International Journal of Security and Its Applications
Vol.9, No.11 (2015), pp.281-292
http://dx.doi.org/10.14257/ijsia.2015.9.11.26

A Novel Image Encryption Method Based On Couple Mapped Lattice and Two-Stage Diffusion

Yunsheng Zhong[1] and Xu Xu[2]

[1,2]Department of Computer Science,
Sichuan University Of Arts And Science, Sichuan, china.
Ashunjz@sohu.com

Abstract

In this paper, a novel image encryption method which is based on the coupled map lattice (CML) and two-stage diffusion is proposed. The author employs the two-stage diffusion to process images. The plain image is expanded into two composed of selected four bit-planes and diffuse them at bit-level as first stage diffusion, then reconstruct them as the input of block diffusion, which is served as second stage diffusion. The chaotic coupled map lattice employed in this method generates pseudo-random sequences in block diffusion phase. The experiment results and analysis have proved the novel image encryption method is practical and effective for encryption applications.

Keywords*: Image encryption; Two-stage diffusion; CML*

1. Introduction

C Avoidance of information loss and interception has boosted the development of encryption fields. The real information supposed to covered and keep it secure by re-arranging data in different ways. For image encryption, including spatial domain image encryption and frequency domain image encryption, there are some factors should be considered just like the intrinsic features of images—huge amount of information, high redundancy, strong correlation between pixels. Traditional encryption strategies such as the Data Encryption Standard (DES), International Data Encryption Algorithm (IDES), and RSA perform badly. Currently, the using of chaos has become more popular because of its essential characters such as periodicity and sensitivity to initial conditions [1].

Most methods have been proposed on the chaotic image encryption [2-9], but many have proved the weak security for some chaotic encryption schemes [10-13]. Most common problems among unsecured encryption schemes are the chaotic dynamics degradation. While CML-based spatiotemporal chaotic system performs well on account of its high efficiency on numerical simulation and parallel iteration, it has been employed widely in chaotic encryption field recently [14-16]. Besides this, the CML has more initial values and it is bound to have large secret keys space, so it is very suitable for image encryption. So in this paper, the author proposes a CML-based chaotic encryption method.

Fridrich designed the typical architecture for image encryption which is composed of two stages, *i.e.*, permutation and diffusion [17]. Most pixels are relocated through the first step, the value of pixels are modified by the diffusion step. They have stated their image encryption schemes [18-19], in which pixel is the basic processing element. In fact, the internal information of pixel hardly varies during the whole procedure. Since each pixel bits contains different percentage of information, to ensure the alteration of percentage between bit-planes is the key

Point for current schemes. Zhang proposed an image encryption scheme at [20], in which consider it is be feasible and effective when processing the image at bit-level. In

ISSN: 1738-9976 IJSIA

our proposed method, the pixel-level processing is compound with bit-level processing to improve performance.

Up to now, plenty of image encryption methods adopted traditional diffusion step, which perform logical XOR operation with the former cipher and chaotic sequence, and obtain the cipher values of pixel. This process spread the randomness toward whole image. Besides this, the block diffusion are widely used in that the parallel computation is of popularity, moreover, multitude of variable control parameters are able to introduced to enhance the link between plain image and the key sensitivity. Differently with other block diffusions, an intermediate block is constructed to make diffusion based on input block and CML block. In our proposed method, the bit-level diffusion is employed before the block diffusion, *i.e.*, Two-Stage diffusion.

This paper is organized as follows. In section 2, the structure of CML and the definition of two-stage diffusion are introduced. In section 3, the encryption scheme is described in detail. In section 4, the simulation and results is given for our proposed method. Finally, we make a conclusion in section 5.

2. The Preliminary Work

2.1. The Coupled Map Lattice

The coupled map lattice is a classical spatiotemporal chaos system. Rather than other dynamic systems, CML has continuous states on the basis of discrete time and discrete space. Besides this, it has conserved the features about local maps. All these characters make us prefer it in encryption schemes.

The two-way coupled map lattice system is defined as follows:

$$x_{n+1}(j+1)=(1-\varepsilon)f(x_n(j))+\frac{\varepsilon}{2}\left[f(x_n(j-1))+f(x_n(j+1))\right],\ (j=1,2,\ldots,16) \tag{1}$$

where j is the lattice site index, n is the time index, $\varepsilon\in(0,1)$ is a coupling constant, which can be set as a secret key, $x_n(j)$ refers to the state variable for the j th site at time n , and L is the lattice length. The period boundary condition is $x_n(0)=x_n(L)$.

$$f(x_n)=ux_n(1-x_n) \tag{2}$$

where $f(x)$ is a logistic map, and $0<f(x)\leq 1$, μ is the logistic map coefficient. The sequence generated behaves chaotic when $3.57\leq\mu\leq 4$ In proposed method, we set $u=4$ and $L=16$.

2.2. Two-Stage Diffusion

2.2.1. Bit-Level Diffusion Phase : Bit-level diffusion is introduced as first stage diffusion. Considering the enhancement of relation between cipher image and original image, the mean pixel values about the above two bit-level permutated image respectively are calculated as initial values of chaotic logistic map, which is employed to generalize chaotic sequence for bit-level diffusion, the calculation formulation of initial values $x_1^{'}$ and $x_2{'}$ is defined as follows:

$$x^{,}1=\frac{\sum_{i=1}^{m\times n}p1(i)}{15\times m\times n}\qquad x^{'}{}_2=\frac{\sum_{i=1}^{m\times n}p_2(i)}{15\times m\times n} \tag{3}$$

where $p_1(i)$ ($i = 1,2,\cdots,16$) is the pixel value in first bit-level permutated image. Similarly, we may obtain the second mean value $x_2^{'}$ from above formula. They can be treated as one part of secret keys.

2.2.2. Image Block Diffusion Phase : Image block diffusion has been proposed because of the popularity of parallel computing and more secure communication on noisy channels. After Bit-level diffusion, make block partition is made for further operation. In this method, an intermediate block should be acquired on the basis of the permutated block and chaotic sequence, which is generalized by the couple, mapped lattice (CML), then perform logical XOR operations orderly within current intermediate block. Noteworthily, we will give a special value for the first pixel's logical XOR operation in different blocks.

(1) The construct of intermediate block

Construct an intermediate block as the input for small-block diffusion; because this step will make diffusion more random .This construction for the intermediate block is based on permutated image and CML sequence.

Step 1 Iterate the CML once, obtain a CML sequence of whose length is 16, then the value of sequence is modified by following formula (4):

$$d\ \ (j) = \left\lfloor d(j) \times 10^{12} \right\rfloor \bmod 256,\ j = 1,2,\cdots,16 \qquad (4)$$

Step 2 Assume a permutated block as B, the chosen CML sequence d is reshaped into a matrix D of sized, then get the two matrices as below:

$$\begin{pmatrix} B(1) & B(5) & B(9) & B(13) \\ B(2) & B(6) & B(10) & B(14) \\ B(3) & B(7) & B(11) & B(15) \\ B(4) & B(8) & B(12) & B(16) \end{pmatrix} \begin{pmatrix} d(1) & d(5) & d(9) & d(13) \\ d(2) & d(6) & d(10) & d(14) \\ d(3) & d(7) & d(11) & d(15) \\ d(4) & d(8) & d(12) & d(16) \end{pmatrix}$$

Step 3 Based on two matrices; a substitution table T is obtained which determine the values of intermediate block. Firstly, we select a pixel in permutated block , then other four pixels will be located in CML block , whose positions are able to mapped its corresponding center, adjacent (right and down)and diagonal(lower right)pixels. If the value in right (or down, lower -right) corner does not exist within CML block, other values should be selected in left (or top, upper left) corner to replace. Based on these pixels, the values are calculated by following rules to fill in the substitution table T. Just take the pixel for example, the pixel is selected from CML block, and then we will finish the first column in substitution Table T.

$$\begin{cases} T(1,j) = ((d_{right} \oplus d_{down} \oplus d_{lower-right}) + B(j))\ )\bmod 2^8 \\ T(2,j) = ((d_{right} \oplus d_{down} \oplus d_{center}) + B(j))\ )\bmod 2^8 \\ T(3,j) = ((d_{right} \oplus d_{low-right} \oplus d_{center}) + B(j))\ )\bmod 2^8 \\ T(4,j) = (d_{center} \oplus B(j))\ )\bmod 2^8 \end{cases},\quad j = 1,2......16$$

where $T(l,i)(l=1,2,3,4)$ means the optional values for every pixel $B'(j)$ $(j=1,2,......16)$ within the intermediate block .

Step 4 Use another logistic map to get a sequence M , modify its value range within [1, 4] by formula (6). Especially, we get the initial value x0 for logistic map by Formula (5).

$$x_0=\frac{\sum_{j=1}^{16}B(j)}{16\times 255}, \tag{5}$$

$$M^{'}(i)=(\lfloor (M(i)\times 10^{12}\rfloor \bmod 4)+1, i=1,2,\cdots,16 . \tag{6}$$

Step 5 The new sequence with the integer range within [1, 4] is used to select which value should be chosen from table T, then become the new value in intermediate block, finally get all values for the intermediate block.

(2) Small block diffusion

The XOR operations are defined as below formula (7-8):

$$C_i(1)=p\oplus d\ (1)\oplus B_i^{'}(1), \tag{7}$$

$$C_i(j)=C_i(j-1)\oplus d(j)\oplus B_i^{'}(j), j=2,3,\cdots,16 \tag{8}$$

where $i=1,2,\cdots,sum$ is the number index of processing block; $B_i^{'}(j)$ ($j=2,3,\cdots,16$) is the value of pixel within an intermediate block ; $d(j)$ is the corresponding value of CML sequence used for diffusion; $C_i(j)$ is the final cipher block ; p is given specific values according to the different blocks. Other related details are presented in next part.

3. The Process of Encryption

The process of our proposed method will be summarized in following steps and corresponding secret keys and parameters are given.

Step 1. A decimal sequence K with 128 bits is employed to be the secret keys. Dividing them into 18 groups, then we obtain a series of values by Formula (9).

$$K=k_1k_2k_3k_4k_5k_6k_7k_8k_9k_{10}k_{11}k_{12}k_{13}k_{14}k_{15}k_{16}\cdots k_{120}k_{121}k_{122}k_{123}k_{124}k_{125}k_{126}k_{127}k_{128}$$
$$x_i=0.k_{(i-1)\times 8+1}k_{(i-1)\times 8+2}\cdots k_{(i-1)\times 8+7}k_{i\times 8}, (\mathrm{i}=1,2,\cdots,16) \tag{9}$$

Step 2. Assume the size of the original image P is $m\times n$, extract the corresponding 1th, 3th, 6th, 8th bit-plane from image P to form one new image P_1, and the remained 2th, 4th, 5th, 7th bit-plane is transformed another image P_2 . The new pixel value range within [0, 15] in image P_1 and P_2 .

Because different bit-plane have different percentage of information contents, this method give a new definition of calculating the new pixel in image P_1 and P_2 by formula (10-11).

$$P_1(i) = p(i,1)\times 2^3 + p(i,8)\times 2^2 + p(i,3)\times 2^1 + p(i,6)\times 2^0, \tag{10}$$

$$P_2(i) = p(i,4)\times 2^3 + p(i,5)\times 2^2 + p(i,2)\times 2^1 + p(i,7)\times 2^0, i = 1,2,\cdots,m\times n \tag{11}$$

wher $p(i, j)$ denote j bit for the pixels in image P ; $p_1(i)$ and $p_2(i)$ refer to pixels in image P_1 and P_2 respectively.

Step 3. Based on two given fixed key $perkey\_1$ =0.67540987724 and $perkey\_2$ =0.45639241951, calculate the initial value key_1 and key_2 by following formula (12) respectively, then employ the logistic map with the secret keys key_1 and key_2 to generate two sequence s_1 and s_2 whose length are $m\times n$, then modify their value by formula (13-14) . The logistic is defined by formula (2):

$$key\_1 = perkey\_1 + \frac{x_1'}{4}, \; key\_2 = perkey\_2 + \frac{x_2'}{4}, \tag{12}$$

$$s_1(i) = \lfloor s_1(i)\times 10^{12} \rfloor \mathrm{mod}(m\times n) + 1, \tag{13}$$

$$s_2(i) = \lfloor s_2(i)\times 10^{12} \rfloor \mathrm{mod}(m\times n) + 1. \tag{14}$$

Step 4. Permutate two image P_1 and P_2 using the modified s_1 and s_2 accordingly, obtain two bit-level permutated image P_1' and P_2' .

Step 5. For image P_1' and P_2' , perform bit-level diffusion mentioned above. Use the logistic map with the control parameters x'_1 and x'_2 to create two sequences s_3 and s_4, the logical XOR operation is performed by formula (15-16):

$$I_1(i) = p'_1(i) \oplus s_3(i), \tag{15}$$

$$I_2(i) = p'_2(i) \oplus s_4(i). \tag{16}$$

where I_1 and I_2 are defined as the two bit-level diffusion cipher text.

Step 6 Transform two cipher-texts I_1 and I_2 into one by formula (17-19), reshape the new cipher text I' and obtain the bit-level diffusion cipher image A of size $m\times n$.

$$I'(i) = temp1 + temp2, \tag{17}$$

$$temp1 = I_1(i,1)\times 2^7 + I_1(i,2)\times 2^0 + I_1(i,3)\times 2^5 + I_1(i,4)\times 2^2, \tag{18}$$

$$temp2 = I_2(i,1)\times 2^4 + I_2(i,2)\times 2^3 + I_2(i,3)\times 2^6 + I_2(i,4)\times 2^1. \tag{19}$$

where i $(i = 1,2,.....m\times n)$ denotes the position in cipher text I' .

Step 7. The image is split into blocks of group, obtain small blocks $B_1, B_2, B_3,.....B_{sum}$ (sum is total numbers of blocks). If the width and height are not divisible by 4, some columns or rows should be added with 0.

Step 8 Iterate the CML once with the initial values $(j = 1,2,......16)$ and $\varepsilon = 0.367543987623764509\text{-}73216$ to obtain $d(j)$ $(j = 1,2,......16)$ to construct CML block D of sized 4×4.

Step 9. Construct the intermediate block B'_i based on the small block B_i and CML block D, calculate the parameter p by following formula (20).Especially, we set $p_0 = 100, \alpha = 56, (\alpha \in [0,255])$.

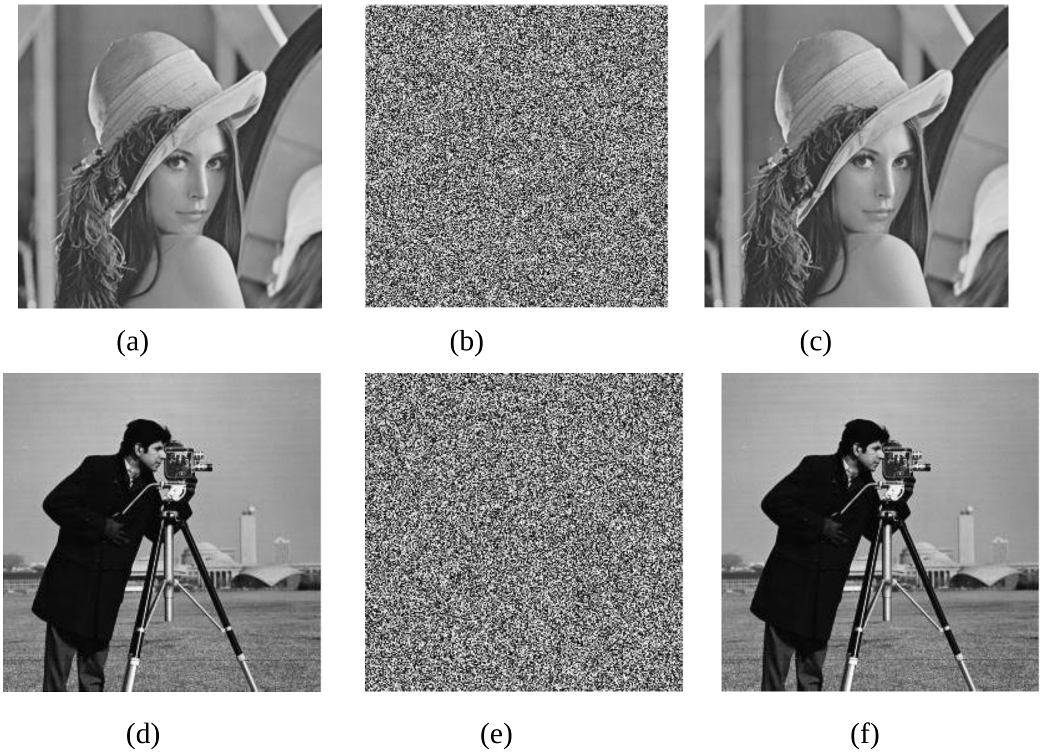
$$p_{i-1} = \left\lfloor \frac{\sum_{j=2}^{16} B'_i(j) + \alpha}{16 \times 255} \times 10^8 \right\rfloor \mathrm{mod}\, 256, \tag{20}$$

Step 10. Input the obtained intermediate block B'_i, p_{i-1} and sequence $d(j)$ $(j = 1,2,......16)$ to perform the small block diffusions. Get the small block cipher C_i.

Step 11. Iterate the step 8-10 until all small blocks $B_1, B_2, B_3, ...B_{sum}$ are encoded, reconstruct the obtained cipher C_i $(i = 1,2.....sum)$ get the final cipher image C.

4. Simulation Results and Analysis

In this section, the simulation results and analysis for proposed method are given. The simulation adopt the Matlab 2013a to testify out proposed method, all the simulation were performed on a personal computer with 2GHz CPU, 4G memory Microsoft Windows 7 operation system. Figure 1 (a-f) show the simulation results. The plaintext image we choose are "Lena" and "Camera" of size 256 256 (as Figure 1 (a), Figure 1 (d)).Some secret keys for image "Lena" are set $x'_1 =$ 0.508599853515625, $x'_2 =$ 0.504786173502604, while the value of x_1' and x_2' is differ from every image. Besides the initial values of CML are set $X = [x_1, x_2......x_{16}]$.



(a) (b) (c)

(d) (e) (f)

Figure. 1 Encryption and decryption results of (a)-(c)”Lena” and (d)-(f) “Camera”

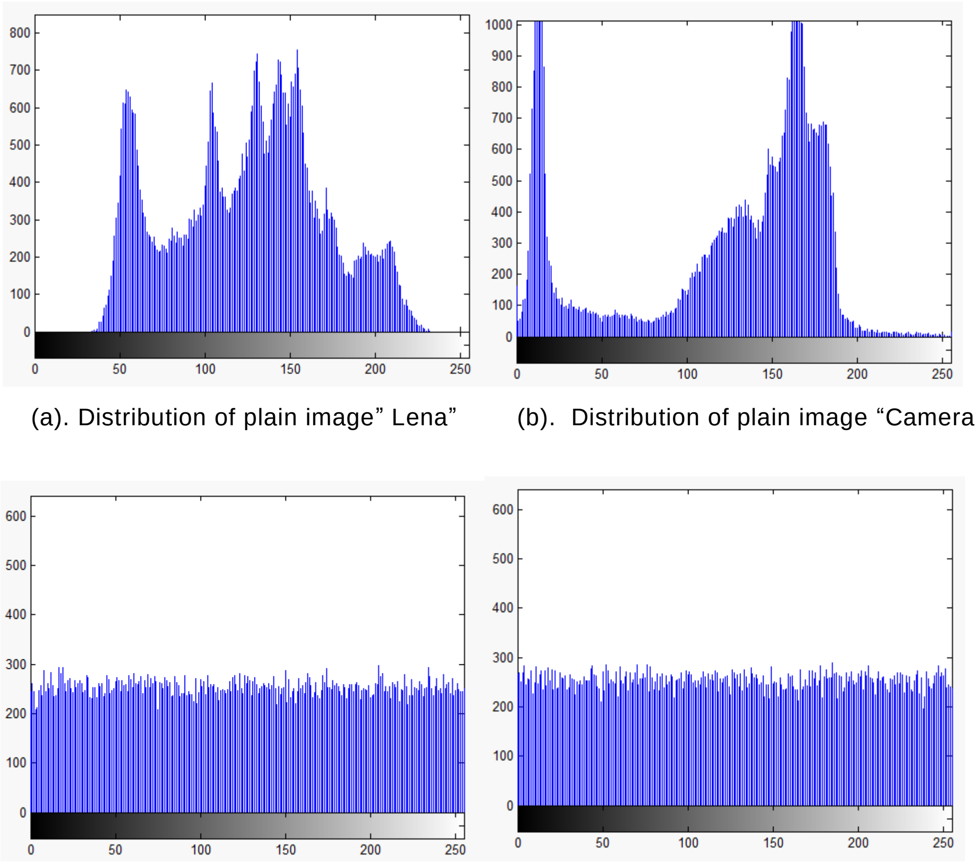
4.1. Key Space Analysis

An image encryption method which performs well should have enough large key spaces, so that the brute-force attack is infeasible for information eavesdroppers. In proposed method, several initial values such as u,α,x_1',x_2' , per_key1 , per_key2 and ε have been treated as secret keys, the initial array which include all initial values for CML should also be included as the part of the secret keys .We have verified this fact that the secret key spaces is large enough, it will be much time-consuming and complex to attack and acquire original images.

4.2. The Histograms of Images

Modifying the distribution features should be concerned for image encryption. A histogram is defined as a graph that shows the distribution of pix values of an image. It has been noticed that statistics attacks will be very effective and high-performed when some statistics data are captured, such as histograms. If the cipher fails to cover its original values, which causes obtained histogram is not flat-enough, thus we should reconsider the performance of this method we adapt. Therefore, A flat distribution is desirable for image encryption.

Figure 2(a)-(d), illustrates the histograms of plain images “Lena”, “Camera “and their cipher images. It is clear that Our proposed methods have satisfy this requirement.



(a). Distribution of plain image” Lena”

(b). Distribution of plain image “Camera”

(c). Distribution of cipher image “Lena”

(d). Distribution of cipher image “Camera”

Figure 2. Histograms of the Plain Images and Ciphered Images

4.3. Information Entropy Analysis

Information entropy is a most important measure of randomness. The source of information is defined as m ; we can obtain the formula (21) for calculating information entropy:

$$H(m)=\sum_{i=0}^{M-1}p(m_i)\log\frac{1}{p(m_i)} \tag{21}$$

where M is the total number of symbols $m_i \in m$; $p(m_i)$ denotes the probability of symbols. It is assumed that an information source send out 256 symbols, we may get ideal value $p(m_i)$ by formula (21), which reveals the information is completely random. The more the experiment information entropy is close to 8, the better performance of random is, and it will be less possibility for attacker to decrypt cipher image. The information entropy is listed in Table 1.

Table 1. Information Entropies of Plain Image and Cipher Image

Original image	Entropy of plain image	Entropy of cipher image
Lena	7.3482	7.9973
camera	7.1048	7.9970

It is evident that entropy is close to 8 in our proposed method, so we conclude it will be difficult to indulge information.

4.4. Differential Attack

A good image encryption method must be resistant to differential attack, which refers that the slight alteration in a plain image should bring a substantial change in cipher image. Therefore, two quantity measure indexes are put forward--Number of pix change rate (NPCR) and Unified average changing intensity (UACI).

Number of pix change rate (NPCR) are designed to evaluate the changed pix numbers in cipher image, when we only change one pix in plain image. More closely the NPCR is to 100%, the more effective our methods will perform. Unified average changing intensity (UACI) refers to average values of difference in intensity between two cipher images. Bigger the UACI is, the better our method resist the differential attack. They are defined as follow formula (22-23):

$$NPCR=\frac{1}{W\times H}\sum_{i=1}^{W}\sum_{j=1}^{H}D(i,j)\times 100\%, \tag{22}$$

$$UACI=\frac{1}{W\times H}\left(\sum_{i=1}^{W}\sum_{j=1}^{H}\frac{|C_1(i,j)-C_2(i,j)|}{255}\right)\times 100\%, \tag{23}$$

where W,H represent the width and height of image, respectively; C_1 and C_2 are respectively cipher images before and after one pixel is changed in plain image; $D(i,j)$ is defined by the rules: if $C_1(i,j)\neq C_2(i,j)$, then $D(i,j)=1$, otherwise, $D(i,j)=0$.

For the gray images, the ideal value of NPCR and UACI is 99.60% and 33.4% respectively. In our test, the NPCR and UACI of image “Lena” and “camera” are listed in Table 2. The experiment data have shown our proposed method could resistant the differential attacks effectively.

Table 2 NPCRs and UACIs of image “Lena” and “Camera”

Plain image	NPCR (%)	UACI (%)
Lena	99.6429	33.4269
Camera	99.6353	33.5412

4.5. Correlation Analysis

Correlation reflects a linear relationship between two random variables. In image processing, it is employed to measure the relativity extent between two adjacent pixes. The correlation between adjacent pixes generally is high in discernible images, which may bring some security problems if this feature is neglected. Therefore, the method should break this correlation between adjacent pixes as much as possible. The less correlation is, the more effective our method perform, so the correlation coefficients should be computed between horizontally adjacent pixels, two vertically pixels and two diagonally adjacent pixels by following definition (24):

$$r_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{24}$$

where,

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

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \quad , \quad D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 .$$

To test the three correlation mention above, we randomly select 2000 pixels pairs of adjacent position in each direction from plain image “Lena”, “Camera “and their corresponding cipher image respectively. The correlation efficient are calculated and listed in Table 3.

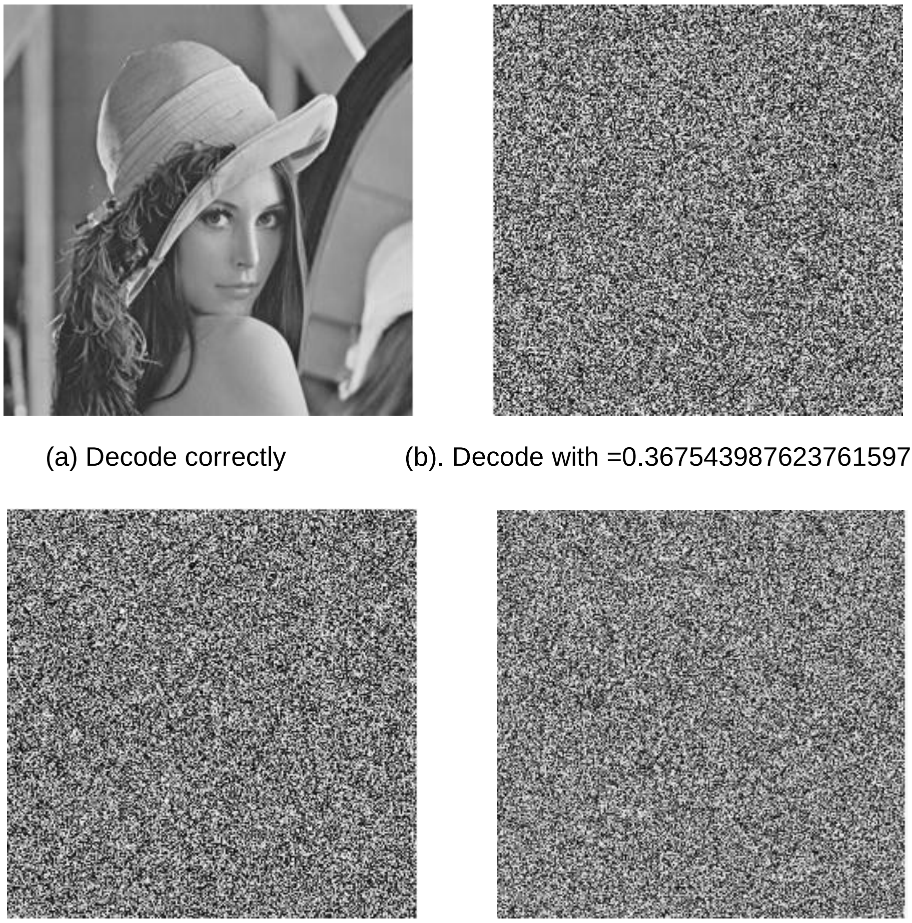
Table 3 have shown the high correlation efficient in original images, which demonstrate the fact that the existence of strong relationships between adjacent pixels indifferent direction. Contrary to the plain images, there are low correlation efficient in obtained cipher image by proposed method, they are indicated a negligible correlation.

Table 3 Correlation Coefficients of the Plain Images and Their Ciphered Images

		horizontal	vertical	diagonal
Plain image	Lena	0.9717	0.9458	0.9192
	Camera	0.9610	0.9245	0.9157
Cipher image	Lena	-0.0092	0.0043	-0.0138
	Camera	0.0015	0.0030	0.0093

4.6. Key Sensitivity

Key sensitivity should not be neglected when designing an effective and high security image encryption method. Taking the secret key ε , x_1' and x_2' for example. We employ the image “Lena” to make sure the key sensitivity. The test strategy adopted is to make a small change for key ε , x_1' and x_2' when other keys keep the same as before, then decrypt the cipher image, obtained test results by proposed method have been shown in Figure 3, We use the correct secret key and obtain the original image as shown in Figure 3(a), while the decrypted image shown in Figure 3(b-d), is too messy to figure out the plain image when the secret key ε is altered at the precision with 10^{-15} . Thus we can make the similar changes for secret key x_1' and x_2' .Therein, we may conclude that our proposed method is sensitive to secret keys and is resistant to plaintext attack.



(a) Decode correctly (b). Decode with =0.36754398762376159 73216

(c). Decode with 0.508599853515629 (d). Decode with =0.504786173502601

Figure 3. Decoding Correctly Image and Decoding by a Slightly Changed Key

4.7. Resisting Chosen-Plaintext Attacks Analysis

Our proposed method employs some probability parameters as one part of secret keys, which is able to resist the plaintext attack. Some parameters are calculated on the basis of from original images and small-block images, so they will vary from different images.

This idea is introduced during the whole encryption process to ensure the ability to resist chosen-plaintext attack.

4.8. Comparison

In this section, our proposed method is compared with the Image encryption based on the finite field cosine transform[22], Image encryption based on the fractional Fourier transform over finite fields[23], Image encryption process based on chaotic synchronization phenomena [24]. The image “Lena” and “Camera” have been adopted to compare performance when using different algorithms. Table 4 has shown the detailed values of NPCR and UACI.

From Table 4, it is shown that our proposed method perform best compared with. The high values of NPCR and UACI can resist the differential attacks. Besides this, we have found that the algorithm [4] has a low precision in the test of key sensitivity. The proposed method can reach a level of 10^{-15} compared with 10^{-10} in scheme [25]. If the precision of key sensitivity is not high enough, it will be very tough to resist all kinds of attacks.

Table 4 NPCRs and UACIs of Image “Lena” and “Camera” Based on The Our Method and Compared Methods

	Image	NPCR (%)	UACI (%)
Our method	Lena	99.6429	33.4269
	camera	99.6353	33.5412
Method [22]	Lena	99.6098	33.4366
	Camera	99.6113	33.4469
Method[23]	Lena	98.5610	33.1187
	Camera	98.1977	32.9900
Method[24]	Lena	99.5863	33.4035
	Camera	----	----

5. Conclusion

The second and following pages should begin 1.0 inch (2.54 cm) from the top edge. On all pages, the bottom margin should be 1-3/16 inches (2.86 cm) from the bottom edge of the page for 8.5 x 11-inch paper; for A4 paper, approximately 1-5/8 inches (4.13 cm) from the bottom edge of the page.

References

[1] B. Liu, J. Peng. “Nonlinear dynamics. Beijing: High Education Press”, **(2004)**

[2] G. Chen, Y.B. Mao,C.K. Chui. “A symmetric image encryption scheme based on 3D chaotic cat maps”, Chaos Solitons &Fractals, vol. 21, no. 3, **(2014)** , pp. 749-761.

[3] H. J. Liu, X. Y. Wang. “Colour image encryption based on one-time keys and robust chaotic maps”, Computers & Mathematics with Applications, vol. 59, no. 10, **(2010)**, pp. 3320-3327.

[4] N. K. Pareek,V. “Patidar,K.K. Sud. Image encryption using chaotic map”, Image and Vision Computing, vol. 24, no. 9, **(2006)**, pp. 926-934.

[5] Y. B. Mao,G. R. Chen,S. G. Lian. “A novel fast image encryption based on 3D chaotic baker maps”, International Journal of Bifurcation and Chaos, vol. 14, no. 10, **(2004)**, pp. 3613-3624.

[6] Y. C. Zhou,L. Bao,C. L. P. Chen. "Image encryption using a new parametric switching chaotic system. Signal Processing", no. 93, no. 11, **(2013),** pp. 3039-3052.

[7] N. K. Pareek,V. Patidar,K. K. Sud. "Diffusion-substitution based gray image encryption scheme", Digital Signal Process, vol. 23, no. 3, **(2013)**, pp. 894-901.

[8] X. F. Liao, S. Y. Lai, Q. Zhou. "A novel image encryption algorithm based on self-adaptive wave transmission", Signal Processing, vol. 90, no.9, **(2010)** pp. 2714-2722.

[9] A. Akhshani, A. Akhavan, "A. Mobaraki. Pseudo random number generator based on quantum chaotic map", Communications in Nonlinear Science and Numerical Simulation, vol. 19, no .1, **(2014)**, pp. 101-111.

[10] S. Ercan, C. Cahit, O. T. Yildiz. "Cryptanalysis of Fridrich's Chaotic Image Encryption", International Journal of Bifurcation and Chaos, vol. 20, no. 5, **(2010)**, pp. 1405-1413.

[11] L.Y. Zhang, C. Q. Li. Cryptanalyzing a chaos-based image encryption algorithm using alternate structure. Journal of Systems and Software, 2012, 85(9): 2077-2085

[12] S. J. Lian, J. S. Sun, Z. Q. Wang. "Security analysis of a chaos-based image encryption algorithm", Physica A-Statistical Mechanics and its Application, vol. 351, no. 2-4, **(2005)**, pp. 645-661.

[13] R. Rhouma, B. Safya. "Cryptanalysis of a new image encryption algorithm based on hyper-chaos", Physics Letters A, vol. 372, no. 38, **(2008)**, pp. 5973-5978.

[14] Wang, X. Qin, "A new pseudo-random number generator based on CML and chaotic iteration", Nonlinear Dynamics, vol. 70, no. 2,**(2012)**, pp. 1589-1592.

[15] X. Y. Wang, L. Teng. "An image blocks encryption algorithm based on spatiotemporal chaos". Nonlinear Dynamics, vol. 67, no. 1, **(2012)**, pp. 365-371.

[16] Y. Tang, Z. D. Wang, J. A. Fang. "Image encryption using chaotic coupled map lattices with time-varying delays", Communications in Nonlinear Science and Numerical Simulation, vol. 15, no.9, **(2010)**, pp. 2456-2468.

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

[18] I. Hussain,T. Shan, M. A. Gondal. A novel image encryption algorithm based on chaotic maps and GF(2(8)) exponent transformation. Nonlinear Dynamics, vol. 72, no. 1-2, **(2013)**, pp. 399-406.

[19]] R. S. Ye. "A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism", Optics Communications, vol. 284, no. 22:, (**2011**), pp. 5290-5298.

[20] Y. S. Zhang, D. Xiao. "An image encryption scheme based on rotation matrix bit-level permutation and block diffusion", Communications in Nonlinear Science and Numerical Simulation, vol. 19, no. 1, **(2014)**, pp. 74-82.

[21] F. Y. Sun, L. Z. Wang. Digital image encryption with chaotic map lattices. Chinese Physics B, vol. 20, no. 4, **(2011)**, 040506

[22] J. B. Lima, E. A. O.Lima, F. Madeiro. "Image encryption based on the finite field cosine transform", Signal Processing Image Encryption, vol. 28, no. 10, **(2013)**, pp. 1537-1547.

[23] J. B. Lima, L. F. G. Novaes. "Image encryption based on the fractional Fourier transform over finite fields", Signal Processing, 94:, **(2014)**, pp. 521-530.

[24] Ch. K. Volos, I. M. Kyprianidis, A. Mobaraki. " Image encryption process based on chaotic synchronization phenomena", Signal Process, vol. 95, no. 5, **(2013)**
pp. 1328-1340.

[25]] H. J. Li, Y. R. Wang, H. T. Yan. "Double-image encryption by using chaos-based local pixel scrambling technique and gyrator transform", Optics and Lasers in Engineering, vol. 51, no. 12, **(2013)**, pp. 1327-1331