frequency and time domains. An analysis of the chaotic functions and their application in encryption systems is presented in Section 4.1. Section 4.2 and Section 4.3 also provide the details of the proposed algorithm.

4.1 An Analysis of the Chaotic Functions and Their Application in Encryption Systems

4.1.1 Relationship Between Chaotic Systems and Encryption Systems

There is a very close relationship between chaotic and encryption systems in various aspects. First, dynamic properties of a chaotic system can be appropriately used in an encryption system. [5, 6, 19].

Chaotic signals are pseudo-random signals: i.e. they seem like a noise, but in fact they can be produced using a predefined key. The relationship between chaotic and encryption systems has been designated in Table 1 [5, 6].

Table 1. Relationship between chaotic systems and cryptosystems

Traditional Cryptosystems	chaotic systems
Confusion	Ergodicity
Diffusion	Sensitivity to initial condition and system parameters
Encryption Key	Parameters
Cipher round	Iteration

Due to the strong relationship between encryption and chaos, chaotic maps have been widely used in encryption systems. There are three practical ways to use chaos theory in an encryption system, as described below:

(1) Using chaotic maps as a source for generating pseudo random bytes with desirable statistical properties for the purpose of materialization of permutation in an encryption system,
(2) Using chaotic maps as a source for generating pseudo random pixels with desirable statistical properties for the purpose of substitution in an encryption system,
(3) Using two chaotic maps for implementation of two operations of permutation and substitution in an encryption system.

Consequently, one may take advantage of Chaos Theory in an encryption system. The primary conditions and parameters of a chaotic map play the role of an encryption key. The iterations in a chaotic map equals to the rounds of an encryption function. Considering the algorithm presented, chaos is used as a source to generate pseudo random pixels for the purpose of materialization of substitution in an encryption system.

4.1.2 Choosing the Most Appropriate Candidate for Generating Pseudo-random Image

In order to choose the most appropriate candidate for generating pseudo random images, a computer simulation has been conducted using some of one-dimensional chaotic maps.

In the algorithm presented in Section 4.2, advantage is taken of one-dimensional chaotic maps. That is because these 1-D maps are simple and fast. The pseudo random images, generated this way, are assessed in terms of security efficiency assessment standards. Then, according to the results given in Table 2, the best candidate for generating pseudo random images is the tent map, which is used in our design.

4.2 Frequency Domain

In the first step of this part, a Fourier transform of the plain image and key image is taken their phase and amplitude are separated. In the second step, **key image** (Each image can be used including usual and normal images or the noise image) **phase** and plain image phase are combined according to (14) which leads into a new phase. Then having combined the new phase and the amplitude of plain image, we arrive at a new image. This image is the ciphered image in the first part [1].

$$PE = (PK + d * PO)/(1 + d) \tag{14}$$

Where PE is the new image phase, PK is the key image phase, and PO is the original(plain) image phase. Parameter d is generated by the chaotic tent map and Exclusively ORed key image pixels.

In order to generate a value for parameter d, first the pixels of the key image are Exclusevely ORed to each other. Then, these values are transferred to the $[0, 1]$ interval. Finally, this value is also added to a random number, generated through tent chaotic function, and divided by 2 to calculate parameter d. In this part, all operations are only applied on the original image phase and its amplitude remains unchanged.

The most important information of each image is located in its phase [20]. For example, let's transform two images into the frequency domain. Then, we alternate their phases provided that their amplitude remains unchanged. Finally, we return them back into the time domain. It is observed that the two images are replaced. That is because the most important information of each image is located in its phase.

Thus, it should be noted that when the respective phase of an image is encrypted, a major part of its information is encrypted as well. In this case, in order to have a more uniform distribution histogram and a stronger encryption system, time domain has been used accordingly.

The block diagram of this stage is depicted in Figure 8.

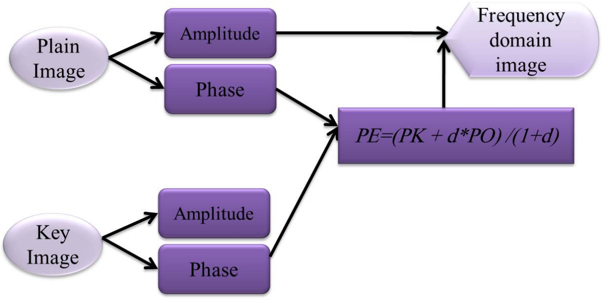


Figure 8. Block diagram of the first operations in the Frequency domain

4.3 Time Domain

In order to access to a more uniform distribution histogram, we add a substitution stage after the pervious stage. Tent map is a kind of chaotic function which is widely used in encryption systems. One dimensional tent mapping [11, 17] can be stated by the following equation:

$$x_{n+1} = \begin{cases} \frac{x_n}{a} & 0 \ \leq x_n \leq a \\ \frac{1-x_n}{1-a} & a \ < x_n \leq 1 \end{cases} \tag{15}$$

Table 2. Comparison of security efficiency of pseudo random images, generated using various chaotic maps

Map	chi-square value	horizontal correlation	vertical correlation	diagonal correlation	correlation coefficient average
Logistic	14920	-0.0044	-0.0033	0.0133	0.0019
Tent	198.4688	-0.1037	-0.0115	-0.0016	-0.0389
Chebyshev	15125	-0.0052	-0.0091	0.0011	-0.0044
Sawtooth	527.875	0.2121	0.0104	0.0188	0.0804
Sine	10047	0.2159	0.0037	0.0085	0.076

Where x_0 is the initial value and $x_n \in [0,1]$. The control parameter $a \in (0,1)$ and when $a \neq 0.5$, the system enters a chaotic state [5, 11, 17].

In the time domain, the ciphered image in the frequency domain is Exclusively ORed to a pseudo random image, produced through a chaotic process. In this process, the chaotic tent map is employed to generate this pseudo random image [1].

Figure 9. illustrates the block diagram of this stage.

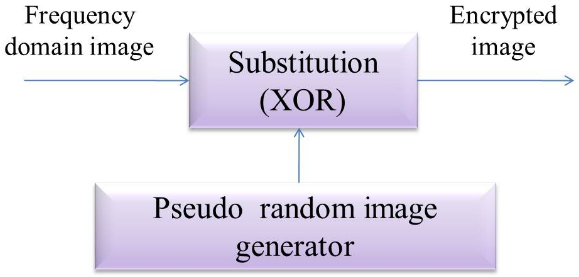


Figure 9. Block diagram of the final operations in the time domain

In this symmetric encryption algorithm, respective components, which are devised to act as a key between the transmitter and receiver, are namely the initial value (x_{d0}) and control parameter (α_d) of the tent chaotic map, used in order to participate in generating parameter d, the initial value (x_0) and control parameter (α) of a tent chaotic map for generating the pseudo random image, the key image (which may be a noise image or a natural image), three arrays of A, B, and C which include trivial information about the encrypted image in frequency domain (the encrypted image of the first phase of encrypting) and the size of these arrays, being shared by the transmitter and the receiver for a more precise reconstruction of the image in the receiver, depending on the dimension of the plain image.

5 Simulations and Security Analysis

A good encryption procedure should be robust against all kinds of cryptanalytic, statistical and brute-force attacks. In this section, an analysis the security of the proposed image encryption scheme is provided which includes the statistical analysis, sensitivity analysis with respect to the key and plain text, key space analysis, etc., in order to prove that the proposed cryptosystem is secure against the most common attacks. To this end, a computer simulation is used to carry out the evaluation procedure. Some experimental results are also reported on, to ensure the efficiency and security of the proposed scheme. In this section, the performance of the proposed chaotic image encryption scheme is thus analyzed using statistical procedures such as Chi-square test of histogram, Correlation Coefficients of pixels (CC), Number of Pixel Change Rate (NPCR), Unified Average Changing Intensity (UACI), Mean Square Error (MSE) and Mean Absolute Error (MAE). Two other criteria for the security analysis are key space and key sensitivity [1, 5, 11].

It is noteworthy here that the proposed algorithm is resistant against the most common attacks. For example, the low Chi-square value of the proposed method is an indicator of its high entropy. That is because information entropy of an image can show the distribution of the gray scale value. In fact, the more uniform the distribution of the gray scale value, the greater the image information entropy. As a result, information leakage in the encryption process is negligible and the encryption system can be concluded as being secure against the entropy attack.

In addition, the high NPCR and UACI test values provide evidence for its resistance against any differential attacks.

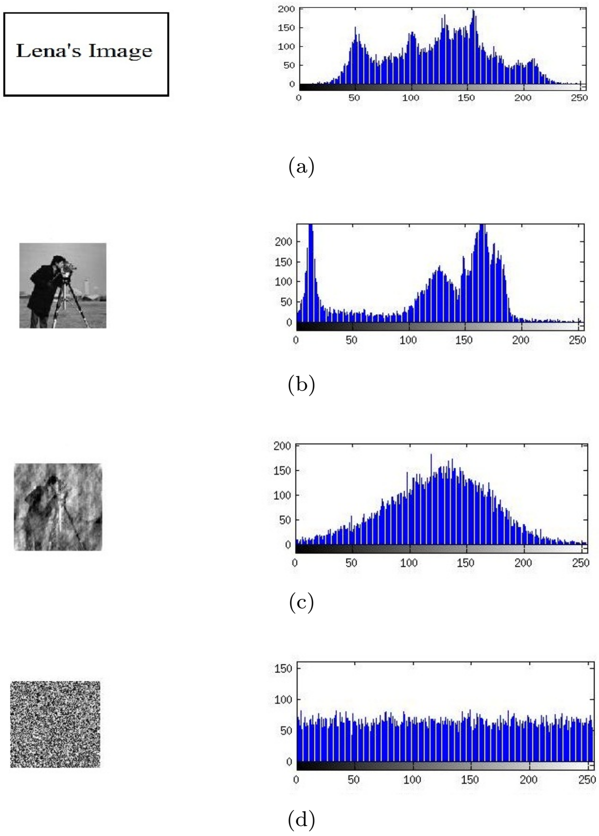
In order to withstand the known-plaintext attack and the chosen-plaintext attack, a tiny change in the plain image should cause a significant change in the cipher image. This can be supported by two performance indices, namely the number of pixel change rate (NPCR) and the unified average changing intensity (UACI).

Besides, the chaos based image encryption technology has the advantage of fast encryption speed and it is strong against known plaintext attack.

Given the select-plaintext attack, some plaintexts with little difference may be selected to analyze the corresponding difference between their cipher texts. Thus, a large difference between cipher texts is expected in order to keep a high security. This is in relation with the key sensitivity and plaintext sensitivity as well.

In addition, for a secure image cipher, the key space should be large enough to make the brute force attack infeasible.

To show an example of an image being encrypted by this algorithm, the plain image, Lena, with the size of 128*128 mp is considered with each pixel having a gray level value between 0 to 255,. Applying the encryption algorithm, where the chaotic tent maps parameters are chosen as $a_d = 0.27$, $x_{d0} = 0.546$, $x_0 = 0.95$ and cameraman as the key image, the encrypted images is produced in the frequency and time domains, as shown in Figure 10.



(a)

(b)

(c)

(d)

Figure 10. (a) Plain image and its histogram, (b) Key image and its histogram, (c) Frequency domain ciphered image and its histogram, (d) Final time domain ciphered image and its histogram.

5.1 Histogram

Chi-square test of a histogram, as expressed by (16), is one of the important criteria in Security Analysis. In fact, this value indicates the uniformity of the histogram. The less the chi-square value of an image, the more uniform the histogram and in turn, the more secure the image encryption system is proved to be.

$$x^2 = \sum_{k=1}^{256} \frac{(O_k - E_k)}{E_k} \tag{16}$$

Where k is the number of gray levels, O_k is the observed occurrence frequencies of each gray level and E_k is the expected occurrence frequency of each gray level. Table 3 reports the values of chi-square test on Lena image.

Histogram analysis is used to illustrate the superior confusion and diffusion properties of the encrypted image. The original image and the encrypted image together with their corresponding histograms are shown in Figure (10a) and Figure (10d), respectively. Comparing these two histograms, we can observe that the histogram of the encrypted image is fairly uniform and is significantly different from that of the original image. And hence, the encrypted images transmitted do not provide any suspicion to the attacker. We can thus conclude that this method can strongly resist histogram based attacks such as the known plaintext attack.

Table 3. Chi-square test results of Lena image

Image	Plain Image	Encrypted Image
Chi-square	10229	206.875

5.2 Correlation Coefficient

Correlation coefficient, as expressed by (18), gives the statistical relationships between two adjacent pixels in vertical, horizontal and diagonal sets. For better resistant of an image encryption system against the statistical attacks, correlation coefficients of pixels in the encrypted image should have low values [5, 11].

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

where

$$D(x) = \frac{1}{\mathrm{N}}\sum_{i=1}^{N}\left(x_i - \frac{1}{\mathrm{N}}\sum_{i=1}^{\mathrm{N}} x_i\right)^2 \tag{17}$$

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

and

$$E(x) = \frac{1}{\mathrm{N}}\sum_{i=1}^{N} Z_i$$

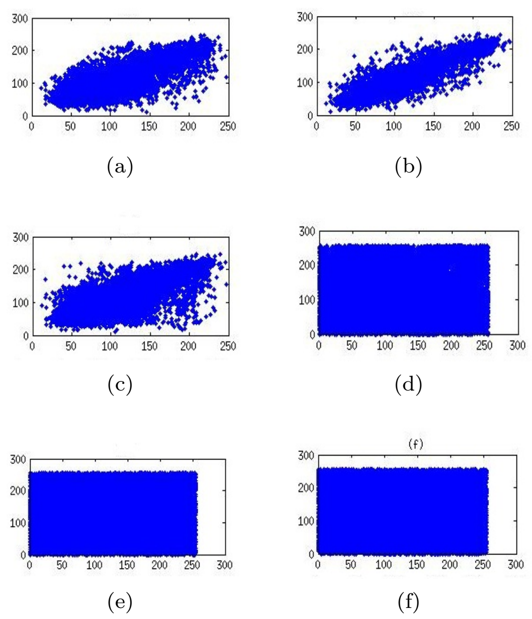
Parameters x and y are the gray levels of two adjacent pixels.

The results of correlation coefficient test of Lena image are summarized in Table 4.

Table 4. Correlation coefficient test results of Lena image

Image Correlation	Plain Image	Encrypted Image
Vertical	0.9527	0.0192
Horizontal	0.8948	-0.0576
Diagonal	0.8563	0.0137
Average	0.9012	0.0301

The correlations between two horizontally, vertically and diagonally adjacent pixels of the plain image are shown in Figure (11a), (11b), and (11c), respectively. The correlation values of the encrypted image are also provided in Figure (11d), (11e), and (11f), respectively.



(a) (b) (c) (d) (e) (f)

Figure 11. (a) Horizontal correlation of the plain image, (b) Vertical correlation of the plain image, (c) Diagonal correlation of the plain image, (d) Horizontal correlation of the encrypted image, (e) Vertical correlation of the encrypted image, (f) Diagonal correlation of the encrypted image

5.3 MSE and MAE

The ciphered image should show a significant difference with the plain image. This difference can be measured with Mean Square Error (MSE) and Mean Absolute Error (MAE) criteria. MSE and MAE values are stated in (18) and (19) respectively [5, 11].

$$MSE = \frac{1}{W * H} \sum_{j=1}^{H} \sum_{i=1}^{W} (a_{ij} - b_{ij})^2 \qquad (18)$$

$$MAE = \frac{1}{W * H} \sum_{j=1}^{H} \sum_{i=1}^{w} |(a_{ij} - b_{ij})| \qquad (19)$$

In the two equations above, parameters W and H are the width and height of the image. a_{ij} is the gray level of the pixel in the plain image and $b_{i,j}$ is the gray level of the pixel in the encrypted image. MSE and MAE values of the encrypted image are reported in Table 5.

Table 5. MSE and MAE test results

Image	Encrypted Image
MSE	7679.7
MAE	72.6360

As can be viewed from the table, MSE and MAE tests have yielded high values which can ensure the resistance of the algorithm against any differential attacks.

In order to withstand the known-plaintext attack and the chosen-plaintext attack, a tiny change in the plain image should cause a significant change in the cipher image.

5.4 NPCR and UACI

Number of Pixel Change Rate (NPCR) is a criterion proportionate to the number of pixels whose gray levels are changed in an encrypted image. NPCR is defined in (20) [5, 11].

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W * H} * 100\%$$

where

$$D(i,j) = \begin{cases} 0 & C_1(i,j) = C_2(i,j) \\ 1 & C_1(i,j) \neq C_2(i,j) \end{cases} \qquad (20)$$

Parameters W and H stand for the width and height of the image. $C_1(i,j)$ and $C_2(i,j)$ signify the gray level of a pixel in a plain image and an encrypted image, respectively.

We have also measured the number of pixels change rate (NPCR) to see the influence of changing a single pixel in the original image on the image encrypted by the proposed algorithm. The NPCR indicates the percentage of different pixel numbers between the two images.

For example, using our encryption scheme, we obtained the NPCR for a LENA image, which was found to be over 99.5%, thereby showing that the encryption scheme is very sensitive with respect to small changes in the plaintext.

The Unified Average Changing Intensity (UACI) value is another criterion which is proportionate to the average changing intensity between the plain image and the encrypted image. The formula can be stated as (21).

$$UACI = \frac{1}{\mathrm{W*H}} * \sum_{\mathrm{i,j}} \frac{|\mathrm{C_1\,(i,j)} - \mathrm{C_2\,(i,j)}|}{255} * 100\% \qquad (21)$$

In (21), parameters W and H are the width and height of the image. $C_1(i,j)$ and $C_2(i,j)$ indicate the gray level of a pixel in a plain image and a ciphered image, respectively. The average value of NPCR and UACI in the encrypted images are shown in Table 6.

5.5 Key space

In order to protect an encryption system against any brute-force attack, it requires to have a large key

Table 6. NPCR and UACI

Image	Encrypted Image
NPCR	99.5728%
UACI	28.4847%

space [5, 11]. In the system proposed here, there are various keys, including the key image, the initial values (x_{d0}, x_0) and the control parameters (a_d, a) of chaotic tent maps. Three arrays of A, B, and C transmit the tiny information of the encrypted image, resulted in the frequency domain, in order to get the best decoded image. The sizes of these arrays depend on the size of the plain image.

Given the above example, at least 64 bits are considered for each key of the tent maps, resulted in a 2^{265} key space. For more security, three arrays of A, B, and C, and the key image can be regarded as keys. As a result, the algorithm is of a large key space to protect the proposed encryption system against any brute-force attacks.

5.6 Key sensitivity

Key sensitivity is one of the important criteria in image encryption algorithms [5, 11]. In order to measure this element in the proposed scheme, we attempted to fix all keys except for the control parameter of one tent map. It was observed that a small change in the control parameter led into a significant change in the decrypted image. The decrypted image with correct keys is illustrated in Figure (12a) with its corresponding shown in Figure (12b).

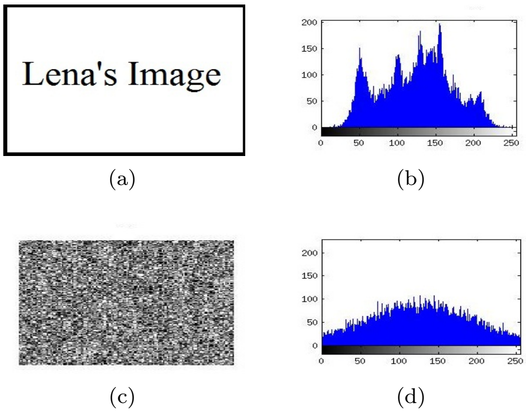
The incorrect decrypted image with $a = 0.4000000000000001$, together with its histogram are also depicted in Figure (12c) and 12(12d), respectively.

High key sensitivity is regarded as one of the requirements to have secure cryptosystems. In other words, the cipher text cannot be decrypted correctly when there is only a slight difference between the encryption or decryption keys. However, this guarantees the security of a cryptosystem against brute-force attacks to some extent.

Moreover, the difference between the cipher texts encrypted by different keys is large enough to keep high security against this kind of known-plaintext attack.

6 Comparison

In order to draw comparisons between the performance of the proposed algorithm and other methods, first the proposed method is used and applied to Lena image for 20 times with different values for keys and its performance is evaluated against the six criteria.



(a) (b)

(c) (d)

Figure 12. (a) Correct decrypted image with a=0.4, (b) Histogram of the correct decrypted image, (c) Incorrect decrypted image with $a = 0.4000000000000001$,(d) Histogram of the incorrect decrypted image.

The averages of these criteria are obtained and reported in Table 7. The six criteria used in this comparison are the Chi-square of histogram, Correlation Coefficients of pixels (CC), Number of Pixel Change Rate (NPCR), Unified Average Changing Intensity (UACI), Mean Square Error (MSE), and Mean Absolute Error (MAE).

In Table 7, the results of the proposed encryption system running on one round can be compared to the other encryption systems, running on one or two rounds. For example, the average results of the proposed algorithm are compared to the results of the Mao algorithm [8] with 1 round of algorithm execution. These results are also comparable to the Xin Zhang [10] algorithm with 2 rounds of algorithm execution.

Two rounds of algorithm execution means the results are obtained in two iterations of the algorithm, which, due to the need for creating an encryption with a higher security, would certainly incur a higher cost compared to a single iteration of implementation. Although an algorithm may produce acceptable results on a given image, it leads to generally undesirable results on different images [3, 7].

Most of the algorithms in the literature have been tested in terms of their performance using only the Lena image. Our algorithm is tested on 9 standard images, including Woman-Darkhair, House Airplane, Peppers, Baboon, Lena, Splash, Lake, and Cameraman. In these tests, the algorithm is applied on each image 8 times with different keys and key images. The proposed algorithm is run only for one iteration in each test and the average of the results obtained from the algorithms operations on each image are summarized in Table 8.

Table 7. Comparison of the proposed method to other methods based on seven criteria

Criteria Schemes	chi-square	MSE	MAE	verage of Correlation Coefficient	NPCR	UACI
Wang *et al.* [21] 1nd round	NA	NA	NA	0.005919	44.27%	14.87%
Mao *et al.* [8] 1nd round	NA	NA	NA	0.03121	37%	9%
Xin Zhang *et al.* [10] 2nd round	NA	NA	NA	0.015	25.00%	8.50%
Borujeni *et al.* [11]	290	NA	35.1	0.13	99.70%	29.30%
Khanzadi *et al.* [12]	243	NA	NA	0.003164	99.61%	33.35%
Zhang *et al.* [22] 1nd round	NA	NA	NA	NA	37.64%	12.70%
Zhang *et al.* [23] 2nd round	NA	NA	NA	0.0411	21.50%	2.50%
Gao *et al.* [24]	NA	NA	NA	0.03786	37%	NA
Wang *et al.* [25] 1nd round	NA	NA	NA	0.0059194	44.33%	14.89%
Average value of proposed method	237.669	7650	72.533	0.0563	99.59%	28.45%

Table 8. The average performance of the proposed method on nine standard images

Criteria Image	Image	Chi-square	NPCR	UACI	CC (average H,V,D)	MAE	MSE
Lena	Lena's Image	225.94	99.59%	28.44%	0.066	72.524	7642.87
Peppers		237.35	99.61%	29.51%	0.046	75.263	8312.75
Camera Man		245.37	99.61%	30.85%	0.055	78.678	9222.12
Splash		245.9	99.61%	30%	0.051	76.519	8651.87
Lake		247.76	99.62%	31.30%	0.054	79.825	9501.5
Baboon		243.79	99.61%	27.09%	0.032	69.096	6738.37
House		244.46	99.61%	28.43%	0.027	72.504	7635.25
Airplane		255.1	99.60%	32.40%	0.019	82.674	1019
Woman		250.19	99.61%	31.69%	0.057	80.81	9749.5
Average		241.526	99.61%	29.72%	0.0262	75.79	7319.8

7 Conclusion

In the present paper, a new algorithm was proposed for image encryption using chaotic tent maps and the desired key image. This algorithm consisted of two parts. The first part of the encryption system worked in frequency domain and the second part in the time domain. In the frequency domain, a desired key image and a parameter of *d* were used to change the phase of the plain image. This changed the pixels value and shuffled the pixels location in time domain.

Besides, a pseudo random image was produced using the chaotic tent map. In the time domain, the image resulted from the frequency domain was combined with this pseudo random image, to generate the final encrypted image.

A computer simulation was also used to evaluate and compare the images encrypted by the proposed algorithm with those of other methods. These comparisons were based on chi-square test of histogram, correlation coefficients of pixels (CC), number of pixel change rate (NPCR), unified average changing intensity (UACI), mean square error (MSE), mean absolute error (MAE), key space, and key sensitivity. The results provided sufficient evidence for the superiority of the proposed chaotic image encryption system over its rivals.

References

[1] E. Hasani, M. Eshghi, "Chaotic Image Encryption In Time and Frequency Domain", 7th Iranian Machine Vision & Image Processing, IEEE conference, 2011.

[2] H. S. Kwok and W. K. S. Tang, "A Fast Image Encryption System Based on Chaotic Maps with Finite Precision Representation", J. of Chaos, Solitons & Fractals, vol. 32, pp. 1518-1529, 2007.

[3] Y. Wang, K. W. Wong, X. Liao and G. Chen, "A New Chaos-based Fast Image Encryption Algorithm", J. of Applied Soft Computing, Vol. 11, Issue 1, pp. 514-522, 2011.

[4] S. Sam, P. Devaraj and R. S. Bhuvaneswaran, "A Novel Image Cipher based on Mixed Transformed Logistic Maps", J. of Multimedia Tools and Applications, Vol. 56, pp. 315-330, 2012.

[5] Kwok Sin Hung, "A Study On Efficient Chaotic Image Encryption Schemes", Department of Electronic Engineering, CITY UNIVERSITY OF HUNG KONG, 2007.

[6] Sh. lian, "MultiMedia Content encryption", Taylor & Francis Group, 2009.

[7] S. M. Seyedzadeh and S. Mirzakuchaki, "A Fast Color Image Encryption Algorithm based on Coupled Two-Dimensional Piecewise Chaotic Map", J. of Signal Processing, Vol. 92, pp.1202-1215, 2012.

[8] Y. Mao, G. Chen, and S. Lian, "A novel Fast Image Encryption Scheme Based on 3D Chaotic Baker Maps", International Journal of Bifurcation and Chaos, vol.14, no.10, pp. 3613-3624, 2004.

[9] Q. Zhou, K-wo. Wong, X. Liao, T. Xiang and Y. Hu, "Parallel image encryption algorithm based on discretized chaotic map", Chaos, Solitons & Fractals, vol. 38, pp.1081-1092, 2008.

[10] X. Zhang, C. Wei-bin "A New Chaotic Algorithm for Image Encryption", ICLIP2008, IEEE conference, 2008.

[11] S.E. Borujeni and M. Eshghi, "Chaotic Image Encryption Design Using Tompkins-Paige Algorithm", J. of Mathematical Problems in Engineering, 2009.

[12] H.Khanzadi, M.Eshghi, "Image Encryption Using Random Bit Sequence Based on Chaotic Maps", submitted to International Journal of Bifurcation and Chaos, 2012.

[13] Sh. Liu, J.Sun, Zhe. Xu, J. Liu, "Analysis on an Image Encryption Algorithm", IEEE Computer society, 2008 International Workshop on Education Technology and Training & 2008 International Workshop on Geoscience and Remote Sensing.

[14] Ch. Wei-bin, X. Zhang, "Image Encryption Algorithm Based on Henon Chaotic System", IEEE, 2009.

[15] K. T. Alligood, T. D. Sauer, J. A. Yorke, "CHAOS: An Introduction to Dynamical Systems", Corrected third printing 2000, Springer-Verlag, New York, 1996.

[16] STEVEN H. STROGATZ, "Nonlinear Dinamics AND Chaos", Perseus Books Publishing, 1994.

[17] H. G. Schuster and Wolfram Just, "Deterministic Chaos", Fourth, Revised and Enlarged Edition, WILEY-VCH Verlag GmbH & Co, 2005.

[18] Y. Heng-fu, W. Yan-peng and T. Zu-wei, "An Image Encryption Algorithm Based on Logistic Chaotic Maps and Arnold Transform", J. of Hengshui University, pp. 40-43, 2008.

[19] H. Khanzadi, M. A. Omam, F. Lotfifar and M. Eshghi "Image Encryption Based on Gyrator Transform Using Chaotic Maps", Signal Processing (ICSP) conference, China, 2010.

[20] Gonzalez and Wood, "Digital Image Processing", 3rd edition, Prentice Hall, 2008.

[21] Y. Wang, K. W. Wong, X. Liao and G. Chen, "A New Chaos-based Fast Image Encryption Algorithm", J. of Applied Soft Computing, Vol. 11, Issue 1, pp. 514-522, 2011.

[22] G. Zhang and Q. Liu, "A Novel Image Encryp-

tion Method based on Total Shuffling Scheme", J. of Optics Communications, Vol. 284, pp. 2775-2780, 2011.

[23] X. Zhang and W. Chen, "A New Chaotic Algorithm for Image Encryption", ICALIP, pp. 889-892, 2008.

[24] H. Gao, Y. Zhang, S. Liang and D. Li, "A new chaotic algorithm for image encryption", J. of Chaos, Solitons & Fractals, vol. 29, pp. 393-399, 2006.

[25] Y. Wang, K. W. W, X. L and G. C, "A new chaos-based fast image encryption algorithm", J. of Applied Soft Computing, vol. 11, pp. 514-522, 2009.

Elham Hasani was born in 1986 in Iran. She received her B.S. degree in Hardware Engineering from Islamic Azad University, Central Tehran Branch, in 2008 and her M.S. degree in Computer Architecture from Islamic Azad University, Science & Research Branch, Tehran, Iran. She is now with the Tehran Municipality ICTO, Applied Science and Technology Center as lecturer. Her main research interest is image encryption systems, security systems and networks.

Mohammad Eshghi (B.S. 78, M.S. 89 and Ph.D. 94) Mohammad Eshghi got his B.S. in Electrical Engineering from Sharif University of Technology in 1978, his M.S. degree in EE from Ohio University, Athens, Ohio, and his Ph.D. in EE from Ohio State University, Columbus, Ohio, USA, in 1989 and 1994 respectively. He is now with the Electrical and Computer Engineering Faculty at Shahid Beheshti University, Tehran Iran. He is the manager of Information and Communication Center in that university. His research interests includ digital signal processing and digital circuit design and implementation on field programmable gates arrays (FPGA).

Appendix

Step1: calculate d parameter:

```
for m=1:128
   for n=1:128
      Split key image pixels;
   end
end
for I=1:(128*128)
  L= bitxor( key image pixels);
end
Calculate d1= (L/255);
Calculate d2 from TENT MAP;
Calculate d= (d1+d2)/2;
 if (d>1)
   d=1;
else
   d=d;
end
```

Step2: Encrypt the image:

```
Initialize the parameters;
Calculate a random image using a tent map;
Transfer the original image to frequency domain;
Split phase and amplitude of original image;
Transfer the key image to frequency domain;
Split phase and amplitude of key image;
Calculate the new phase;
Calculate the primitive encrypted image in the
     phase domain;
Calculate the final encrypted image by XORing
     the primitive encrypted image in the time
     domain and pseudo random image;
```

The ISC Int'l Journal of Information Security

ISeCure

January 2013, Volume 5, Number 1 (p. 116)

http://www.isecure-journal.org

Persian Abstract

رمزنگاری تصویر براساس تابع آشوبناک خیمه در حوزه‌های فرکانس و زمان

الهام حسنی[۱] و محمد عشقی[۲]

[۱]مرکز آموزش سازمان فناوری اطلاعات و ارتباطات شهرداری تهران

[۲]عضو هیأت علمی دانشکده برق و کامپیوتر دانشگاه شهید بهشتی

در این مقاله، به ارائه‌ی یک الگوریتم رمزنگاری تصویر با استفاده از تابع آشوبناک خیمه و یک تصویر کلیدی دلخواه پرداخته‌ایم. این الگوریتم از دو بخش تشکیل شده است. بخش اول الگوریتم در حوزه‌ی فرکانس و بخش دوم، در حوزه‌ی زمان کار می‌کند. در حوزه‌ی فرکانس از یک تصویر کلیدی دلخواه و یک عدد تصادفی که توسط نگاشت آشوبناک خیمه تولید شده است برای ایجاد تغییر در فاز تصویر اصلی استفاده می‌شود که نتیجه‌ی آن در حوزه‌ی زمان باعث تغییر و به هم ریختن مکان پیکسل‌ها می‌شود. در پایان در حوزه‌ی زمان از یک تصویر شبه تصادفی که توسط نگاشت آشوبناک خیمه تولید شده است برای ترکیب آن با تصویر حاصل از حوزه فرکانس و رمزنگاری استفاده می‌شود. از شبیه‌سازی کامپیوتری برای ارزیابی کارایی و امنیت الگوریتم و مقایسه نتایج حاصل از تصاویر رمزشده با دیگر کارهاي صورت گرفته استفاده‌شده‌است. معیارهای ارزیابی کارایی عبارتند از تست‌چی‌دو از هیستوگرام، ضریب همبستگی پیکسل‌ها، ضریب تعداد تغییر پیکسل‌ها، میانگین تفاوت سطح خاکستری پیکسل‌ها، میانگین مجذور اختلاف سطح خاکستری تصویر اصلی و رمز شده، میانگین قدر مطلق اختلاف سطح خاکستری تصویر اصلی و رمز شده، فضای کلید و حساسیت به مقادیر اولیه. نتایج مقایسات حاکی از کارایی و امنیت بالاتر الگوریتم رمزنگاری تصویر ارائه شده است.

واژه‌های کلیدی: رمزنگاری تصویر، نگاشت آشوبناک خیمه، تصویر کلیدی، حوزه فرکانس، حوزه زمان.