Images Encryption Using Chaos and Random Generation

Dr. Yossra Hussain Ail
Computer Sciences Department ,University of Technology/ Baghdad.
Email: yossra_1@yahoo.com
Zahraa A.H. Alobaidy
Computer Sciences Department ,University of Technology/ Baghdad.
Email: zahraaalobaidy@gmail.com

Received on:12/9/2015 & Accepted on:20/1/2016

ABSTRACT

Due to the network and multimedia application development information security become important since information can be attacked over the transmission channels and the combination of cryptography and chaotic become important filed of information security, where many encryption algorithm are based on chaotic mapping due to the inherent features of image like high redundancy and bulk data capacity. In this paper, three chaotic maps are used to achieve good diffused image by setting the initial conditions to generate the shuffling sequence randomly by 2D zaslevskii map and employ them in 2D cat map for shuffling the image pixels positions, also baker map is used to decomposed image into four rectangles and shuffle them. To increase the security level of the encryption algorithm Geffe random key generator is used to generate 128 bit key and employ it with exclusive-OR equation to the diffused image. The results indicated that the combination of chaotic and cryptography proved to be good for high security level. All the experimental results show that the proposed algorithm is secure due to the large key space and the high sensitivity to the secret key.

Keywords: Image encryption, chaotic system, cat map, random generation

تشفير الصور بأستخدام نظرية الفوضى و التوليد العشوائي

الخلاصة

نظرآ للتطور الحاصل في الشبكات وتطبيقات الوسائط المتعددة والهجوم الذي تتعرض له البيانات عبره قنوات النقل أصبحت أمنية المعلومات مهمة. الجمع بين علم التشفير ونظرية الفوضى مجال مهم في امنية المعلومات. ان الكثير من خوازميات تشفير الصور تعتمد على خرائط الفوضى بسبب الميزات الكامنة في الصور كالتكرار وسعة البيانات الكبيرة. في هذا البحث تم استخدام ثلاث خرائط فوضى للحصول على صوره مشفره بشكل جيد وتم ذلك من خلال وضع القيم الاولية لتوليد سلسلة من القيم العشوائية باستخدام خريطة Zaslevskii وتوظيف هذه القيم العشوائيه في خريطة Cat لبعثرت مواقع البكسل في الصوره، كذلك استخدمة خريطة Baker لتقطيع الصوره الي اربع مستطيلات و بعثرت كل منها. لزيادة مستوى الامنيه في هذه الخوارزمية تم استخدام المولد Geffe لتوليد مفتاح عشوائيا بطول ١٢٨بت وتوظيفه في معادلة exclusive-OR مع الصوره المبعثره. ان الجمع بين علم التشفير ونظرية الفوضي اعطى مستوى عالي من الامنيه وقد اظهرت النتائج ان الخوارزمية المقترحة أمنة نظرا لحجم المفتاح ودرجة الحساسيه العاليه للوصول الى المفتاح.

INTRODUCTION

Image encryption schemes have been progressively more studied to protect images from illegal access providing secure image transmission over communication channels. Traditional encryption schemes such as RSA, AES and DES are not suitable for image

https://doi.org/10.30684/etj.34.1B.19
2412-0758/University of Technology-Iraq, Baghdad, Iraq

encryption because they have weakness of lower level efficiency when the image is large and the images inherent features like bulk data capacity and elevated data redundancy [1, 2].

Due to the important properties of chaos signals they are conceded good for image encryption and increases the robustness of cryptosystem against statistical attacks. These properties includes pseudo-random, non-periodicity and high sensitive to system parameters and initial conditions, etc. Therefore, combining cryptography with chaotic theory is concedered one of the important fields in information security [3, 4].

The chaos based encryption algorithm lead to new efficient ways to develop images security schemes to satisfy the demand secure image transmission over the communication channel. Therefore, many encryption algorithms are based on chaotic maps like a standard map, Logistic map, Zaslavskii map, Cat map, Baker map, Henon map, Chen map, etc. So, as to get better security performance of image encryption algorithm, the concept of diffusion is used to change the pixels position of plain image and confusion is used to change the gray level value of diffused image [3, 5].

In recent years, many researches studied the image security system using chaos and random generators, such as: Lv et al. [6], designed a scheme that employ henon and cat maps to encrypte the original image by confusing and diffusing the image pixels positions and values. Banthia et al. [7], used random number generator to generat key for shuffling and logistic map to generat index for shuffling then combined the two methods. Mishra et al. [4], presnt an algorithm based on combination of pixel shuffling and three chaos map for encryption.

In this paper, three chaotic maps are used to achieve good diffused image and random key generator is used for confusion to increase the security level of the proposed encryption algorithm.

CHAOTIC MAPPING

The chaos maps used in the proposed scheme are summarized as the following:

a) Zaslavskii Map

The 2D Zaslavskii map is a discrete-time dynamical system, and is defined as [8]:

$$\mathrm{X}_{n+1} = (\mathrm{X}_n + \nu \left(1 + \mu \mathrm{Y}_n\right) + \varepsilon\nu\ \mu \cos\ (2\pi\ \mathrm{X}_n)) \bmod 1 \qquad (1),$$

$$Y_{n+1} = e^{-\tau}\ (Y_n + \varepsilon \cos\ (2\pi\ X_n)) \qquad (2),$$

And $\mu = \dfrac{1-e^{-\tau}}{\tau}$,

where X_n, Y_n are current chaotic values and X_{n+1}, Y_{n+1} are the next produced chaotic values and ε, ν, τ are control parameters and e stand for exponentiation. The Zaslavskii map key set is $\{X_0, Y_0, \varepsilon, \nu, \tau\}$. The system is chaotic when the initial values are X0= 0.01, Y0= 0.01, ν=12.6695, ε=0.3, τ=3.0 and X, Y sequence generated by iterating the Equations (1), (2) *n* times where *n* is the image size.

The statistical properties of the generated sequence of Zaslavskii map can be improved by the preprocessing equations defined as[9]:

$$x_n = (abs(x_n) - (Floor(abs(x_n))10^{14}) \bmod 256 \qquad (3),$$

$$y_n = (abs(y_n) - (Floor(abs(y_n))10^{14}) \bmod 256 \qquad (4),$$

where Floor(x,y) returns the value of x to the nearest integer, mod(x,y) returns the reminder of the division and abs(x_n, y_n) returns the absolute value of x,y. The preprocessed sequence lead to a batter balance distribution and better correlation properties also they can be used in the encryption process.

b) Baker Map

The baker's map from the unit square into itself. The name baker’s map comes because it is similar to baking process, and it is defined as [3]:

X = [0, 1)^2 = [0, 1) × [0, 1) is the unit square.

$$F(x,y)=2x,\frac{y}{2} \qquad \text{If } 0\le x<\frac{1}{2} \qquad (5),$$

$$F(x,y)=2x-1,\frac{y+1}{y} \qquad \text{If } \frac{1}{2}\le x<1 \qquad (6),$$

where, F is found by cutting [0, 1)^2 into two vertical rectangles R0 = [0, 1/2) × [0, 1) and R1 = [1/2, 1)×[0, 1), these rectangles are stretched and compressed to produce an interval of horizontal width 1 and vertical height 1/2 and then place them on top of each other.

c) Cat Map

The cat map is a 2-D invertible chaotic map, it uses two parameters and can be defined as [10]:

$$x' = (x + ay)\bmod n \qquad (7),$$

$$y' = (bx + (ab+1)y)\bmod n \qquad (8),$$

where, a, b are positive integers stand for the control parameters, x,y is the old pixel position and x’,y’ is the new pixel position. The cat map is applied to the original image and pixel positions are shuffled, after several iterations the image will be meaningless and distorted and the correlation among adjacent pixels is completely disturbed. But, after iterating many times the original image will be returned due to cat map periodicity [2, 11]. To deal with this problem a, b parameters are generated randomly by using a 2-D Zaslavskii map.

Random Generator

Several computational methods for random number generation are carefully designed to generate a sequence of numbers or symbols. In this proposal Geffe random generator is used to generate keys for confusion.

Geffe generator uses three LFSRs mutual in a nonlinear manner [12]. Two of the LFSRs are input into a multiplexer, and the third LFSR controls the output of the multiplexer. If LFSR1, LFSR2 and LFSR3 are the outputs of the three LFSRs, then the output of the Geffe Generator (result) is found using the nonlinear function given by the equation:

$$result = (LFSR1 \wedge LFSR2) \oplus ((\overline{LFSR1}) \wedge LFSR3) \qquad (9)$$

From the '*result*' of this equation any number of bits can be taken to form the random sequence. The procedure can be repeated to produce more random numbers so that the length of the random sequence produced can be increased as desired, see Figure 1., [12].

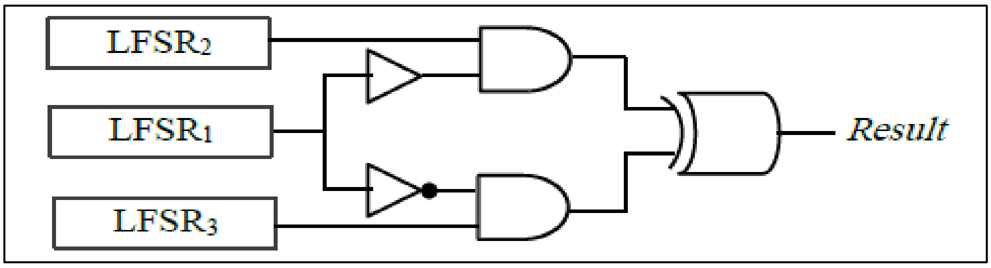

Figure 1: Geffe Generator

The Proposed Algorithm

The high correlation among image adjacent pixels is considered as a weak point in image security, to overcome this weakness the correlation need to be disturb completely. An image diffusion and confusion scheme is proposed to accomplish this. The diffusion and confusion are the two main steps of the proposed image encryption algorithm. First in diffusion scheme 2D cat map and baker map are used to shuffle the image pixel position then to increase the security level, confusion scheme is used to change the pixel value of the diffused image by using randomly generated key and exclusive-OR equation.

In this proposed algorithm, control parameters and key are generated randomly first by generating x, y sequence by 2D zaslavskii map, then preprocessed them to obtain a, b sequence. First, the map of the Equations (1), (2) are iterates 1000 times with initial conditions as: X0= 0.01, Y0= 0.01, ν=12.6695, ε=0.3, τ=3.0, these 1000 values of *x, y* are discarded to overcome the cat map periodicity weakness. The map iterated again *n* times to produce x_i and $y_{i,}$ where *n* is the image size i= 1, 2 … *n*. then $x_{i,}$ y_i are preprocessed by Equations (3), (4) to produce $a_{i,}$ b_i control parameter. Second, the key is generated by Geffe generater, this is done by taking two random 8X8 matrices and multiply them to prudence one matrix then select the first three rows from the matrix where each row will be convert to binary and used as the input for the linear feedback register (LFSR). Then, after creating the LFSRs for Geffe generator as initial seeds to generate the key by Equation (9).

The encryption algorithms are sensitive to keys and control parameters $a_{i,}$ b_i and key are made sensitive, so the diffusion and confusion schemes become sensitive to the minor change in keys and the attacker cannot obtain the original image without the secret key. The following steps illustrate image encryption scheme:

Step 1. Let the plain image I_0 (x, y) of size NxN the input to be diffused, where x, y=1, 2, 3… N.

Step 2. Decompose the entire image I (x, y) into 8x8 size blocks, B1, B2 …. $B_{nob.}$

Step 3. Apply cat map Equations (7), (8) within each block B*i* by the use of control parameters $a_{i,}$ b_i to shuffle the pixels within each block and this step is done *n* time to obtain partially diffused image I_1 (x, y).

Step 4. Apply baker map within whole diffused image I_1(x, y) to produce four stretched and compressed rectangles R_0 R_1 R_2 $R_{4.}$

Step 5. Apply cat map Equations (7), (8) within each rectangle twice using the control parameters $a_{j,}$ b_j to obtain a partially diffused image I_2(x, y), where j= 1, 2 … r, and r is the rectangle size.

Step 6. Apply cat map Equations (7), (8) within complete image I_2(x, y) by the use of control parameters *ai, bi* to shuffle pixels, this step is done *n* time to obtain a final diffused image I_3(x, y).

Step 7. Convert the diffused image I_3(x, y) into binary $Db_{(x,\ y)}$, where x, y= 1, 2 … N and generate the binary key Kb_i using Geffe generator, where *i= 128 bit* is the key size. The diffused image is encrypted by:

$$Eb_{(x,\ y)} = Db_{(x,\ y)} \oplus Kb_i \qquad (10),$$

where E*b*(x, y) is the binary equivalent of a confused image within the pixel coordination (x, y) and the sign $\oplus$ symbolizes the exclusives-OR operation.The binary encrypted image E*b*(x, y) is converted to decimal to obtain the confused image I_4(x, y). Figure (2) shows the block diagram of the proposed scheme. To reconstruct the original image apply the algorithm steps in reverse order.

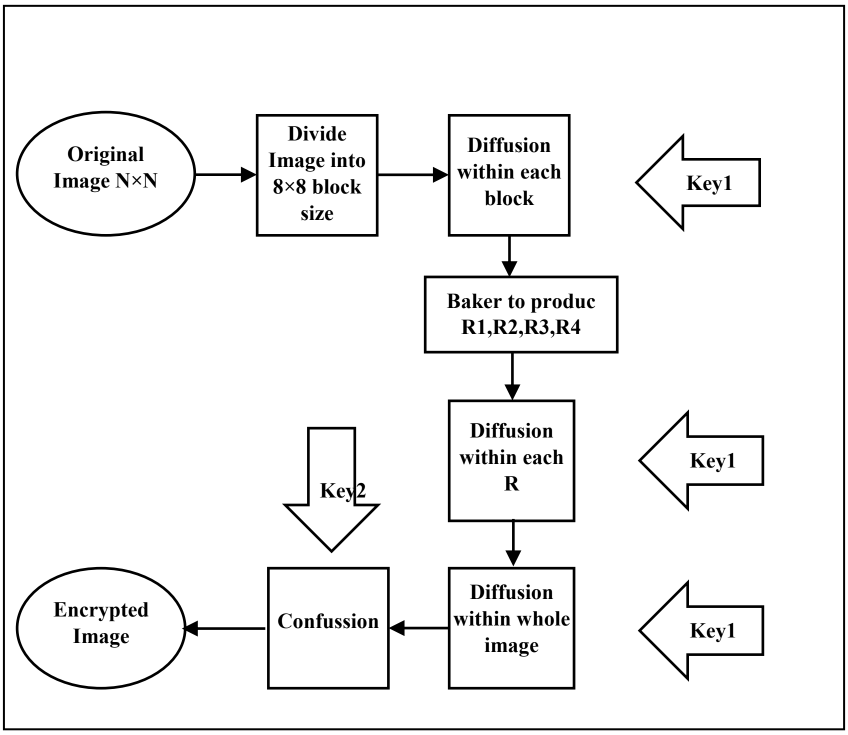
Original Image N×N
Divide Image into 8×8 block size
Diffusion within each block
Key1
Baker to produc R1,R2,R3,R4
Key2
Diffusion within each R
Key1
Encrypted Image
Confussion
Diffusion within whole image
Key1

Figure 2: The general proposed scheme

As shown in figure (2), the encoding process of proposed scheme consists of main steps listed in algorithm:

Algorithm: Encoding Process Scheme	
Input	*I(x,y)* // array original RGB color image *Key1* // Generated by Zaslavskii map *Key2* // Generated by Geffe generator
Output	*Encrypted Image*

Step1*:* Read the original RGB color *I(x,y).*
Step2: Decompose the entire image I (x, y) into 8x8 size blocks B_i.
Step3: Input the system parameter *Key1* and *Key2*, values.
Step4: Difuse each block B_i by cat map using key1.
Step5: Apply baker map to produce $R_0 R_1$ R_2 R_4.
Step6: Difuse R_0 R_1 R_2 R_4 by cat map using key1.
Step7: Difuse whole image by cat map using key1.
Step8: Confuse the difused image by Equation (10) using key2.

Experimental Results

This proposed algorithm is implemented using the C# simulation program, and color image "Lena" of size 400x400 was taken as a test image. The initial parameters of the proposed algorithm are {X_0= 0.01, Y_0= 0.01, ν=12.6695, ε=0.3, τ =3.0}, where X_0, Y_0 are intial chaotic values and ν, ε, τ are control parameters.

Histogram Analysis

The statistical features of images are presented using histogram that plots the occurrences frequency of image pixel value, this analysis is done to compare original and encrypted images where there should be no similarities between original image and encrypted image histograms.The Figure (3) shows the original image with its histogram, Figure (4) shows the proposed diffusion scheme for *n*=2 with its histogram and Figure (5) shows result of proposed confusion schemes with its histogram.

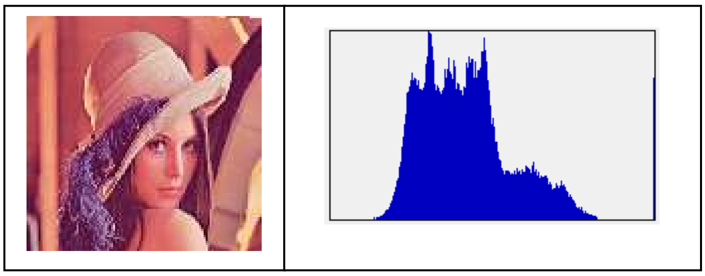

Figure 3: Original image and its histogram

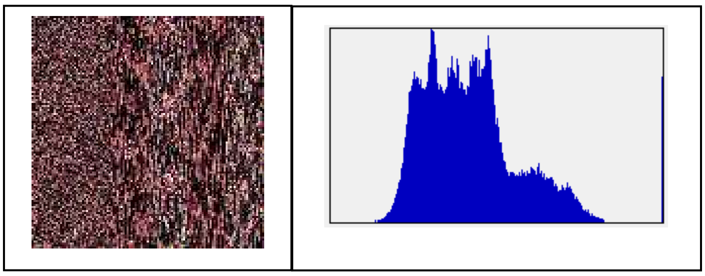

Figure 4: Diffused image and its histogram

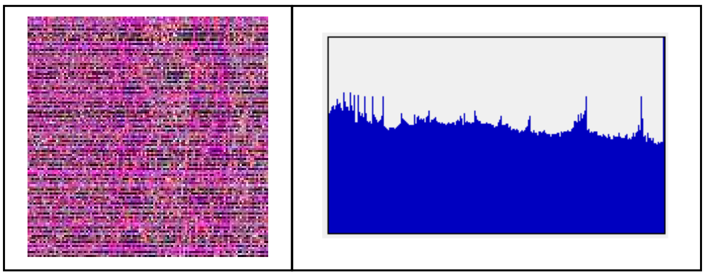

Figure 5: Confused image and its histogram

The diffusion and confusion results show how the image is completely distorted and uncorrelated adjacent pixels, and the histogram of encrypted image is almost uniform and different from original image histogram. The encrypted image has good balanced features due to the distribution of pixel value in the image and as a result the attackor cannot extract any information.

a) Correlation Coefficient Analysis

The correlation coefficient between adjacent pixels of an encrypted image can be calculated using the following equation [13]:

$$Correlatio\,nCoefficient = \frac{COV(x,y)}{\sigma_x \sigma_y} \qquad (11),$$

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

$$E(x)=\frac{1}{L}\sum_{i=1}^{L}x_i\,,\quad \sigma_x=\frac{1}{L}\sum_{i=1}^{L}(x_i-E(x))^2$$

where x, y are the gray level value of two adjacent pixels in an encrypted image and L is the number of pixels involved in calculation. The adjacent pixels either selecte horizontally, vertically, or diagonally.The closer correlation coefficient value to zero is, the better quality of encryption algorithm.

Table 1: Correlation Coefficent of Two Adjacent Pixels in Encrypted Images

	Original Image	Deffused Image	Confused Image
Horizontal	1	0.010817	0.00099431
Vertical	1	0.02946	0.034251
Diagonal	1	0.026391	0.0089969

Accourding to Table 1. The value of correlation coefficients of the original image are equal to 1, indicating that high correlation exists among adjacent pixels, while the correlation coefficients of diffused and confused images are close to 0, i.e., there is a highly uncorrelated adjacent pixels in the encrypted image.

b) Analysis of Key Space

The key space indicate the entire number of keys that are possible to use in an encryption algorithm. In order to resist any attack this key should be as large as possible. The encryption algorithm should be sensitive to all secret keys. In diffusion scheme, the initial five parameters of Zaslavskii map are {x_0, y_0, v,ε,τ } for each 8 bits so the total binary key size is 40 bits. In confusion scheme key of 128 bits is used where the key was randomly generated by Geffe genretor and LFSR using two randomly selected matrices as input. In such case the key space is 2^{168} and it is large enough to fight the attack.

c) Analysis of Key Sensitivity

A high-quality encryption algorithm should be sensitive to a small change in secret keys, where such change leads to completely different decrypted image. To evaluate the key sensitivity property of the proposed algorithm, the same key is used in decryption except that the value of x_0 is changed to 0.65 and the decrypted image, as shown in Figure 6.

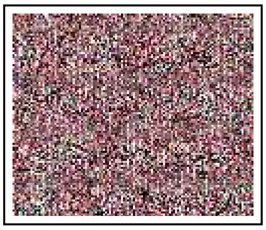

Figure 6: Decrypted image with wrong key

CONCLUSION

An efficient image encryption and decryption algorithm based on combination of chaos and cryptography along with random generator is proposed in this paper. This combination proved to be good for high security level. All the experimental results show that the proposed algorithm is secure due to the large key space and the high sensitivity to the secret key. The algorithm demonstrated in this paper can be widely used in any information security areas.

REFERENCES

[1] K. Sakthidasn Shankaran, and B.V. Santhosh Krishna, "A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images", International Journal of Information and Education Technology Vol. 1, No.2, 137-140, 2011.

[2] Z. LV, L. Zhang, and J. Guo "A Symmetric Image Encryption Scheme Based on Composite Chaotic Dispersed Dynamics System", Proceedings of the Second Symposium International Computer Science and Computational Technology (ISCSCT '09) Huangshan, P. R. China, 191-194, 2009.

[3] A. Anto Steffi, and D. Sharma "Modified Algorithm of Encryption and Decryption of Image using Chaotic Mapping", International Journal of Science and Research (IJSR), Vol. 2, No 2, 77-80, 2013.

[4] M. Mishra, P. Singh, and C. Garg "A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping", International Journal of Information and Computation technology, Vol. 4, No. 7, 741-746, 2014.

[5] C. Dongming, Z. zhiliang, and Y. Guangming "An Improved Image Encryption Algorithm Based on Chaos" in Proceedings of IEEE International Conference for Young Computer Scientists, 2792-2796, 2008.

[6] Z. Lv, L. Zhang, and J. Guo "A Symmetric Image Encryption Scheme Based on Composite Chaotic Dispersed Dynamics System", Proceedings of the Second Symposium International Computer Science and Computational Technology (ISCSCT '09) Huangshan, P. R. China, 191-194, 2009.

[7] A. Kr. Banthia, N. Tiwari, "Image Encryption Using Pseudo Rnadom Number Generators", International Journal of Computer Application, Vol. 67, No. 20, 2013.

[8] G. Hanchinamani and L.Kulakarni "Image Encryption Based on 2-D Zaslavskii Chaotic Map and Pseudo Hadmard Transform", International Journal of Hybrid Information Technology Vol.7, No.4, 185-200, 2014

[9] A. Karim, S. Mahmoud "Image Encryption Based on Hyperchaotic Liu System Algorithm", Eng. &Tech.Journal,Vol.33, No.2, 204-212, 2015.

[10] S. Keshari, and S. G. Modani, "Image Encryption Algorithm based on Chaotic Map Lattice and Arnold cat map for Secure Transmission", International Jornal Of Computer Science And Technology, Vol. 2, No. 1, 132-135, 2011.

[11] ZH. Guan, F. Huang, and W. Guan, "Chaotic Based Image Encryption Algorithm", Physics Letters A, Vol. 346, No. 4-5, 153-157, 2005.

[12] K. Zeng, C-H. Wang, D-Y. Wei, and T.R.N. Rao "Pseudorandom Bit Generators in Stream-Cipher Cryptography", IEEE computer magazine, Vol.24, No. 2, 8-17, 2002.

[13] A.T. Hashim, and B. H. Helal, "Measurement of Encryption Quality of Bitmap Images with RC6, and two modified version Block Cipher", Eng.& Tech. Journal ,Vol. 28, No.17, 2010.