I.J. Computer Network and Information Security, **2014, 4, 37-45**
Published Online March 2014 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2014.04.05

An Image Encryption Scheme Based on Chaotic Systems with Changeable Parameters

Ruisong Ye, Wenhua Guo
Department of Mathematics, Shantou University Shantou, Guangdong, 515063, P. R. China
Email: rsye@stu.edu.cn

***Abstract* —** This paper proposes an image encryption scheme based on chaotic system with changeable parameters depending on plain-image. A generalized Arnold map, whose control parameters are changeable and image-dependent during the iteration procedure, is utilized to generate chaotic orbits applied to permute the pixel positions. A diffusion function is also designed to realize the diffusion effect by piece-wise linear chaotic map. In both the permutation process and the diffusion process, the keystreams generated by chaotic maps are all strongly dependent on plain-image, and thereby can improve the encryption security efficiently. The major merits of the proposed image encryption scheme include a huge key space, good statistical nature resisting statistical analysis attack, differential attack, and good resistance against known-plaintext attack and chosen-plaintext attack, etc. Experimental results have been carried out with detailed analysis to show that the proposed scheme can be a potential candidate for practical image encryption.

***Index Terms* —** Image-dependent; generalized Arnold map; piece-wise linear chaotic map; ergodicity; permutation; diffusion.

I. INTRODUCTION

With the rapid development of multimedia and network technology, a bulk of digital visual data, such as digital images, video, and audio, etc. has revolutionized in the way of largely stored, manipulated, and transmitted over the Internet and wireless networks. Creative ways of storing, accessing and distributing data have generated lots of benefits into the digital multimedia field. However, the visual data often contain private or confidential information or are associated with financial interests, and therefore the data security encounters a serious threat in the process of transmission due to the openness and sharing of the networks. To meet the demand of real-time secure image transmission, techniques are required to provide security functionalities like privacy, integrity, or authentication especially suited for image data types. As a matter of fact, these techniques for providing privacy and confidentiality of visual data play an important role in many applications, such as military image databases, confidential video conferences, cable TV, medical imaging system, online private photograph album, etc. To provide the protection of digital data, two complementary techniques have been developed: encryption and watermarking. Because images possess some intrinsic features, such as bulk data capacity, high correlation among adjacent pixels, redundancy of data, less sensitivity as compared to the text data, the traditional block ciphers, such as Date Encryption Standard (DES), International Date Encryption Algorithm (IDEA) and Advanced Encryption Standard (AES) are thereby not suitable for practical image encryption in real time, because their speed is low due to a bulk data volume and strong correlation among adjacent pixels [1]. Recently, chaos-based image encryption schemes [2-8] have shown their superior performance thanks to its ergodicity, pseudo-randomness and high sensitivity to initial conditions and control parameters, which are close to confusion and diffusion in cryptography. These properties make chaotic systems a potential choice for constructing cryptosystems [9, 10].

Chaos-based image cryptosystems can be classified into three categories according to their architecture, that is, permutation-only, diffusion-only and permutation-diffusion form. Among them, the permutation-only type image cipher is superior in the aspect of efficiency due to its lowest computational complexity. It only shuffles the position of each pixel in a secret order while it does not alter its gray value, therefore cannot change the histogram of plain image. The diffusion-only one changes the pixel gray value one by one or block by block, which gets greatly modified histogram for cipher-image which is generally uniform distributed and therefore significantly different from the histogram of plain image. In this sense, diffusion-only can resist the statistical analysis, differential attacks efficiently and so remedy the default of permutation-only type encryption methods. The permutation-diffusion mechanism not only permutes the pixels positions utilizing chaotic systems, but also alters the pixel gray values sequentially by some diffusion functions. The modification made to a pixel usually depends on the accumulated effect of all the previous pixels' gray values, so that a slight change in one pixel can be spread out to almost all the subsequent pixels. However, among the existing image encryption schemes, the key streams generated by chaotic systems in both the permutation process and the diffusion process are generally fixed and independent of plain-images, which becomes the most serious flaw for chaos-based ciphers. Cryptanalysis has shown that chaos-based image encryption schemes can be broken, especially for the

permutation process [11-15]. The opponents can analyze the cryptography schemes via chosen-plaintext or known-plaintext attack to obtain the key streams and so equivalently obtain the keys. The major reason lies in the keystreams yielded by chaotic systems are nothing with the plain-images. A number of chaos-based schemes with good diffusion functions are designed to resist known-plaintext attack and chosen-plaintext attack [16-19]. However there are few image encryption schemes considering the issue in the permutation process. In this paper, a novel image encryption scheme based on chaotic system with changeable parameters is proposed. An essential difference between the encryption scheme proposed here and the conventional encryption scheme is that the parameters of the chaotic system here are changing at each iteration of the chaotic system. The changeable parameters are strongly related to the plain-images and therefore the proposed permutation process can efficiently resist known-plaintext attack and chosen-plaintext attack. A diffusion function is also designed to finish the diffusion stage to make the proposed scheme more secure. In both the permutation process and the diffusion process, the key streams are generated strongly dependent on the plain-images. As a result, the proposed encryption can achieve one-time keystreams in which different plain-images will generate different keystreams. Other merits of the proposed image encryption scheme are achieved as well, including a huge key space, great sensitivity to cipher keys, good statistical properties resisting statistical attack and differential attack, good entropy analysis, etc. Experimental results have been carried out with detailed analysis to show that the proposed scheme can be a potential candidate for practical image encryption.

The rest of this paper is organized as follows. In Section II, the generalized Arnold map and the piece-wise linear chaotic map are introduced briefly. Section III proposes a novel image encryption based on chaotic system with changeable parameters dependent on plain-images. Section IV gives the detailed experiment results and security analysis. Section V makes some conclusions.

II. THE GENERALIZED ARNOLD MAP AND THE PIECE-WISE LINEAR CHAOTIC MAP

A. The generalized Arnold map

Arnold map is also called cat map. It is a two-dimensional invertible chaotic map introduced by Arnold and Avez [20]. The classical Arnold map is described by

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod 1 \qquad (1)$$

where "$x \bmod 1$" means the fractional part of a real number x by adding or subtracting an appropriate integer. Therefore (x_n, y_n) is confined in the unit square $[0,1)^2$. The map is area preserving since the determinant of its linear transformation matrix is 1. As shown in Fig.1, the unit square is first stretch by the linear transform matrix and then folded back to the unit square by the modulo operation.

The above 2D cat map (1) can be generalized to the following form by introducing two integer control parameters $a>0$ and $b>0$,

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & 1+ab \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod N. \qquad (2)$$

The generalized Arnold map (2) has one Lyapunov characteristic exponent $\sigma_1 = 1 + \frac{1+ab+\sqrt{a^2b^2+4ab}}{2} > 1$, so the map is always chaotic for $a>0$, $b>0$.

In this paper, we extend the integer control parameters a and b to real numbers. This is an essential difference from the control parameters in conventional generalized Arnold maps. As a result, we can enlarge the key space significantly. Fig. 2 (a) shows an orbit of $(x_0, y_0) = (0.5231, 0.7412)$ with length 1500 derived by the generalized Arnold map (2) with a=5.324, b=18.2, the x-coordinate and the y-coordinate sequences of the orbit are plotted in Fig. 2 (b) and Fig. 2(c) respectively.

B. The piece-wise linear chaotic map

The piece-wise linear chaotic map (PWLCM) can be described as follows

$$x_{i+1} = F_p(x_i) = \begin{cases} x_i / p, & 0 \le x_i < p, \\ (x_i - p)/(0.5 - p), & p \le x_i < 0.5, \\ F_p(1 - x_i), & 0.5 \le x_i < 1, \end{cases} \qquad (3)$$

where $x_i \in [0,1)$, when control parameter $p \in (0, 0.5)$, the PWLCM system (3) evolves into chaotic state [21]. p and x_0 can be served as cipher keys. The PWLCM system has uniform invariant distribution and very good ergodicity, confusion and determinacy, so it can provide excellent random sequence, which is suitable for cryptosystem.

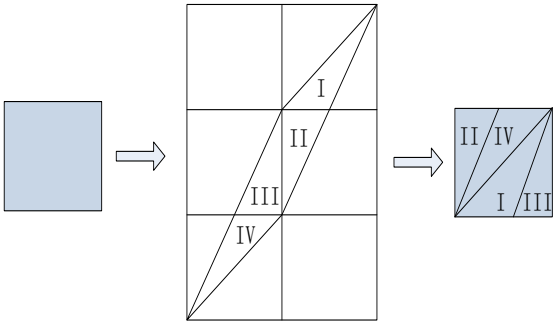
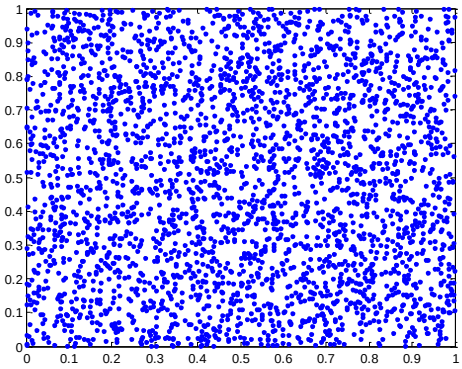
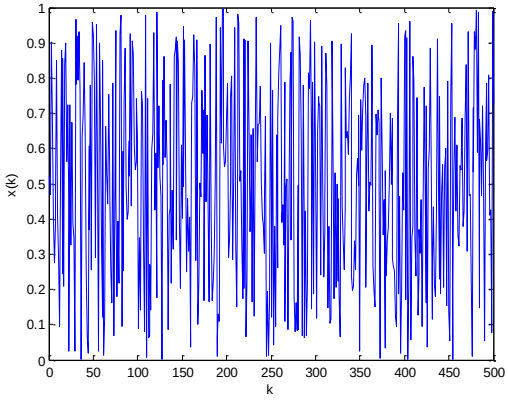


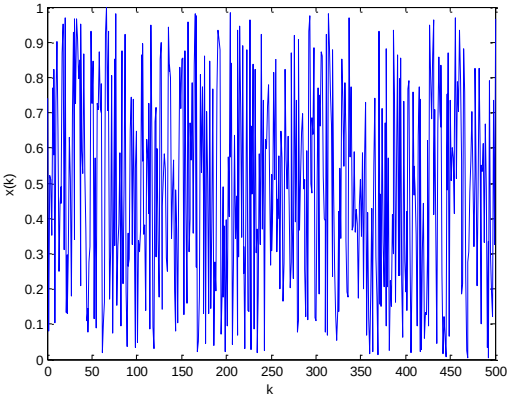
Figure.1 The Arnold map



(a) The orbit of (0.5231, 0.7412)



(b) x -coordinates sequence



(c) y -coordinates sequence

Figure.2. Orbit derived from the generalized Arnold map with a=5.324, b=18.2

III. THE PROPOSED IMAGE ENCRYPTION SCHEME

The proposed image encryption scheme consists of one permutation stage and one diffusion stage. Without loss of generality, we assume that the plain-image A is a gray image of size $L = M \times N$ and 256 gray-scale levels; A is an integer matrix of M rows and N columns, in which the values range from 0 to 255 representing the gray values of the digital image with 256 gray-scale levels.

A. Permutation stage

Given the initial conditions x_0 , y_0 and control parameters a , b , we iterate generalized Arnold map (2) to generate an orbit $\{(x_k, y_k); k = 0,1,2,..., N_0\}$ with iteration time N_0 large enough. Let

$$s_k = floor(x_k \times M) + 1, t_k = floor(y_k \times N) + 1.$$

Then $(s_k, t_k), k = 0,1,\cdots, N_0$ must be the positions of some pixels in A. In case that some coordinates are the same, we delete the repeated coordinates and preserve the first one. Then the pixel values of those preserved coordinates in A are put in a vector V with length $L = M \times N$ orderly. According to the ergodicity of the Arnold map, as long as the orbit is long enough, all the coordinates of the pixels in A can be found in

$$\{(floor(x_k \times M) + 1,\ floor(y_k \times N) + 1); k = 0,1,..., N_0\}$$

However, one suitable N_0 is applied in order to save computational time and storage, and therefore there may be some coordinates that cannot be found in the finite orbit sequence. Find out these pixel values and put in the rest part of V . Then reshape V back to one 2D matrix to yield the shuffled image A_1 . The detailed permutation process is outlined as follows.

Step1: Set the values of x_0 , y_0 , a , b for the generalized Arnold map.

Step2: Iterate map (2) to generate the orbit of (x_0, y_0) : $\{(x_k, y_k) : k = 0,1,2,..., N_0\}$ by the following formula

$$\begin{pmatrix} x_k \\ y_k \end{pmatrix} = \begin{pmatrix} 1 & a_{k-1} \\ b_{k-1} & 1 + a_{k-1} b_{k-1} \end{pmatrix} \begin{pmatrix} x_{k-1} \\ y_{k-1} \end{pmatrix},\ k = 1,2,..., N_0,$$

where

$$a_0 = a, b_0 = b,$$
$$a_k = A(\ floor(x_k \times M) + 1,\ floor(y_k \times N) + 1),$$
$$b_k = floor(x_k \times M) + floor(y_k \times N) + 2,$$
$$k = 1,2,... N_0.$$

Throughout the paper, "*floor*" operation on x returns the largest value not greater than x.

Step3: Perform the following formula to transform (x_k, y_k) into integer sequence:

$$i_k = floor(x_k \times M) + 1, \quad k = 0,1,2,...N_0,$$
$$j_k = floor(y_k \times N) + 1, \quad k = 0,1,2,...N_0.$$

Step4: Let i_k be the first column and j_k be the second column to construct a coordinate matrix S sized $N_0 \times 2$, then each row of S can be regarded as the coordinates of a certain pixel in A. If there are repeated coordinates in S, then only preserve the first one to get a coordinates matrix $S1$ with different coordinates and size $l \times 2$.

Step5: Let B be a $M \times N$ indexing matrix initialized by zero matrix, then set

$$B(S1(i,1), S1(i,2)) = 1, \ i = 1,2,....,l.$$

Find out the positions in B whose element values are zero and then place them in a vector T sized $(L-l) \times 2$.

Step6: Permute the pixels in the plain-image to get a vector V with length L by the following way

$$V(i) = A(S1(i,1), S1(i,2)), \quad i = 1,2,....,l,$$
$$V(l+j) = A(T(j,1), T(j,2)), \ j = 1,2,...,L-l.$$

Step7: Reshape V back to a 2D matrix to yield the shuffled image A_1.

B. Diffusion stage

Diffusion stage can enhance the resistance to statistical analysis and differential attack greatly, in which the histogram of the cipher-image is fairly uniform, and is significantly different from that of the plain-image. A slight change in one pixel could be spread out to almost all the subsequent pixels. The diffusion process is outlined as follows.

Step1: Transform the shuffled image A_1 into a one-dimensional vector denoted by q with length $L = M \times N$.

Step2: Set the values of initial condition t_0 and control parameter p of the PWLCM system. Iterate the PWLCM system k times to discard the transitional part and set $w(1)=t_k$.

Step3: Let $i=1$.

Step4: Use the following formula to yield $b(i)$

$$b(i) = floor(w(i) \times 10^{14}) \bmod 256.$$

Step5: Compute the pixel gray value in the cipher-image by

$$c(i) = ((c(i-1) + q(i)) \bmod 256) \oplus b(i),$$

where $c(i)$ is the pixel value of cipher-image; $c(0)$ can be set to one part of the cipher keys in the diffusion process.

Step6: Compute h by $h = (c(i) \bmod 3) + 1$ to get the next $w(i+1)$ by iterating the PWLCM system with parameters p on $w(i)$ for h rounds.

Step7: Let $i=i+1$ and return to step 4 until i arrives at L.

Step8: Reshape c back to one 2D matrix to yield the cipher-image A_2.

IV. EXPERIMENTAL RESULTS AND PERFORMANCE ANALYSIS

We set the initial values and control parameters as follows.

Permutation process:

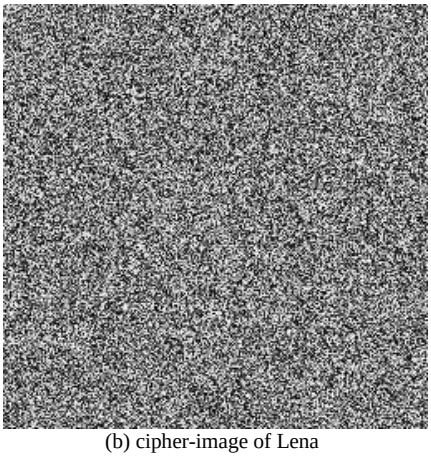
$$x_0 = 0.3201, y_0 = 0.6317, a = 3.631, b = 27, N_0 = 230000.$$

Diffusion process:

$$t_0 = 0.2356, p = 0.3651, c(0) = 56, k = 100.$$

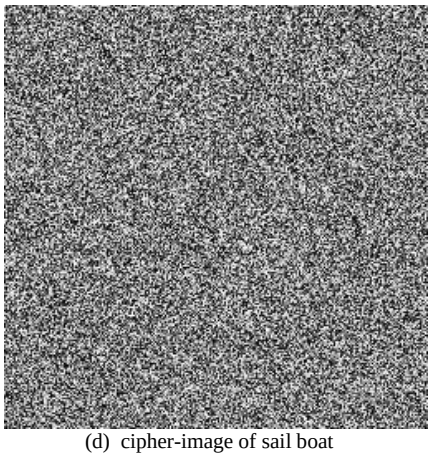
We choose the 256×256 gray images Lena and sail boat for simulation. Figs. 3(a), (c) are the plain-images Lena and sail boat respectively, Figs. 3 (b), (d) are the corresponding cipher-images respectively.

(a) plain-image Lena

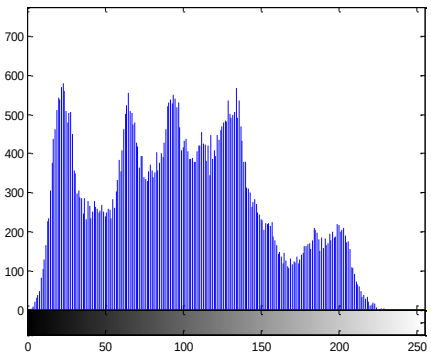


(b) cipher-image of Lena

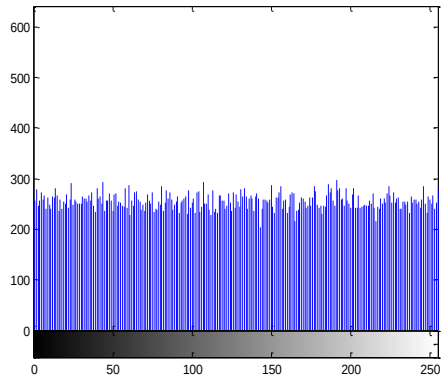
(c) plain-image sail boat



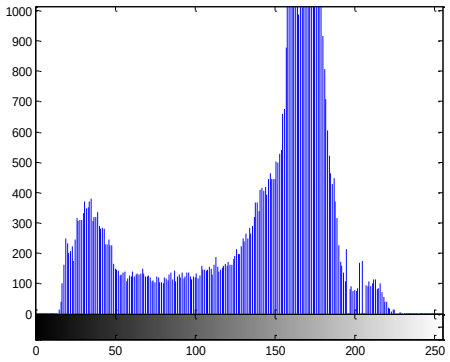
(d) cipher-image of sail boat



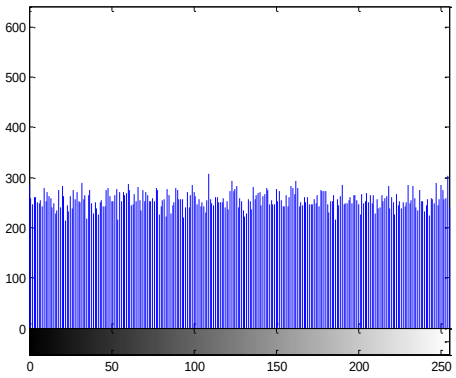
(e) Histogram of the plain-image Lena



(f) Histogram of the cipher-image of Lena



(g) Histogram of the plain-image sail boat



(h) Histogram of the cipher-image of sail boat

Figure 3. The encrypted results.

The crucial measure for the quality of a cryptosystem is its capability to withstand the attempts of an unauthorized participant or an opponent to gain knowledge about the unencrypted information. A good cryptosystem should resist all kinds of known attacks, such as known /chosen plaintext attack, statistical attack, differential attack, and brute-force attack. In the following subsections, security analyses have been performed for the proposed image encryption scheme, including the most important ones like key space analysis, statistical analysis, and differential attack. All the analyses show the proposed image encryption scheme is highly secure.

A. Key space analysis

Key space size is the total number of different keys which can be used in the encryption. A good encryption algorithm should be sensitive to the cipher keys, and the key space should be large enough to make brute-force attack impossible.

The analysis result regarding the sensitivity and the key space are summarized as follows. Assume that we want to verify the sensitivity of parameter K, we encrypt the plain-image $A=(A(i,j))_{M\times N}$ with K, K-ΔK and $K+\Delta K$ respectively while keeping the other parameters unchanged, the corresponding encrypted images are A_1, A_2, A_3 respectively, where ΔK is the perturbing value. The sensitivity coefficient of parameter K is then calculated by

$$P_s(K)=\frac{1}{2\times M\times N}\sum_{i,j}[N_s(A_1(i,j),A_2(i,j))+N_s(A_1(i,j),A_3(i,j))]\times 100\%$$

Where

$$N_s(x,y)=\begin{cases}1, & x\neq y,\\ 0, & x=y.\end{cases}$$

In the case that ΔK is small, the larger $P_s(K)$ means the more sensitivity for parameter K. Table I shows the results of the sensitivity test. The variations for the considered cipher keys are shown as follows.

Permutation process:

$$\Delta a=10^{-15},\Delta b=10^{-14},\Delta x_0=10^{-15},\Delta y_0=10^{-15},$$

Diffusion process:

$$\Delta t_0=10^{-16},\Delta p=10^{-16},\Delta c(0)=1,\Delta k=1.$$

The result in Table I shows that the parameters x_0, y_0, a, b, t_0, p, $c(0)$, k are all strongly sensitive. It also implies from the result that the key space is more than 10^{91}, which is large enough to frustrate brute-force attacks.

TABLE I. SENSITIVITY OF THE CIOPHER KEYS.

K	a	b	x_0	y_0
$P_s(K)$	99.59	99.60	99.58	99.61
K	t_0	p_0	$c(0)$	k
$P_s(K)$	99.58	99.62	99.61	99.60

B. Statistical analysis

A good cryptosystem should be robust against any statistical attack. In order to verify the robustness of the proposed scheme, we perform the following statistical tests such as the histogram, information entropy, and the correlation of two adjacent pixels in the images.

(I) Histogram. An image histogram shows that how pixels in an image distribute by plotting the number of pixels at each gray-scale level. The histogram of the encrypted image is very important; it should not leak the information about the plain-image or the relationship between plain-image and the cipher-image. Figs. 3(e), (g) show the histograms of the plain-images Lena and sail boat respectively, Figs. 3(f), (h) are the histograms of their encrypted images respectively. From Figs. 3(f), (h), we can see that the histograms of the encrypted images yielded by the proposed encryption scheme are fairly uniform and significantly different from the histograms of the plain-images, and hence it does not provide any useful information for the opponents to perform the statistical attack.

(II) Correlation of adjacent pixels. For an ordinary image having definite visual content, each pixel is highly correlated with his adjacent pixels either in horizontal, vertical or diagonal direction. However, an efficient image cryptosystem should produce the encrypted image with sufficient low correlation in the adjacent pixels.

To test the correlation between two adjacent pixels in plain-image and the cipher-image, we randomly select 2500 pairs of two-adjacent (at horizontal, vertical, and diagonal directions) from plain-image and cipher-image, and calculate the correlation coefficient of each pair by the following formula.

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

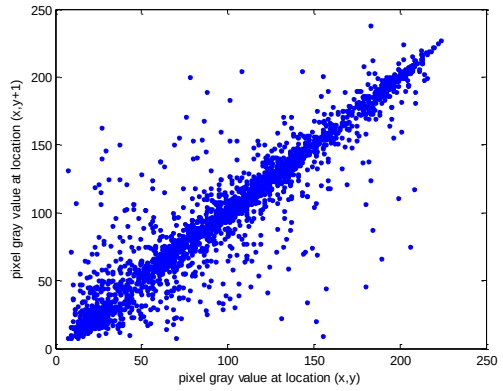
$$\mathrm{cov}(x,y)=E[(x-E(x))(y-E(y))],$$

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

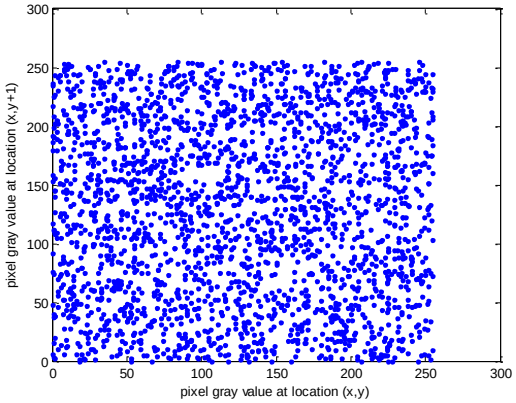
where x and y are gray-scale values of two adjacent pixels in the image, and T denotes the total number of samples. The correlation distributions of two horizontally adjacent pixels of the plain-image and the encrypted image produced by the proposed scheme are shown in Fig. 4, from which we can see that the strong correlation between adjacent pixels in plain-image is greatly reduced in the encrypted image. Table II shows the correlation coefficients of horizontal, vertical, and diagonal adjacent pixels for the plain-images and the cipher-images. The results indicate that the correlations of two adjacent pixels of the encrypted Lena and encrypted sail boat are much smaller compared with the plain-images, which implies that the proposed image encryption scheme is efficient to achieve good statistical nature.

TABLE II. CORRELATION COEFFICIENTS OF TWO ADJACENT IN PLAIN-IMAGES AND CIPHER-IMAGES

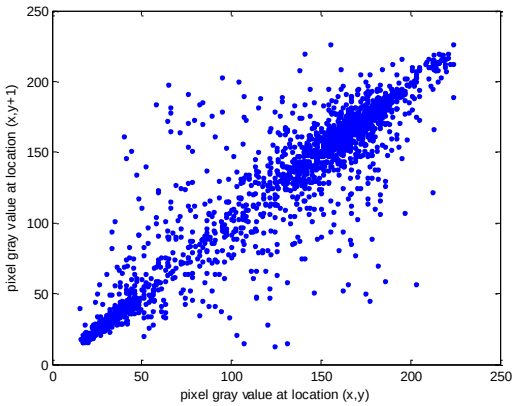
	Horizontal	Vertical	Diagonal
Lena image	0.9439	0.9663	0.9225
Encrypted Lena	-0.0148	-0.0027	0.0015
Sail boat	0.9217	0.9242	0.8793
Encrypted sail boat	-0.0045	0.0014	0.0079



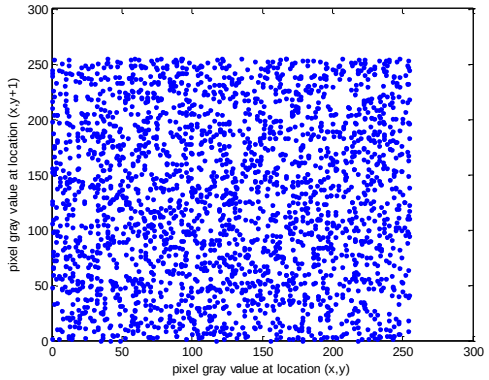
(a) plain-image Lena



(b) cipher-image of Lena



(c) plain-image sail boat



(d) cipher-image of sail boat

Figure. 4. Correlation distributions of plain-images and cipher-images.

(III) Information entropy. Information entropy is the most important feature of randomness. Let m be the information source. The formula to calculate information entropy is

$$H(m) = -\sum_{i=0}^{2^n-1} p(m_i)\log_2 p(m_i)$$

where n is the number of bits to represent a symbol $m_i \in m$ and $p(\mathrm{m}_i)$ represents the probability of symbol m_i.

For a truly random source emitting 2^n symbols, the entropy is $H(m) = n$. Therefore, for an encrypted image with 256 gray-scale levels, the entropy should be ideally $H(m) = 8$, which shows the information is completely random. Hence the information entropy of the encrypted image should be close to 8 after encryption to decrease the possibility of information leakage. The information entropy for the cipher-image of Lena is 7.9902, which implies the cipher-image is close to random sources.

C. Differential attack

Attackers usually make a slight change (e.g. modify only one pixel) of the plain-image and apply the proposed scheme to encrypt the original and the modified plain-images to get two cipher-images. Attackers can observe difference between the two cipher-images to find out the relationship between the plain-image and the cipher-image. This is the so-called differential attack. To test the robustness of the image cryptosystem against differential attack, two measures NPCR (net pixel change rate) and UACI (unified average changing intensity) are usually used. NPCR measures the percentage of different pixel numbers between the two encrypted images. UACI measures the average intensity of difference between the two encrypted images. They can be calculated by the following formulae:

$$\mathrm{NPCR} = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\%,$$

$$\mathrm{UACI} = \frac{1}{M \times N}\left[\sum_{i,j} \frac{|c_1(i,j) - c_2(i,j)|}{255}\right] \times 100\%$$

where c_1 and c_2 are the two cipher-images and $D(i, j)$ is defined as

$$D(i,j) = \begin{cases} 1, & c_1(i,j) \neq c_2(i,j), \\ 0, & \text{otherwise.} \end{cases}$$

We perform the test by changing a pixel gray value with a difference 1, for example, replace $A(23,36)$ to $A(23,36)-1$, then two plain-images are encrypted with same key to generate the cipher-images c_1 and c_2. The results are shown in Tables III-IV, from which we can see that the values of NPCR and UACI can reach 99.55% and 33.40% at the second round. It implies that the proposed scheme is sensitivity to small changes in the plain-image, in other words, the proposed scheme can resist differential attack efficiently.

TABLE III. NPCR PERFORMANCE.

Rounds	Lena image	Sail boat
1	80.54	30.21
2	99.59	99.61
3	99.55	99.57
4	99.60	99.59
5	99.64	99.59

TABLE IV. UACI PERFORMANCE.

Rounds	Lena image	Sail boat
1	27.08	10.01
2	33.46	33.41
3	33.35	33.32
4	33.52	33.40
5	33.50	33.52

V. CONCLUSIONS

An image encryption scheme based on chaotic systems with changeable parameters is proposed. In the proposed scheme, the parameters of the generalized Arnold map at the permutation process are changing for every iteration as they are plain-image dependent. A diffusion function is also designed to make the proposed scheme more secure. In both the permutation process and the diffusion process, the keystreams are generated strongly dependent on the plain-images. The proposed image encryption scheme can achieve one-time keystreams in the sense that different plain-images generate different keystreams. Other merits of the proposed image encryption scheme are achieved as well, including a huge key space, great sensitivity to cipher keys, good statistical properties resisting statistical attack and differential attack, good entropy analysis, etc.

ACKNOWLEDGMENT

This research is supported by National Natural Science Foundation of China (No. 11071152 & No. 11271238).

REFERENCES

[1] B. Schneier, Cryptography: Theory and Practice, CRC Press, Boca Raton, 1995.
[2] E. Alvarez, A. Fernandez, P. Garcia, J. Jimenez, A. Marcano. New approach to chaotic encryption. Physics Letters A, 263 (4-6), 1999, pp. 373-375.
[3] G. Chen, Y. Mao, C.K. Chui. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons & Fractals, 21(3), 2004, pp. 749-761.
[4] P. Li, Z. Li, W.A .Halang, G. Chen. A stream cipher based on spatiotemporal chaotic system. Chaos, Solitons & Fractals, 32(5), 2007, pp. 1867-1876.
[5] M.S. Baptista. Cryptography with chaos. Physics Letter A, 240, 1998, pp. 50-54.
[6] J. Scharinger. Fast encryption of image data using chaotic Kolmogorov flows. Journal of Electronic imaging, 7(2), 1998, pp. 318-25.
[7] H. Cheng, X.B. Li. Partial encryption of compressed images and videos. IEEE Transactions on Signal Processing, 48(8), 2000, pp. 2439-2451.
[8] J. Fridrich, Symmetric ciphers based on two-dimensional chaotic maps. International Journal of Bifurcation and chaos, 8(6), 1998, pp. 1259-1284
[9] R. Ye, Y. Ma, A Secure and Robust Image Encryption Scheme Based on Mixture of Multiple Generalized Bernoulli Shift Maps and Arnold Maps, I. J. Computer Network and Information Security, 2013,5(7), 21-33.
[10] Y.B. Mao, G. Chen, S.G. Lian. A novel fast image encryption scheme based on 3D chaotic Baker maps. Chaos, Solitons & Fractals, 14(10), 2004, pp. 613-624
[11] Cahit Cokal, Ercan Solak, Cryptanalysis of a Chaos-based image encryption algorithm, Physics Letters A, 373, 2009, pp. 1357-1360.
[12] D. Xiao, X. Liao, P. Wei, Analysis and improvement of a chaos-based image encryption algorithm, Chaos, Solitons and Fractals, 40, 2009, pp. 2191–2199.
[13] J. M. Liu, Q. Qu, Cryptanalysis of a substitution-diffusion based on cipher using chaotic standard and logistic map, Third International Symposium on Information Processing, 2010, pp. 67-69.
[14] R. Rhouma, E. Solak, S. Belghith, Cryptanalysis of a new substitution-diffusion based image cipher, Commun. Nonlinear Sci. Numer. Simulat., 15, 2010, pp. 1887–1892.

[15] X. Wang, G. He, Cryptanalysis on a novel image encryption method based on total shuffling scheme, Optics Communications, 284, 2011, pp. 5804–5807.
[16] G. J. Zhang, Q. Liu, A novel image encryption method based on total shuffling scheme, Optics Communications, 284. 2011, pp. 2775–2780.
[17] R. Ye. A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism. Optics Communications, 284, 2011, pp. 5290-5298.
[18] H. Liu, X. Wang, Color image encryption based on one-time keys and robust chaotic maps, Computers and Mathematics with Applications, 59, 2010,pp. 3320-3327.
[19] Atieh Bakhshandeh, Ziba Eslami, An authenticated image encryption scheme based on chaotic maps and memory cellular automata, Optics and Lasers in Engineering, 51, 2013, pp.665-673.
[20] V. Arnold, A. Avez, Ergodic problem in classical mechanics, Benjamin, New York, 1986.
[21] T. Xiang, X.F. Liao, C.K. Chui, An improved particle swarm optimization algorithm combined with piecewise linear chaotic map, Applied Mathematics and Computation. 190(2), 2007, pp. 1637-1645.

Ruisong Ye, born in 1968 and received the B.S. degree in Computational Mathematics in 1990 from Shanghai University of Science and Technology, Shanghai, China and the Ph. D. degree in Computational Mathematics in 1995 from Shanghai University, Shanghai, China. He is a professor at Department of Mathematics in Shantou University, Shantou, Guangdong, China since 2003. His research interest includes bifurcation theory and its numerical computation, fractal geometry and its application in computer science, chaotic dynamical system and its application in computer science, specifically the applications of fractal chaotic dynamical systems in information security, such as, digital image encryption, digital image hiding, digital image watermarking, digital image sharing.

Wenhua Guo, master degree candidate at department of mathematics in Shantou University.

How to cite this paper: Ruisong Ye, Wenhua Guo,"An Image Encryption Scheme Based on Chaotic Systems with Changeable Parameters", IJCNIS, vol.6, no.4, pp.37-45, 2014. DOI: 10.5815/ijcnis.2014.04.05

