New image encryption algorithm based on block chaotic encryption

Prof.Dr.Hilal Hadi Saleh[1]   Dr.Luma Fayeq Jalil[2]
Ekhlas Abass Albhrany[3]

[1,2], Department of Computer Science, University of Technology, Baghdad
[3] Department of Computer Science, Mustansiriyah University, Baghdad, Iraq,
e-mail: akhlas_abas@yahoo.com,dr_lumafaik79@yahoo.com,
hhsrq888@yahoo.com.

Abstract.

In this paper, we propose new image encryption algorithm based on block chaotic cipher. *Algorithm*, A new block cipher algorithm is introduced, which encrypts and decrypts a block size of 64 (8×8) byte. In this algorithm, we used S-box that we previously designed by using 2d logistic map and cross chaotic map. Each block is first permuted by using standard map and then substituted by the bytes in S-box. The resulted block is then Xored with the key. A random key generator based on tent map is proposed to generate the key sequences that used in the encryption and decryption process. *Results***,** the result from key space analysis, differential attack analysis, information entropy analysis, correlation analysis of two adjacent pixels have proven that the proposed algorithm can resist cryptanalytic, statistical and brute force attacks, and achieve higher level of security.

Keywords: Image encryption, block chaotic cipher, 2d logistic map, cross map, S-Boxes, tent map.

خوارزمية جديدة لتشفير الصورة تعتمد على التشفير الكتلي الفوضوي

د.هلال هادي صالح   د.لمى فائق جلال   اخلاص عباس البحراني

الملخص.

في هذا البحث، تم اقتراح خوارزمية جديدة لتشفير الصور على أساس التشفير الكتلي الفوضوي. خوارزمية التشفير الكتلي التي تم اقتراحها تشفر وتحلل كتلة بحجم byte (8×8) 64 من البايت. في

هذه الخوارزمية، استخدمنا S−box الذي تم تصميمه سابقا باستخدام معادلة التحويل اللوجستية ذات البعدين ومعادلة العبور للفوضى. أولاً كل كتلة تبدل ترتيب عناصرها باستخدام معادلة التحويل القياسية ثم يتم اجراء عملية التعويض للبايتات باستخدام S−box. ثم الكتلة الناتجة يتم دمجها بالمفتاح باستخدام عملية الXored. مولد مفتاح عشوائي يعتمد على معادلة خيمة الفوضوية تم اقتراحه ليولد سلاسل المفاتيح الرئيسية التي تستخدم في عملية التشفير وفك التشفير .النتائج التي تم الحصول عليها قد أثبتت ان تحليل أساسي الفضاء، تحليل الهجوم التفاضلي، تحليل كمية المعلومات، تحليل ارتباط البكسل المتجاورة ، أن الخوارزمية المقترحة يمكن أن تقاوم هجمات القوة الإحصائية و هجوم القوة العنيف ، وتحقيق مستوى أعلى من الأمان.

الكلمات المفتاحية : تشفير الصورة، التشفير الكتلي الفوضوي ، معادلة التحويل اللوجستية ذات البعدين ، معادلة التحويل القياسية ، S−Boxes ، ومعادلة العبور التحولية.

Introduction

The principle motivation behind this paper to plan a novel block image encryption algorithm by using chaos theory. Chaos theory reliably assumes a dynamic part in current cryptography. The primary point of interest of the chaos-based method lies on the arbitrary behavior and the affectability to the control parameters and initial conditions. An important difference between chaos and cryptography lies on the fact that systems used in chaos are defined only on real numbers [1], while cryptography deals with systems defined on finite number of integers [2]. The close relationship between chaotic maps and cryptosystems has been observed in [3,4,5]. This relationship can be built up: ***first*** ergodicity in chaos versus confusion in cryptography. ***Second:*** sensitive reliance on beginning conditions and control parameters of turbulent maps versus dissemination property of a decent cryptosystem for a little alters in the plaintext and in the mystery key. ***Third:*** chaotic random-like behavior can be used for producing pseudorandom sequences as a key in cryptography.

Many scholars have made efforts to investigate block encryption algorithm in order to promote short processing time in encryption and decryption. In [6] a block encryption was proposed that creates chaos based ciphers by using a systematic procedure. Two well-known chaotic maps, exponential and logistic maps are used in this procedure. The reference [7] has proposed a block encryption algorithm where different encryption key value is generated for each block to resist the differential and linear cryptanalysis. In [8,9], they have proposed a symmetric key block cipher algorithm using a one-dimensional and multiple one dimensional chaotic maps. In 2006 [10] they developed a block cryptosystem based on iterating a chaotic map. In this paper, a new block chaotic cipher system for image encryption is suggested. In the proposed algorithm consist of five transformations which implemented based on the chaotic system.

The remaining part of the paper is sorted out as takes after: section 1 the basic theory of the chaotic functions, section 2 the propped algorithm. Section 5 presents the statistical analysis. The security analysis of the generator is achieved in Section 6, before conclusions.

1. Basic theory.

In this paper we used five chaotic maps: cross map, 2d logistic map, cat map, standard map and tent map.

1.1 Cross map.

Cross-chaotic map is defined as following:

$$\chi_{i+1} = 1 - \mu y^2$$
$$y_{i+1} = \cos(k.\cos^{-1}\chi_i), \chi, y \in [1.-1] \qquad (1)$$

Where μ and k are the control parameters of the system, respectively. When μ=2 and k=6, this system exhibits a great variety of dynamics behavior [12].

1.2 2D logistic map.

One of the most known and widely used chaotic systems is the 1D Logistic map, which is defined as follows [13]: -

$$\mathrm{f(x)} = \mu\chi(1-\chi) \qquad \chi \in (0,1) \qquad (2)$$

where μ is the control parameter. The system is in chaos on condition that 3.569<μ<4.0.

1D logistic map is extended to the 2D logistic map. The extended logistic map has extensive key space and more reliance on control parameters. The extended logistic map, it is more complex to estimate the secret information. It additionally indicates more amount of chaotic behavior on the producing of sequence [14]. In overall, it increases the complexity of the algorithm. The 2D logistic map is defined as follows: -

$$f(x) = \begin{cases} \chi_{i+1} = \mu_1 \chi_i (1 - \chi_i) + \gamma_1 y_i^2 \\ y_{i+1} = \mu_2 y_i (1 - y_i) + \gamma_2 (\chi_i^2 + \chi_i y_i) \end{cases} \tag{3}$$

When 2.75 <μ_1<=3.4, 2.75 < μ_2<=3.45, 0.15 <γ_1<=0.21, 0.13 <γ_2<=0. 15, the system is in chaotic state and can generate two chaotic sequences in the region (0, 1].

1.3 Cat Map.

A 2D Cat map is first presented by V.I. Arnold in the research of ergodic theory [15]. Let the coordinates of a positions P = {(x, y) | x, y = 1, 2, 3, . . ., N}, a 2D Cat map with two control parameters is as follows [15]:

$$\begin{cases} x' = (x + ay) mod\ N \\ y' = (bx + (ab + 1)y) mod\ N \end{cases} \tag{4}$$

Where, a, b are control parameters which are positive integers and (x′, y′) is the new position.

1.4 Standard map.

The so-called standard map was introduced in [16], [17], and is described by: -

$$\begin{cases} a_{i+1} = (a_i + b_i) mod\ 2\pi\ , \\ b_{i+1} = (b_i + K \sin(a_i + b_i)) mod\ 2\pi, \end{cases} \tag{5}$$

here the both ith states a_i and b_i take real values in [0,2π) for all i and K is the control parameter and k > 0. The standard map was discretized in a directed manner by exchanging x = aN/2 π, y = bN/2π, K = kN/2π into Eq. (4), which maps from [0,2 π) * [0,2π) to N * N. After discretization, the map becomes

$$\begin{cases} x_{i+1} = (x_i + y_i) mod\ N\ , \\ y_{i+1} = (y_i + K \sin \dfrac{x_{i+1} N}{2\pi}) mod\ N\ , \end{cases} \tag{6}$$

where K is a positive integer. This discretized map properties may not be as good as the original one, but it can be executed in the integer domain, which reduces the computational complexity. In addition it is more appropriate for real-time data encryption. The standard map is used to implement data permutation [17].

In the standard map the corners pixels of a square image have some particular properties. For example, after any number of iterations, the pixel at location (0, 0) stays unchanged. In order to avoid it, [18] a method to avoid this weakness, the location of pixels at the corners (0, 0), (N- 1, 0) , (N- 1,N - 1) and(0,N -1) is modified. That is, the normal scan order is changed into a random one. After the iteration of chaotic map, an arbitrary-pair (r_x, r_y) is created, which represents the location of an arbitrary chosen pixel in the square image.

The two parameters r_x and r_y both belong to range [0.. N-1] and the modified chaotic map becomes

$$\begin{cases} x_{i+1} = \left(x_i + r_x + y_i + r_y\right) mod\ N\ , \\ y_{i+1} = (y_i + r_y + K \sin\frac{x_{i+1}N}{2\pi}) mod\ N. \end{cases} \quad (7)$$

1.5 Tent map.

Tent map is a discrete time chaotic system described by relation [19]:-

$$\mathrm{x}_{\mathrm{n}+1} = \mathrm{f}(\mathrm{x}_{\mathrm{n}}) = \begin{cases} \frac{\mathrm{x}_{\mathrm{n}}}{\mathrm{a}}, & \text{if } \mathrm{x} \in [0, \mathrm{a}], \\ \frac{(1-\mathrm{x}_{\mathrm{n}})}{(1-\mathrm{a})}\ , & \text{if } \mathrm{x} \in (\mathrm{a}, 0] \end{cases} \quad (8)$$

where, a $\in$ [0,1] is the control parameter and x_n is the current state of the system. Tent map has uniform invariant probability density in [0, 1] interval.

2. The proposed algorithm.

In this Section, we describe the proposed image encryption algorithm in details. The algorithm consists of two major algorithms: encryption algorithm and decryption algorithm. Each algorithm has three main steps which are:-

- **First**: - Create the Substitution S-Boxes.
- **Second**: - Generation of pseudorandom key K.
- **Third:** - encrypt/decrypt the plain image.

We will describe each step in details in the next section.

2.1 Create the Substitution S-Boxes.

In this algorithm, we create S-box using the method in [20]. The proposed S-box is a table of 16 × 16 integer values (256 bytes). The S-box is created by using 2d logistic map and cross map.

2.2 Generation of pseudorandom key K.

The core of the pseudorandom key is the tent chaotic map. Four integer numbers are generated in each round of the generator. The main idea of the proposed generator consists of the following major steps:-

- **Step 1**: the initial condition (x_0) and control parameters (a) are input to the Tent map. These numbers are floating point numbers where the precision is 10^{-16} for each of x_0 and a, considered as the keys of the generator.
- **Step2:** iterate tent map two times. The two outputs are Xored to produce one output.
- **Step3:** the resulted floating number output is translated to binary sequence of random length.
- **Step4**: the binary sequence is translated to four integer numbers. Each number is in the rang [0..255]. The first number (8-bit number) is started from the bit at the location (1) of the sequence. The second number is started from the bit at the location (10) of the sequence. The third number is started from the bit at the location (20) of the sequence. The last number is started from bit at the location (30) of the sequence.
- **Step5**: repeat from step 2 until the desired number of integer numbers is reached. When the number of generated keys of one block (64 byte) plus to the control values and parameters of chaotic maps (standard map (r_1, r_2, k) and cat map (a, b)) is reached to 69 byte, the parameters of tent map x_0 and a are modified using simple addition operation between the initial and last value of these parameters in order to increase the complexity of detect the keys.

2.3 Encryption algorithm.

We propose a new scheme that has fast performance speed and high level security. The design tools of our scheme are based on chaotic map with non-linear transformation functions. The main steps of the proposed encryption algorithm are (as shown in figure 2):-

- **Step1**: Input the original image ($Pm \times n$), the initial parameters (x_0,y_0) to create the S-box and the control value(a) and the initial parameter (x_0) and control value(a) for the pseudorandom key. These parameters numbers are floating point numbers where the precision is 10^{-16} and considered as the keys of the algorithm.

- **Step2**: create the S-box.
- **Step3**: generate the pseudorandom key by using the algorithm discussed in the section 2.2. The generated key is transformed into blocks $K_1K_2K_3K_4.....K_t$, where B_i ($1\leq i \leq t$) denotes the i-th key block with size 8×8 byte. In addition, for each block five parameters that are necessary for permutation using standard map and form byte substituted in S-box are generated also by this pseudorandom generator.
- **Step4**: The original image ($Pm\times n$) is reshaped or transformed into $P(m\times n)\times 1$ which is a one dimensional array.
- **Step5**: P array is divided into blocks $B_1B_2B_3B_4.....B_t$, where B_i ($1\leq i \leq t$) denotes the i-th image block with size 8×8 pixels. When the last block of the image is less than 8×8 pixels, it treats as one dimensional array B ($1\times L$) where L is the number of pixels in this block.
- **Step6**: for each block do four transformation :-

❖ Getting transformation: get the red, green and blue value of each pixel in the block.

❖ Permutation transformation: each (red, green and blue) block is diffused using standard map.

❖ Mixing transformation: each byte is Xored with the byte in the key block.

❖ Substitution transformation: each byte in the resulted (red, green, blue) block is substituted using S-box.

❖ Gathering transformation: the resulted three blocks (red, green and blue) are gathered to produce one encrypted block which is inserted to the encrypted image.

- **Step7**: the output encrypted image is saved in file.

2.4 Decryption algorithm.

The main steps of the decryption algorithm are:-

- **Step1**: Input the encrypted image ($Cm\times n$), the initial parameters (x_0,y_0) to create the S-box and the control value(a) and the initial parameter (x_0) and control value(a) for the pseudorandom key.
- **Step2**: create the S-box in the method discussed in [20].
- **Step 3**: generate the pseudorandom key by using the algorithm discussed in the section 2.2. The generated key is transformed into blocks $K_1K_2K_3K_4.....K_t$, where B_i ($1\leq i \leq t$) denotes the i-th key block with size 8×8 byte. In addition, for each block five parameters that are necessary for inverse permutation using standard map and form inverse byte substituted in S-box, are generated also by this pseudorandom generator.

- **Step4**: The encrypted image ($Cm\times n$) is reshaped or transformed into $C(m\times n)\times 1$ which is a one dimensional array.
- **Step5**: C array is divided into blocks $B_1B_2B_3B_4.....B_t$, where B_i ($1\leq i \leq t$) denotes the i-th image block with size 8×8 pixels. When the last block of the image is less than 8×8 pixels, it treats as one dimensional array B ($1\times L$) where L is the number of pixels in this block.
- **Step6**: for each block do four transformation :-

❖ Getting transformation: get the red, green and blue value of each pixel in the block.

❖ Invers Substitution transformation: each byte in the resulted (red, green, blue) block is substituted using inverse substitute S-box.

❖ Mixing transformation: each byte is Xored with the byte in the key block.

❖ Invers Permutation transformation: each (red, green and blue) block is return to its original positions using inverse standard map.

❖ Gathering transformation: the resulted three blocks (red, green and blue) are gathered to produce one original block which is inserted to the image.

- **Step7**: the output original image is saved in file.

3. Experiment result.

In this paper, the proposed algorithm encrypted bitmap color image by using Delphi 6 programming language. It take any bitmap image with size (m x n) is less than or equal to 500 x 500 pixels. We give some experimental results of the proposed encryption algorithm. Set the original image is 125 × 125 color image Lena, the initial values for creating the S-box are x_0=0.9567432612000124, y_0=0.5550087650432133 and finally the initial value and control value for generating pseudorandom keys are xx_0=0.7665000000002211 and a=0.2768595554321701.

Figure ١(a) shows the original image and (b) the encrypted image. As can be seen from the figure, there is no patterns or shadows visible in the corresponding cipher text.

4. The security and analysis.

In this section, we will discuss the security analysis on the proposed encryption algorithm.

4.1 Key space analysis.

In order to make brute-force attacks infeasible, the proposed algorithm ought to have an extensive key space. The size a key space that is smaller than

2^{128} is not secures enough [21]. Here, the key space is constructed form the parameters that needs for creating the S-box (initial values x_0 and y_0) and the initial and control values (xx_0 and a) that are needed for generating the key. These parameters are floating point numbers. Where x_0, y_0, xx_0 and a $\in[0, 1]$. If the precision is 10^{-16} for each of parameters, the total space of keys for initial conditions and control parameters is $2^{213}((10^{16})^4)$. The key space is sufficiently expansive to oppose a wide range of brute-force attacks.

4.2 Statistical attack analysis.

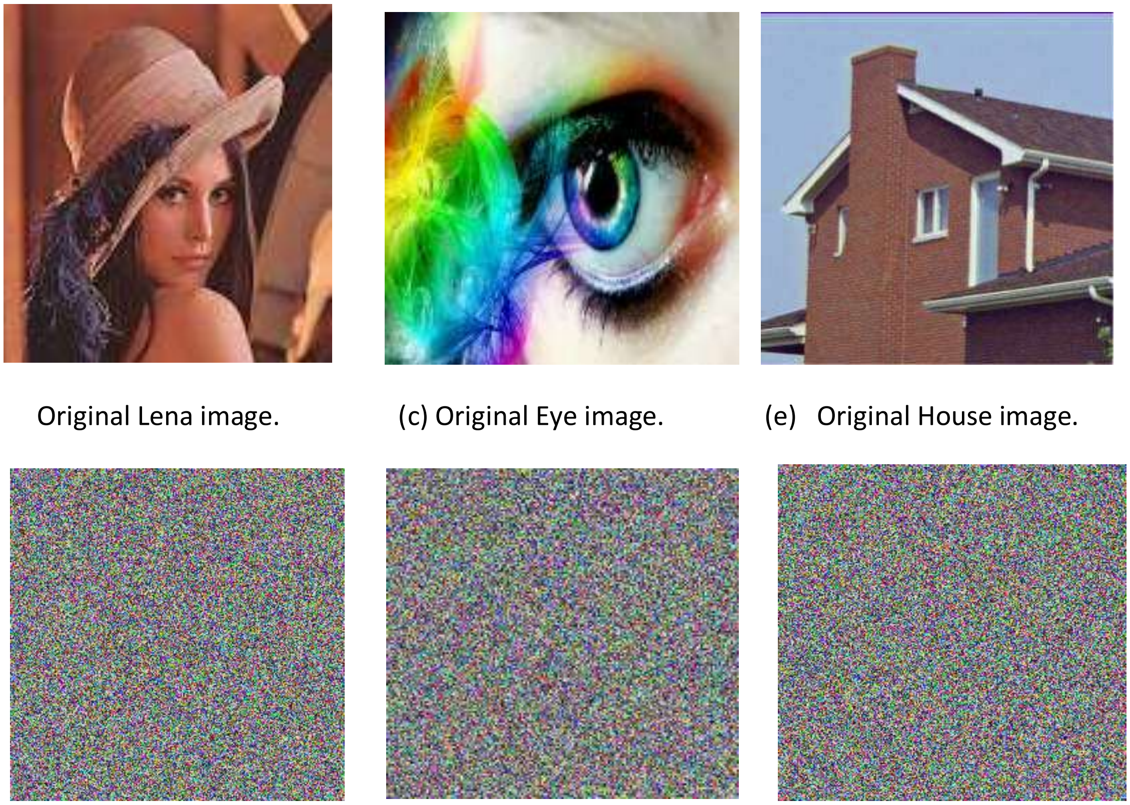
The statistical analysis of the original image and the encrypted image can be considering by:

1. Histogram analysis: the histogram shows the number of pixels for any grey value in the image [10]. By taking images a (255×255) sized “House” and “Lena” images as original images, the histogram of the original images and corresponding cipher images are shown in Figure ٢. As can be seen from Figure ٢, the histogram of the output cipher image is fairly evenly distributed over the scale, and therefore no information about the plain image can be gathered through histogram analysis.
2. Correlation coefficient analysis: the correlation between two diagonally, two horizontal and two vertical. adjacent pixels are analysis in “House”, “Lena” and “Eye” cipher images. We choose 3000 pair of adjacent pixels (horizontal, vertical, and diagonal) from original image and encrypted image. The correlation can be analyzed by using the following relation: -

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)\sqrt{D(y)}}} \qquad (13)$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}\big(x_i - E(x)\big)\big(y_{i\_}E(y)\big) \qquad (14)$$

where cov(x,y) is covariance, D(x) is variance, x and y mean estimations of two contiguous pixels in the image. In numerical computation, the following discrete forms were used: -



Original Lena image. (c) Original Eye image. (e) Original House image.

(b) Encrypted Lena image. (d) Encrypted Eye image. (f) Encrypted House image.

Figure ١4: (a) the original Lena image, (b) the encrypted Lena image, (c) original Eye image and (d) the encrypted image, (e) Original House image and (f) Encrypted House image.

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \qquad (15)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2 \qquad (16)$$

In the results Table ١; we found that the correlation coefficients of the encrypted images are very small. These correlation analyses confirm that the chaotic encryption algorithm satisfies zero co-correlation, indicating that the attacker cannot obtain any valuable information by exploiting a statistic attack.

4.3 Differential attack analysis.

A good encryption algorithm that avoids the known-plaintext attack and the chosen-plaintext attack should have the desirable property where small difference of the plaintext should be diffused to the whole cipher text. In differential attack, attackers often make a small change for the plain image, and utilize the proposed algorithm to encrypt for the plain image before and after changing, through contrasting two ciphered images with figure out the relationship between the plain and the ciphered images. Two common measures that examine the effect of changing one pixel in the original image are called number of pixels change rate (NPCR) which computes the different pixel numbers between two images and unified average changing intensity (UACI) which measures the average intensity of differences between two images. For calculation of NPCR and UACI, let us assume two encrypted images E_1 and E_2 whose relating plain images have only one-pixel contrast. Label the pixels gray-scale values at matrix (i, j) of E_1 and E_2 by E_1 (i, j) and E_2(i, j), respectively. A bipolar array D is defined with the same size as image E_1 or E_2 and D (i, j) is controlled by E_1(i, j)) and E_2(i, j), namely : -
In the event that E1(i, j) = E2(i, j) then D(i, j) = 0
Else
D(i, j) = 1
NPCR is defined by the following formulas:-

$$\text{NPCR} = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%, \qquad (17)$$

$$\text{UACl} = \frac{1}{W \times H}\left[\sum\nolimits_{i,j} \frac{|E_1(i,j) - E_2(i,j)|}{255}\right] \times 100\% \qquad (18)$$

where H and W are the height and width of E_1 or E_2.

Tests have been performed on the proposed algorithm by considering the one-pixel change influence on a 256-gray scale image. The encryption algorithm is performed on the modified original image and then the two measures NPCR and UACI are computed as shown in table ٢. The results show that a small change in the original image will result in a great change in the encrypted image; this implies that the proposed algorithm has an excellent capability to resist the differential attack.

Table ١ . Results of correlation analysis of the proposed image cryptosystem.

Direction	Lena plain image	Lena cipher image	Eye plain image	Eye cipher image	House plain image	House cipher image
Horizontal	**0.9910003**	**-0.030251**	**0.9680413**	**0.0102630**	**0.9142616**	**0.0254514**
Vertical	**0.9791627**	**-0.008243**	**0.9859404**	**0.0267262**	**0.913436**	**-0.018279**
Diagonal	**0.9648011**	**0.0034598**	**0.9613318**	**0.0163779**	**0.8936788**	**0.0233949**

Table ٢. : Results of NPCR and UACI tests

Image name	The point	Old point value	New point value	NPCR (%)	UACI (%)
Lena cipher image	**(36,140)**	**185**	**186**	**99.61553248**	**33.59936072**
Lena cipher image	**(150,210)**	**98**	**99**	**99.61553248**	**33.59954768**
House cipher image	**(36,140)**	**179**	**180**	**99.64321414**	**33.54488394**
House cipher image	**(150,210)**	**65**	**66**	**99.64321414**	**33.54539656**
Eye cipher image	**(36,140)**	**199**	**200**	**99.55323458**	**33.54280499**
Eye cipher image	**(150,110)**	**88**	**89**	**99.55323458**	**33.54325662**

4.4 Information Entropy Analysis.

Information theory is a scientific hypothesis of information correspondence and capacity. The nature of picture encryption is generally measured by the Shannon entropy over the cipher image. The information entropy H(m) of a plaintext message m can be calculated as [23]: -

$$H(m) = \sum_{i=1}^{N} p(m_i) \log_2 \frac{1}{p(m_i)} \qquad (19)$$

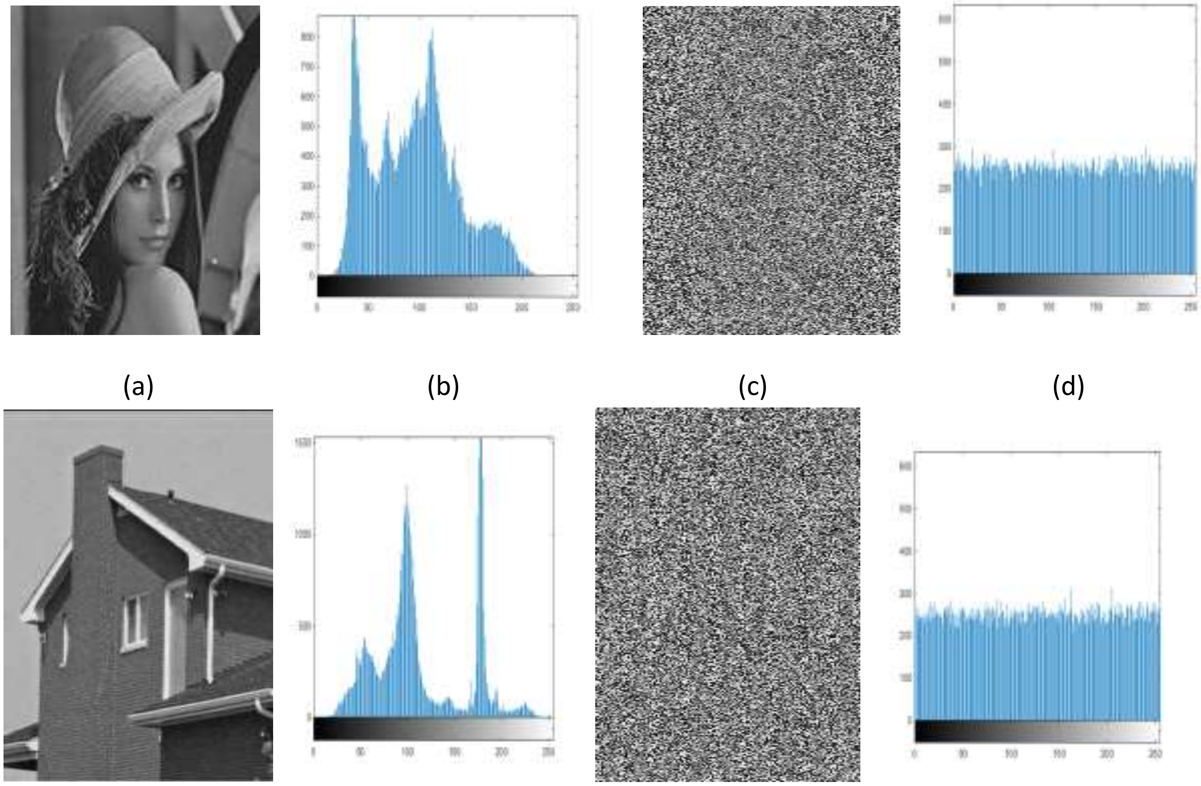
where $p(m_i)$ represents the probability mass function of message m_i and n=256 for image. If every gray value in a 256-gray-scale image has an equal probability, then information entropy equals to 8, indicating that the image is a purely random one. When the information entropy of an image is less than 8, there exists a certain degree of predictability, which will threaten its security. Therefore, we strive for an entropy value of the encrypted image to be close to the ideal value of 8 so as to withstand the entropy attack effectively. The entropy for the three cipher images (Lena, House and Eye) are showed in table ٣. All the entropy values are close to 8 this means that the cipher-image is close to a random source and the proposed scheme is secure against the entropy attack.

Table ٣. . Results of entropy analysis of the proposed image cryptosystem.

Entropy value	**Lena cipher image**	**House cipher image**	**Eye cipher image**
	7.99655	**7.99595**	**7.99538**

5. Conclusion.

In this paper, new color image encryption scheme based on combination of a chaotic map and block cipher is presented. The main idea is to encrypt and decrypt a block size of 8X8 byte (64byte) based on permutation and substitution the byte in S-box. A random key generator based on tent map generates key sequences that used in the encryption and decryption process. Security analyses indicate that the proposed algorithm has desirable properties such key space analysis; statistical attack analysis and differential attack analysis are performed numerically and visually. All the experimental results show that the proposed encryption scheme is secure because of its **large key space**; it’s **highly sensitivity** to the cipher keys and plain-images. The proposed scheme is easy to control and it can be actualized to any color or gray images with unequal width and height as well. All these agreeable properties make the proposed algorithm a potential possibility for encryption of multimedia data such as images, audios and even videos.



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

(e) (f) (g) (h)

Figure ٢. Histograms analysis. (**a**) Lena plain image. (**b**) histogram of (**a**). (**c**) encrypted image. (d) histogram of (c). (e) House plain image. (f) histogram of (e). (g) encrypted image. (h) histogram of (g).

References

[1] J. Gickenheimer and P. Holmes, "Nonlinear Oscillations, Dynamical Systems and Bifurcations of Vector Fields". Berlin, Germany: Springer, 1983.

[2] B. Schneier, Applied Cryptography: "Protocols, Algorithms, and Source Code in C". New York: Wiley, 1996.

[3] Fridrich, J. (1998). "Symmetric ciphers based on two-dimensional chaotic maps". International Journal of Bifurcation and Chaos, 8(6), 1259-1284.

[4] Kocarev, L. (2001). "Chaos-based cryptography: A brief overview. IEEE Circuits and Systems Magazine", 1(3), 6-21.

[5] Wang, X.Y. and Q. Yu, 2009. "A block encryption algorithm based on dynamic sequences of multiple chaotic systems". Commun Nonlinear Sci. Num. Simulat., 14: 574-581. DOI: 10.1016/j.cnsns.2007.10.011.

[6] Lee, C.D., B.J. Choi and K.S. Park, 2004. "Design evaluation of a block encryption algorithm using dynamic key mechanism". Future Generat, Comput.Syst., 20: 327-338. DOI: 10.1016/S0167-739X(03)00148-1.

[7] Pareek, N.K., V. Patidar and K.K. Sud, 2003. "Discrete chaotic cryptography using external key". Phys. Lett. A., 309: 75-82. DOI: 10.1016/S0375-9601(03)00122-1.

[8] Pareek, N.K., V. Patidar and K.K. Sud, 2005." Cryptography using multiple one-dimensional chaotic maps". Commun. Nonlinear Sci. Numerical Simulat., 10: 715-723. DOI: 10.1016/j.cnsns.2004.03.006.

[9] Xua, S., J. Wang and S. Yang, 2008." A novel block cipher based on chaotic maps". Proceedings of the 2008 Congress on Image and Signal Processing, May 27-30, IEEE Xplore Press, Sanya, China, pp: 17-21. DOI: 10.1109/CISP.2008.409.

[10] Radha, N. and M. Venkatesulu, "A Chaotic Block Cipher for Real-Time Multimedia". Journal of Computer Science 8 (6): 994-1000, 2012 ISSN 1549-3636.

[11] Ling Wang, Quen Ye Yaoqiang, Yongxing zou , Bo Zang, "An Image Encryption Scheme based on cross chaotic map" 2008 IEEE

[12] Manisha Raj1 and Shelly Garg, 2014. "An Innovative Approach: Image Encryption with Chaotic Maps using DNA Addition Operation". International Journal of Software and Web Sciences, IJSWS 14-337; ISSN (Print): 2279-0063.

[13] Musheer Ahmad and M. Shamsher Alam, "A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping", International Journal on Computer Science and Engineering, vol. 2(1), 2009, pp. 46-50.

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

[15] Jackson EA.(1991). “Perspectives in nonlinear dynamics”. Cambridge: Cambridge University Press.

[16] Rannou F.(1974). “Numerical study of discrete plane area-preserving map”. A stron Astrophys:289–301.Lian, Jinsheng S., Zhiquan W. (2005). “A block cipher based on a suitable se of the chaotic standard map”. Chaos, Solitons and Fractals 26, 117–129.

[17] Luca, A. Ilyas, A. Vlad, “Generating Random Binary Sequences Using Tent Map”. Proc. IEEE Int. Symposium on Signals, Circuits and Systems (ISSCS), Iasi, Romania, June 30-July 1, 2011, pp. 81-84.SSN.

[18] Janke, W. (2002). “Pseudo random numbers: generation and quality checks”. Quantum Simulations of Complex Many-Body Systems, 10, 447–458.

[19] F. J. Luma , H. S. Hilal and A. Ekhlas(2015). “ New Dynamical Key Dependent S-Box based on chaotic maps”. IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 4, Ver. IV (July – Aug. 2015), PP 91-101

[20] X. Tao, X. F. Liao, G. P. Tang, "A novel block cryptosystem based on iterating a chaotic map.” Physics Letter A, vol. 349, no. 1-4, pp. 109-115, 2006.

[21] Chen, G. R., Mao, Y., & Chui, C. K. (2004). “A symmetric image encryption based on 3D chaotic map”. Chaos, Solitons & Fractals, 21(3), 749-761.

[22] Xiang, T., X. Liao, G. Tang, Y. Chen and K.W. Wong, 2006. “A novel block cryptosystem based on iterating a chaotic map”. Phys. Lett. A., 349: 109-115. DOI: 10.1016/j.physleta.2005.02.083.