International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 12 – No. 4, July 2017 – www.ijais.org

New Chaotic Substation and Permutation Method for Image Encryption

Ekhlas Abbas Albahrani, PhD
Department of Computer Science
Mustansiriyah University
Baghdad, Iraq

Tayseer Karam Alshekly
Department of Computer Science
Mustansiriyah University
Baghdad, Iraq

ABSTRACT
New Chaotic Substation and Permutation Method for Image Encryption is introduced based on combination between Block Cipher and chaotic map. The new algorithm encrypts and decrypts a block of 500 byte. Each block is firstly permuted by using the hyper-chaotic map and then the result is substituted using 1D Bernoulli map. Finally the resulted block is XORed with the key block. The proposed cipher image subjected to number of tests which are the security analysis (key space analysis and key sensitivity analysis) and statistical attack analysis (histogram, correlation, and differential attack and information entropy) and all 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.

Keywords
Image encryption, chaotic map, Block Cipher, hyper-chaotic, Bernoulli map

1. INTRODUCTION
The principle motivation behind this paper is to plan a new Substation and Permutation Method for Image encryption 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. A block cipher is an encryption and decryption system that handles a block of plaintext as a whole and is used to produce an encrypted block of equal length [1]. The original image is encrypted with the random sequence created by the logistic map, and the encrypted image is thereafter processed by the discrete fractional angular transform, which result the cipher text after double encryptions [2]. They propose a safe and strong image encryption based on the chaotic permutation multiple circular shrinking and expanding [3]. In [4] N displays an array of three main stream generators (xi, xiii and xiii), based on the permutations of three chaotic maps (logistic map, Kent map and tent map). This review performed some image encryption algorithm and finally investigated three ways to encrypt images. The first algorithm is to encrypt the original image using the Xi system. The second algorithm relies on the Xii system to randomly generate two sequences of numbers by selecting the appropriate factors along with the seed value. Then, randomly generated numbers are used to permute the image by mixing the rows, columns, and pixels sequentially in a way that uses the first sequence to mix the rows while the second sequence is used to mix the columns. The process of concealment is then achieved by means of XOR operations between adjacent rows and columns .in [5] A novel and strong chaos-based digital image encryption is proposed. This presents a cipher block image encryption using multiple chaotic maps leading increased security. An image block is ciphered by the block-based permutation process and cipher block encryption process. In [6] suggests a method that overcomes the fixed S-box weakened points and get better the performance of AES when utilized for encrypting images, especially when the image data are large. In addition, the MixColumn stage is changed by chaotic mapping and XOR operation to reduce the high computations in MixColumn transform. In [7] a novel image encryption scheme based on DNA encoding and spatiotemporal chaos is proposed. Specially, after the original image is firstly diffused with the bitwise XOR operation, the DNA mapping rule is insert to cipher the diffused image. In order to improve the encryption, the spatiotemporal chaotic system is utilized to confuse the rows and columns of the DNA ciphered image. Propose a new method in [8] for image encryption, which combines the chaos binary sequence with image fusion technology through scrambling and diffusion. These methods not only scramble the position of pixel, but also use the chaos binary sequence to encrypt the pixel one by one. In [9] a chaotic image encryption scheme which based on wavelet transform and logistic maps for shuffling image pixels is suggested. The suggested method uses three chaotic systems, including Lorenz, Chen, and Lu, which cipher the image by using parallel computing.

In this paper, a New Chaotic Substation and Permutation Method for encryption / decryption image is suggested. The proposed method consists of three transformations which implemented based on the chaotic system. The remaining part of the paper is sorted out as takes after: section 2 the basic theory of the chaotic functions, section3 and 4 the proposed algorithm. Section 5 presents the statistical analysis and security analysis of the proposed algorithm, before conclusion.

2. BASIC THEORY
In this paper we used three chaotic maps: hyper-chaotic, 1D Bernoulli map and Block cipher.

2.1 Block Cipher
A block cipher divides the plaintext into separate blocks, and encrypts each of them independently using the same key-dependent transformation to produce ciphertext block with the same size [10].

2.2 Hyper-Chaotic System
A hyper-chaotic system generated from Chen's chaotic system consists of 4D and modeled by [11]:

$$\begin{cases} x_1 = a * (x_2 - x_1) \\ x_2 = -x_1 * x_3 + d * x_1 + c * x_2 - x_4 \\ x_3 = x_1 * x_2 - b * x_3 \\ x_4 = x_1 + k \end{cases} \quad (1)$$

Where a, b, c, d and k are parameters, when a=36, b=3 , c=28, d=-16, and -0.7 ≤ k ≤ 0.7 the system is hyper-chaotic.

2.3 1D Bernoulli Map

Bernoulli map is one dimensional and is described in the following way [12]:

$$x_{n+1} = \begin{cases} r * x_n + 0.5 \; ; \; x_n < 0 \\ r * x_n - 0.5 \; ; \; x_n \geq 0 \end{cases} \quad (2)$$

Where – 0.5 < x < 0.5 and 1.2 < r < 2

In this paper, we normalized the Bernoulli map in a directed manner by exchanging the x rang (– 0.5 < x < 0.5) in equation (2) into new rang (0 < x ≤ 255) and the map becomes:

$$x_{n+1} = \begin{cases} r * x_n + 128 \; ; \; x_n < 128 \\ r * x_n - 128 \; ; \; x_n \geq 128 \end{cases} \quad (3)$$

3. KEY SCHEDULING METHOD

The core of the Chaotic Key Stream Generator (CKSG) is 3D Henoun map and 3D Cat map which we have previously designed in [13]. In proposed algorithm, the key generation algorithm consists of the following steps:-

1. Input the initial parameters (x_0, y_0, z_0, v_0) for CKSG which are floating point numbers with precision is 10^{-16}.
2. The CKSG is generating the key block that will be used for encryption and decryption algorithm.
3. The initial parameters (x_0, y_0, z_0, v_0) are changed by using simple Xor operation as shown in the following equations:

$$\begin{cases} Newx_0 = x_0 \; Xor \; v_0 \\ Newy_0 = y_0 \; Xor \; v_0 \\ Newz_0 = z_0 \; Xor \; v_0 \end{cases} \quad (4)$$

The resulted values are used as new initial parameters for CKSG in order to generate the necessary parameters for the permutation and substitution operations in the proposed encryption algorithm.

4. THE PROPOSED ALGORITHM

The proposed algorithm for image encryption consists of two major algorithms: encryption algorithm and decryption algorithm. Each algorithm has four main steps which are:-

1. Generation of key
2. Hyper-choatic Permutation operations
3. Bernoulli map Substitutions operations
4. XOR operation

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

4.1 Encryption Algorithm

Step 1. Read the original image and divided it into blocks with size of 500 byte. Each block is divided into three channels (red[],green[],blue[]) which is a one dimensional array.

Step 2. Generate the keys that needed in the encryption algorithm based on the key scheduling method discussed in section 2.

Step 3. The channel block (red, green, blue) is doing the following three transformations:

1. Hyper-chaotic Permutation operations

- Hyper-chaotic map equation (1) is iterated 50 times and the results are ignored in order to eliminate the transient effect of chaotic map.
- Hyper-chaotic map is iterated for number of times equal to the size of channel block array. In each iteration, the four floating point outputs are converting to the four integer numbers. These numbers are represented the new positions which will be used to permit the original channels block (red, green, blue) array.
- The original channels block (red, green, blue) array is permuted by using the result new positions.

2. Bernoulli map Substitutions operations

Each byte in the resulted permuted channels block (red, green, blue) array is substitute by new byte in the following way:

- Input each byte of channels block (red, green, blue) array to the 1D Bernoulli map equation (2).
- The output form 1D Bernoulli map equation is Xored with the byte position in channels block (red, green, blue) array.

3. XOR operation

Each byte in the result channel block (red, green, blue) arrays is Xored directly with each byte in key block.

4.2 Decryption algorithm:

The image decryption algorithm is reverse of image encryption algorithm where each operation is easily reversible.

- In reverse permutation operation, Hyper-chaotic map will iterate in the same way as in encryption algorithm where each position defined by Hyper-chaotic map will be used as index to return number in encrypted channels block (red, green, blue) to its original position.
- Reverse Substitutions operation is performed in the same way as in the encryption algorithm but here we use the inverse of 1D Bernoulli map.
- Reverse XOR operation is the same operation in encryption algorithm where it is performed by XORing the encrypted channels blocks (red, green, blue) to the same key block.

5. EXPERIMENT RESULT

In this paper, the proposed algorithm encrypted bitmap color image by using visual basic.net 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 144 × 116 color image Barbara, the initial value and control value for generating keys and initial value of the chaos system are x_0 =1.53892417203467111 , y_0 =-0.92754133745689034 ,

z_0=0.34895129064101731 ,v_0=-1.53892418203467111. Figure 1(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.

(a) (b)

Figure (1): (a) the original Barbara image, (b) the encrypted Barbara image

5.1 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 [14]. The proposed algorithm has a secret key with key space is 2^{213}, that is large adequate to resist brute-force attack according to the computing power of current PCs. Here , key space is constructed form the parameters that needs for generating keys (initial values x_0, y_0,z_0,v_0) These parameters are floating point numbers, where each one belongs to [-1.18, 1,85]. If the precision of each parameter is 10^{-16}, the total space of keys is 2^{213} ($(10^{16})^4$). The key space is adequately far reaching to contradict an extensive variety of brute-force attacks.

5.2 Statistical Attack Analysis

5.2.1 Histogram Analysis

In order to hide the irregular distribution from the plain image, a cryptosystem with high security level needs to produce ciphered images with a regular distribution of pixels in each color channel. To study the distribution of pixel values of image, the most often applied tools for a visual analysis is the histogram [15]. By taking images a "Barbara" and "Lena" images as original images, the histogram of the original images and corresponding cipher images are shown in Figure 2. As can be seen from Figure 2, 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.

1. Correlation coefficient analysis

Correlation coefficient is a calculation of the association (linear dependence) between two variables A and B, which give a value between +1 and −1 [16]. The correlation between two diagonally, two horizontal and two vertical. Adjacent pixels are analysis in "Baboon", "Lena" and "Penguins" cipher images. We choose 9000 pair of adjacent pixels (horizontal, vertical, and diagonal) from original image and encrypted image. The correlation can be analyzed by using the following relation: -

$$r_{x,y} = \frac{cov(x,y)}{\sqrt{D(x)} \quad \sqrt{D(y)}} \tag{6}$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}\big(x_i - E(x)\big)\big(y_i - E(y)\big) \tag{7}$$

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:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{8}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{9}$$

Table 1: Results of Correlation Analysis of the Proposed Image Cryptosystem

Direction	Penguins plain image	Penguins cipher image	Lena plain image	Lena cipher image	Baboon plain image	Baboon cipher image
Horizontal	0.9614	-0.0012	0.9681	-0.00022256	0.9080	-0.0022
Vertical	0.9606	-0.00034652	0.9822	0.00083683	0.8751	0.0036
Diagonal	0.9359	0.0020	0.9542	0.0087	0.8671	0.0033

In the results Table 1; 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.

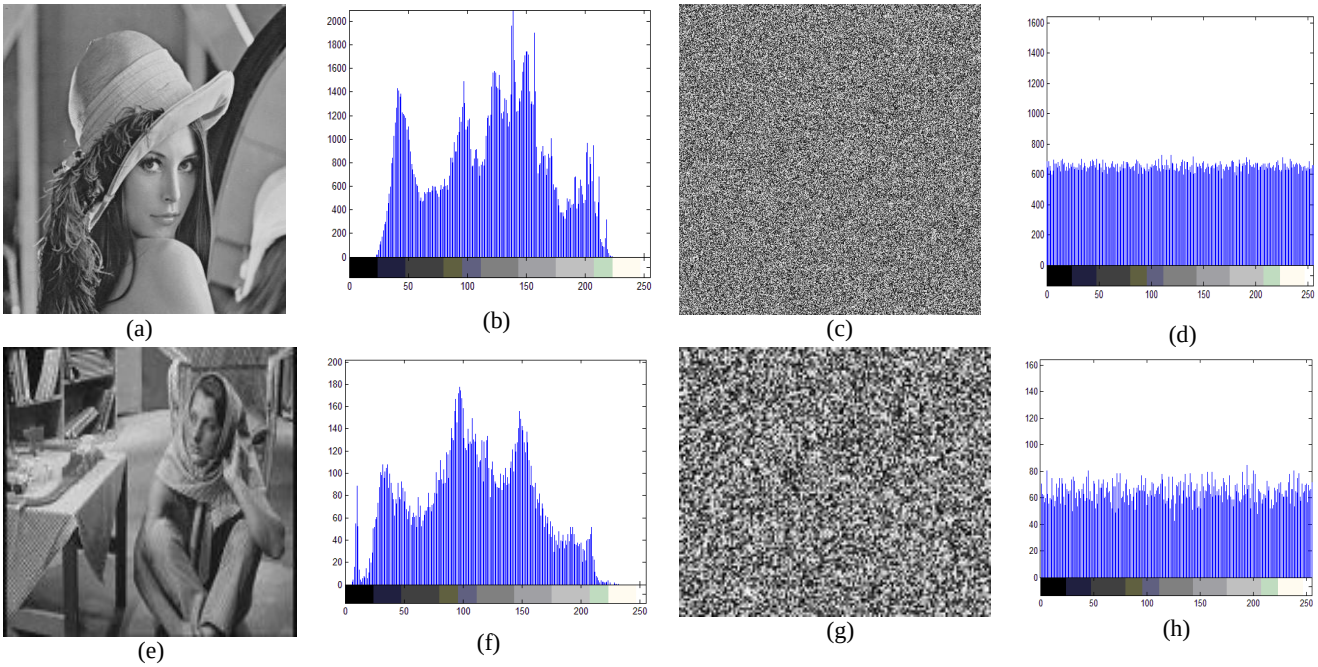

Figure (2) Histograms analysis: (a) Lena plain image. (b) histogram of (a). (c) encrypted image. (d) histogram of (c). (e) Barbara plain image. (f) histogram of (e). (h) encrypted image. (i) histogram of (h)

5.3 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) indicates the rate of the number of pixels that alteration when one pixel in the plain image is changed, The UACI(Unified Average Changing Intensity) indicates the average intensity of differences among the plain image and the encrypted image [17]. For calculation of NPCR and UACI, let us assume two encrypted images E_1 and E_2 where relating plain images have only one-pixel contrast. Label the pixels gray-scale values at matrix (i, j) of E_1 and E2 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:-

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W * H} * 100\% \qquad (10)$$

$$UACI = \frac{1}{W * H}\left[\sum_{i,j} \frac{|E_1(i,j) - E_2(i.j)|}{255}\right] * 100\% \qquad (11)$$

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 2. 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 2: Results of NPCR and UACI Tests

Image name	The point	Old point value	New point value	NPCR (%)	UACI (%)
Penguins cipher image	(5,7)	146	147	99.4578	33.45011
Penguins cipher image	(14,7)	155	156	99.4577	33.45011
Lena cipher image	(4,7)	155	156	99.49902	33.3929
Lena cipher image	(4,5)	152	151	99.49899	33.3929

Baboon cipher image	(11,4)	71	72	99.5508	33.4322
Baboon cipher image	(15,7)	111	110	99.5508	33.4322

5.4 Information Entropy Analysis

In information theory, entropy is a measurement of the uncertainty in a random variable. In this context, the term commonly indicates to the Shannon entropy that quantifies the predictable value of the information contained in a message. Entropy is typically measured inbits, nats, or bans [18]. The information entropy H(m) of a plaintext message m can be calculated as :

$$H(m) = \sum_{i=1}^{2^{n-1}} p(m_i) \log 2 \frac{1}{p(m_i)} \qquad (12)$$

Where p(mi) represents the probability mass function of message mi 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, Penguins and Baboon) are showed in table 3. 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 3: Results of entropy analysis of the proposed image cryptosystem

Image name	Entropy value
Lena cipher image	7.9988
Penguins cipher image	7.9988
Baboon cipher image	7.9946

6. 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 image of different size based on permutation and substitution. Chaotic Key Stream Generator based on 3D Henoun map and 3D Cat map was proposed to generate the 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.

7. REFERENCES

[1] W.STALLINGS," CRYPTOGRAPHY AND NETWORK SECURITY", Prentice Hall, 2011.

[2] J.YU, YUAN LI, X. XIE, N. ZHOU, Z.ZHOU," Image encryption algorithm by using the logistic map and discrete fractional angular transform", Optica Applicata, Vol. XLVII, No. 1, 2017.

[3] Y.Suryanto, Suryadi, K.Ramli," A Secure and Robust Image Encryption Based on Chaotic Permutation Multiple Circular Shrinking and Expanding", Journal of Information Hiding and Multimedia Signal Processing, Volume 7, Number 4, July 2016.

[4] N.S.Ahmed," Multi-Image Encryption Technique Based on Permutation of Chaotic System", International Journal of Video&Image Processing and Network Security IJVIPNS-IJENS Vol:16 No:01,2016.

[5] A.A.Avval, J.ayubi and F.Arab," Digital Image Encryption Based On Multiple Chaotic Maps", ACSIJ Advances in Computer Science: an International Journal, Vol. 5, Issue 1, No.19 , January 2016.

[6] A.ABDULGADER,M.ISMAIL, N.ZAINAL,TARIK IDBEAA," ENHANCEMENT OF AES ALGORITHM BASED ON CHAOTIC MAPS AND SHIFT OPERATION FOR IMAGE ENCRYPTION", Journal of Theoretical and Applied Information Technology, Vol.71 No.1, 10th January 2015.

[7] C.Song and Y.Qiao," A Novel Image Encryption Algorithm Based on DNA Encoding and Spatiotemporal Chaos", Entropy 2015.

[8] R. Qiu, C. Zhu and S.Liu," An chaos image encryption algorithm based on binary sequence and baker mapping", International Industrial Informatics and Computer Engineering Conference,2015

[9] S.Zalipour, S.J.Mirabedini, A.Harounabadi," A Novel Image Encryption Algorithm Based On Wavelet Transform and Hyper-Chaotic System", International

Journal of Review in Life Sciences, ISSN 2231-2935, 2015.

[10] C. D.CANNIÈRE, A.BIRYUKOV, AND B.PRENEEL," An Introduction to Block Cipher Cryptanalysis", IEEE, VOL. 94, NO. 2, FEBRUARY 2006

[11] T.Gao , Z. Chen ," A new image encryption algorithm based on hyper-chaos", Elsevier, 2008

[12] Sheela S.and S. V. Sathyanarayana "Application of chaos theory in data security-a survey", ACCENTS Transactions on Information Security,Vol 2(5), 2017.

[13] Dr. E.A. Albhrany, T.K. Alshekly" A New Key Stream Generator Based on 3D Henon map and 3D Cat map", International Journal of Scientific & Engineering Research, Volume 8, Issue 1, January-2017

[14] W.Liu , K.Sun, C.Zhu "A fast image encryption algorithm based on chaotic map", ElsevierLtd,2016

[15] A.C. Dascalescu, R. Boriga, and M.I.Mihailescu," A novel chaos-based image encryption scheme", Annals of the University of Craiova, Mathematics and Computer Science Series Volume 41(1), 2014.

[16] Geeta, A. Papola," AN ALGORITHM TO SECURE AN IMAGE USING LOGISTIC CHAOTIC MAPPING WITH SHUFFLING", INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING & TECHNOLOGY (IJCET), Volume 5, Issue 9, September (2014).

[17] W.Yao, F.Wu, X. Zhang, Z.Zheng, Z.Wang,W.Wang, W.Qiu," A Fast Color Image Encryption Algorithm Using 4-Pixel Feistel Structure", PLOS ONE, November 8, 2016.

[18] P. TiwariȦ, M. KumarȦ, A. K. Jaiswal, and R. Saxena," Chaos Based Information Securty in Multimedia Communication", International Journal of Current Engineering and Technology, 2014.