I.J. Information Technology and Computer Science, **2014, 01, 82-92**
Published Online December 2013 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2014.01.10

An Image Encryption Scheme Based on Bit Circular Shift and Bi-directional Diffusion

Ruisong Ye
Department of Mathematics, Shantou University, Shantou, Guangdong, 515063, China
E-mail: rsye@stu.edu.cn

Shaojun Zeng
Department of Mathematics, Shantou University, Shantou, Guangdong, 515063, China
E-mail: 10sjzeng@stu.edu.cn

Peiqian Lun
Department of Mathematics, Shantou University, Shantou, Guangdong, 515063, China
E-mail: 09pqlun@stu.edu.cn

Junming Ma
Department of Mathematics, Shantou University, Shantou, Guangdong, 515063, China
E-mail: 10jmma@stu.edu.cn

Chuting Lai
Department of Mathematics, Shantou University, Shantou, Guangdong, 515063, China
E-mail: 10ctlai@stu.edu.cn

***Abstract*—** A novel image encryption scheme based on chaotic system is proposed. The proposed encryption scheme utilizes one tent map to generate a pseudo-random sequence and then shift the bits of the expanding 0-1 image circularly so as to shuffle the image gray values. To make the encryption scheme resist differential attack efficiently, generalized Arnold maps and Bernoulli shift maps are applied to produce two pseudo-random gray value sequences and then diffuse the gray values bi-directionally. The bit circular shift process and diffusion processes greatly confuse the statistical nature between plain-images and cipher-images. Security analyses including key sensitivity analysis, key space analysis, statistical analysis, differential attack analysis and information entropy analysis are performed. All the experimental results demonstrate that the proposed image encryption scheme possesses large key space to frustrate brute-force attack efficiently and can resist statistical attack, differential attack, etc.

***Index Terms*—** Chaotic System, Bit Circular Shift, Diffusion, Image Encryption

I. Introduction

With the rapid development of network and multimedia technology, a lot of personal and public information are disseminated over the network. The security issue of information consequently becomes the research focus in the information explosion era. Thanks to the inherent characteristics of image information, such as visual expression, bulk data capacity, redundancy of data, strong correlation among adjacent pixels, specific data format, as well as the characteristics of human visual system, traditional encryption algorithms, such as DES, IDEA, RSA, are thereby not suitable for practical digital image encryption applications due to the weakness of low-level efficiency while encrypting images[1]. On the other hand, the fantastic properties of chaotic systems, such as highly sensitivity to initial conditions and control parameters, ergodicity, pseudo-randomness and mixing property, are in line with the confusion and diffusion requirements for cryptography. Therefore chaotic systems are especially suitable for constructing image encryption algorithms. Chaotic maps can simulate random behavior in a quite impressive way. In particular, chaotic maps are easy to be implemented by microprocessors and personal computers. Therefore, chaotic cryptosystems generally have high speed with low cost, which makes them better candidates than many traditional ciphers for multimedia data encryption[2-6].

Chaos-based image encryption algorithms are broadly divided into three categories: pixel position scrambling based, pixel gray value scrambling-diffusion

based, and the combined ones[7-10]. Pure pixel position scrambling based schemes attract more cryptanalysis experts and many such a kind of image encryption schemes have been broken[11-13]. Image encryption schemes based on gray value scrambling- diffusion are potential and worthy of studying furthermore. This paper will design an encryption scheme based on chaotic systems with focus on the gray value scrambling and diffusion. The proposed scheme consists of two stages. In the first stage, bit circular shifts are performed for the bit information in the expanding 0-1 image randomly so as to change the image gray value, in which the random numbers are generated by the chaotic skew tent map. The skew tent map has been widely used to design chaos-based image encryption schemes successfully[14]. Bit-level permutation can change the pixel gray values while scrambling the pixel positions[15, 16]. In the second stage, the generalized Arnold map and the generalized Bernoulli shift map are employed to generate two pseudo-random sequences, which are applied to diffuse the image gray values by a bi-directional diffusion mechanism. Through two stages of encryption, one can obviously change the statistical properties of the plain-image and therefore enhance the resistance ability against the statistical attack and differential attack. Furthermore, the key streams generated in the diffusion stage not only depending on the cipher keys, but also closely related to the original plain-images. When the plain-images are different, even with the same cipher keys, the proposed image encryption scheme can also produce different key streams and thereby yield different cipher-images. Therefore the image encryption scheme shows good resistance against chosen plain-text attack, known-plaintext attack.

The remainder of this paper is outlined as follows. Section 2 proposes bit circular shift for the bit information to achieve the gray value scrambling. A diffusion function is also presented to realize gray value diffusion through one bi-directional diffusion mechanism. Section 3 analyzes the security of the proposed encryption scheme. Simulation experiments are carried out with details to demonstrate the security of the image encryption scheme, including the key sensitivity analysis, key space analysis, statistical analysis, differential attack, etc. Section 4 makes a summary.

II. The Proposed Image Encryption Scheme

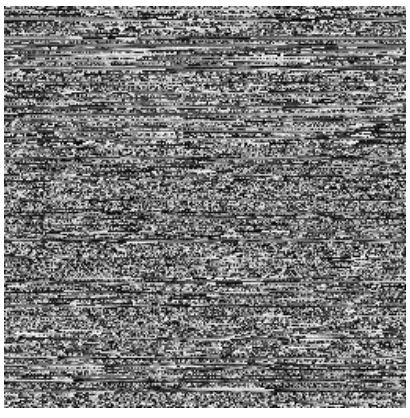
2.1 Scrambling Stage in the Expanding 0-1 Image

Expand the gray image with 256 gray levels to bit planes and 8 bit planes yields. The bit planes are all 0-1 images. Let the gray image to be G expressed by a matrix whose element $G(x, y)$ at the pixel (x, y) belongs to $\{0,1,\cdots,255\}$, therefore $G(x, y)$ can be represented by 8bits in binary

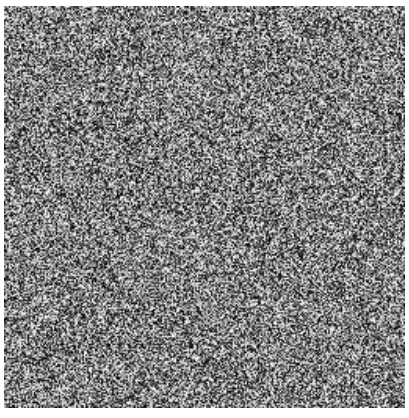
$$G(x,y)=b(7)b(6)b(5)\ldots b(0)$$

where $b(i)\in\{0,1\}, i=0,1,\ldots,7$. As a result, one gray image with size $M\times N$ and 256 gray levels can expanded to be one 0-1 image with size $M\times(8\times N)$. The plain-image Lena and its binary expanding image are shown in figures 1(a), (d).

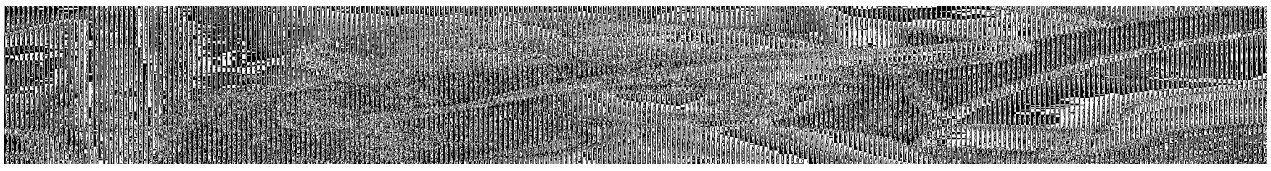
(a) Plain-image Lena



(b) Image by bit circular shift



(c) Cipher-image



(d) The expanding 0-1 image of Lena

(e) The bit circular shift expanding 0-1 image of Lena

Fig. 1: The encrypted results of Lena

The skew tent map is described by

$$x_{k+1} = T(x_k) = \begin{cases} \dfrac{x_k}{a}, & 0 < x_k \le a \\ \dfrac{1-x_k}{1-a}, & a < x_k \le 1 \end{cases}, k = 1,2,\ldots, \qquad (1)$$

where $a \in (0,1)$ is the control parameter, $x_k, x_{k+1} \in [0,1]$ are the states. It is a noninvertible transformation of the unit interval onto itself. As $a = 0.5$, T becomes the regular tent map. The transformation is continuous and piecewise linear, with the linear regions $[0,a]$ and $[a,1]$. Note that the slope of the left branch is $1/a > 1$ and the slope of the right branch is $-1/(1-a) < -1$. A typical orbit of $x_0 = 0.49$ derived from the dynamical system is $\{x_k = T^k(x_0), k = 0,1,\cdots\}$, which is shown in figure 2(a), for $a = 0.45$. Its waveform is quite irregular and indicates that the system is chaotic. For any $a \in (0,1)$, the piecewise linear map (1) has a Lyapunov exponent $-a\ln a - (1-a)\ln(1-a)$, which is larger than 0, also implying that the map is chaotic. So the control parameter a and the initial condition x_0 can be regarded as cipher keys. There exist some good dynamical features in the skew tent map. It has been verified that the density $\rho(x)$ of the skew tent map is the same as the regular tent map[17], that is

$$\rho(x) = \begin{cases} 1, & \text{if } x \in (0,1), \\ 0, & \text{otherwise.} \end{cases}$$

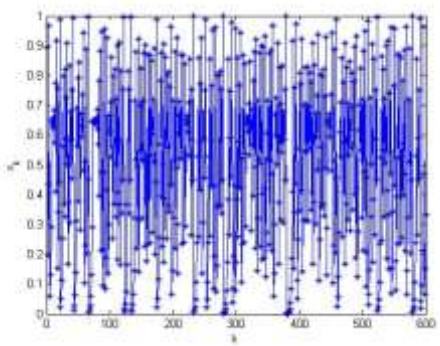


Fig. 2: (a) A typical orbit of skew tent map

The distribution of the points $\{x_k : k = 0,1,\cdots,6000\}$ of a typical orbit of length 6000 is represented by the histogram of figure 2(b). It can be seen that the points of the orbit spread more or less evenly over the unit interval in the course of time. Skew tent map also possesses desirable auto-correlation and cross-correlation features. The iterated trajectories are used to calculate the correlation coefficients, which are shown in figures 2(c)-(d) respectively.

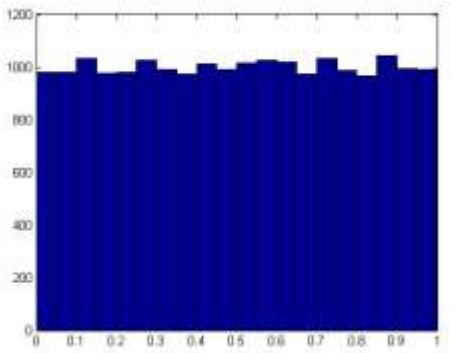


Fig. 2: (b) Histogram of a typical orbit of length 6000

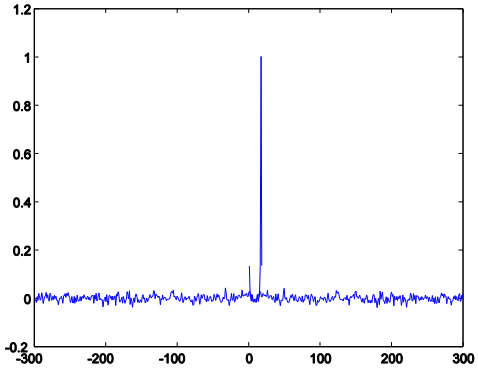
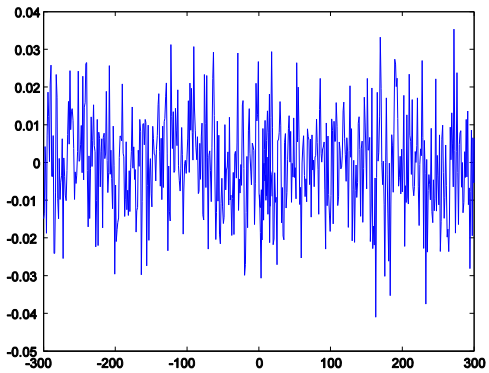


Fig. 2: (c) Auto-correlation



(d) Cross-correlation

Fig. 2: The chaotic nature of skew tent map

The chaotic orbit $\{x_k\}$ can be quantized to generate one new pseudo-random integer sequence, which can be utilized to change the gray values of the plain-image. The bits in the expanding 0-1 image figure 1(d) are shifted circularly to scramble the image gray values. The bits in the kth row of the expanding 0-1 images are all shifted right by l_k bits circularly and thereby change the gray values of the plain-image. Set x_0 =0.49, a =0.45, we get the bit circular shift expanding 0-1 image of Lena shown as figure 1(e), and then construct it to be one gray image with 256 gray levels, shown as figure 1(b). The detailed bit circular shift scrambling process is outlined as follows.

Step 1. Set the initial values of x_0 and the control parameter a .

Step 2. Iterate system (1) by N_0 times, discard the beginning N_0 transitional points to avoid the harmful effect, and make the subsequent sequence more chaotic.

Step 3. Iterate (1) by M times to get one chaotic sequence, denoted by $X=\{x_{N_0+1}, x_{N_0+2}, \cdots, x_{N_0+M}\}$. For the sake of simplicity, we also denote it by $X=\{x_1, x_2, \cdots, x_M\}$.

Step 4. Quantize $X=\{x_1, x_2, \cdots, x_M\}$ to get the shift numbers

$$\{ l_k,\ l_k = (x_k \times 10^8) \bmod (8N) \},\ k=1,2,\ldots,M .$$

The bits in the kth row of the expanding 0-1 bit image are shifted right simultaneous by l_k bits circularly. The final scrambled 0-1 image sized $M\times(8\times N)$ is yielded, which is shown in figure 1(e). The final gray image G1 is shown in figure 1(b) .

2.2 Diffusion Stage of Gray Values

It is well-known that diffusion process can strengthen the resistance to statistical attack and differential attack efficiently. The histogram of the cipher-image encrypted by an efficient diffusion process is fairly uniform and significantly different from that of the plain-image. The opponent can't find any useful clues between the plain-image and the cipher-image and so can't break the cryptosystem even after they spend a lot of time and effort. A good diffusion process should also produce key streams strongly related to plain-images. The key streams generated in the diffusion stage not only depending on the cipher keys, but also closely related to the original plain-images. As plain-images are different, even with the same key, the proposed image encryption scheme can also produce different key streams. Therefore the encryption scheme shows good resistance against chosen plain-text attack, known-plaintext attack. The diffusion process is outlined as follows.

Step 1. Apply the bit circular shift scrambling process in Subsection 2.1 to achieve the gray value scrambling of plain-image and get the scrambled gray image $G1$. Set the initial values of y_0, z_0, w_0 and the control parameters $b, c.d$. For example, we set

$$b=1.16, c=5.93, d=0.3638,$$

$$(y_0, z_0)=(0.6191, 0.2617),\ w_0=0.43 .$$

Step 2. Let $i=0$.

Step 3. Apply the following quantization formula to yield two 8-bit pseudo-random gray value sequences $d_1(i), d_2(i)$:

$$d_1(i)=\text{floor}(L\times y_i),\ d_2(i)=\text{floor}(L\times z_i),$$

where L is the color level (for a 256 grey-scale image, $L=256$), the "floor" operation on x returns the largest value not greater than x .

Step 4. Compute the pixel gray value in the cipher-image by

$$C(2i+1)=\phi(2i+1)\oplus[(d_1(i)+C(2i))\bmod 256];$$
$$C(2i+2)=\phi(2i+2)\oplus[(d_2(i)+C(2i+1))\bmod 256],$$

where $\phi(2i+1), \phi(2i+2)$ are the gray values of the current operated pixel in the shuffled image which has been rearranged according to the order of row or column to a vector with length $M\times N$, $C(2i)$ is the previous output cipher-pixel gray value. The diffusion process is well defined as the initial condition $C(0)$ is provided. $C(0)$ can be set to be part of the cipher keys in the diffusion process or can just take the value of $d_1(0)$ for simplicity.

Step 5. Compute s by $s=1+[C(2i+1)\bmod 3]$ to get the next (y_{i+1}, z_{i+1}) by iterating the generalized Arnold map with control parameters a, b on (y_i, z_i) for s rounds

$$\begin{pmatrix} y_{i+1} \\ z_{i+1} \end{pmatrix} = \begin{pmatrix} 1 & b \\ c & 1+bc \end{pmatrix}^s \begin{pmatrix} y_i \\ z_i \end{pmatrix} \bmod 1.$$

This is the crucial step to generate key streams depending on the plain-image since s is related to $C(2i+1)$, so are y_{i+1}, z_{i+1} . The encrypted image not only relates to the cipher keys, but also relates to the plain-image.

Step 6. Let $i = i+1$ and return to Step 3 until i reaches $M \times N / 2$.

The above diffusion process implies that it can't influence the pixels before the tampered pixel with a gray value change. As a remedy, we here add a reverse diffusion process as a supplement to the above diffusion process. The chaotic map used here is the generalized Bernoulli shift map.

Step 7. Iterate the following generalized Bernoulli shift map to produce another pseudo-random gray value sequence

$$w_{k+1} = (w_k / d) \bmod 1,$$

$$\psi(k+1) = \text{floor}(L \times w_{k+1}), k = 0,1,..., M \times N - 1.$$

Step 8. Execute the reverse diffusion process:

$$D(i) = D(i+1) \oplus [(C(i) + \psi(i)) \bmod L], i = M \times N, ..., 2, 1,$$

where $D(i), i = 1, 2, ..., M \times N$ are the final encrypted vector consisting of the encrypted image pixel gray-scale values. The value of $D(M \times N + 1)$ should be provided to cipher out the sequence $D(i), i = 1, 2, \cdots,$ $M \times N$. $D(M \times N + 1)$ can be handled in the same manner as $C(0)$.

The complete diffusion process is composed of Step 1 to Step 8. The circular shift scrambling process and the diffusion process form the proposed image encryption scheme. The original image Lena is encrypted and the resulted cipher image is shown in figure 1 (c).

III. Security Analysis

According to the basic principle of cryptology [1], an ideal encryption cryptosystem requires sensitivity to cipher keys, i.e., the cipher-text should have close correlation with the keys. Furthermore, an ideal encryption scheme should have a large key space to make brute-force attack infeasible; it should also well resist various kinds of attacks like statistical attack, differential attack, etc. Some security analysis will be performed on the proposed image encryption scheme, including the most important ones like key sensitivity test, key space analysis, statistical analysis, and differential attack analysis. All the analysis shows that the proposed image encryption scheme is highly secure thanks to its high sensitivity of the control parameters and initial conditions of the considered chaotic systems, large key space, and satisfactory diffusion mechanism.

3.1 Key Sensitivity and Key Space Analysis

The high sensitivity of the cipher-image to initial conditions and control parameters is inherent to any chaotic system. A good image encryption scheme needs to contain sufficiently large key space for compensating the degradation dynamics in PC. It should be sensitive to cipher keys as well, and thus can effectively prevent invaders decrypting original data even after they invest large amounts of time and resources. The analysis results regarding the sensitivity and the key space are summarized as follows. Since the permutation process is irrelevant to the diffusion process, the key space consists of the cipher keys in both the circular shift scrambling process and the diffusion process.

In the bit circular shift scrambling process, the initial value of $x_0 \in (0,1)$ and the control parameter $a \in (0,1.0)$ form the cipher keys. The cipher keys in the diffusion process consist of the initial values of y_0, z_0, w_0 and the control parameters b, c, d. The sensitivity tests with respect to all cipher keys have been carried out. To verify the sensitivity of cipher key K, the original plain-image $I = (I(i, j))_{M \times N}$ is encrypted with $K = p$, $K = p - \Delta K$ and $K = p + \Delta K$ respectively while keeping the other key parameters unchanged. Here ΔK is the perturbing value. The corresponding encrypted images are denoted by I_1, I_2, I_3 respectively. The sensitivity coefficient to the cipher key K is then denoted by the following formula

$$P_s(K) = \frac{1}{2 \times H \times W} \sum_{i,j} [N_s(I_1(i, j), I_2(i, j)) + N_s(I_1(i, j), I_3(i, j))] \times 100\%$$

where

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

$P_s(K)$ implies the sensitivity to the perturbation of parameter K. Larger $P_s(K)$ implies more sensitive for cipher key K. Table 1 shows the results of the sensitivity test where the initial key values are set to be

$x_0 = 0.49,\ a = 0.45,$

$y_0 = 0.6191,\ z_0 = 0.2617,\ w_0 = 0.43,$

$b = 1.16,\ c = 5.93, d = 0.3638.$

The variations ΔK for all the considered keys are set to be 10^{-16} except for a_2, b_2 whose variations ΔK are both set to be 10^{-15}. We apply the proposed image encryption scheme one round with only perturbing one cipher key K with the corresponding variation value while fixing other parameters. The results in table 1 imply that the control parameters and the initial values are all strongly sensitive. It also implies from the results that the key space is more than 10^{126}, which is large enough to make brute-force attack infeasible.

Table 1: Results regarding the sensitivity to cipher keys

Key	a	x_0	y_0	z_0
$P_s(K)$	99.62	99.61	99.61	99.63
Key	w_0	b	c	d
$P_s(K)$	99.61	99.65	99.60	99.64

The sensitivity tests can also be demonstrated visually from two aspects. One is to show that the cipher-image is strongly sensitive to the cipher key. If the cipher-key is replaced with a minor change, the cipher-image will become almost completely different visually. The other one can be shown by the decrypted image. Minor perturbation for cipher key will result in tremendous change in the decrypted image and one can't find any hints for the plain-image.

(i) Influence of minor change for cipher keys over encryption. We perform three simulations. The plain-image Lena is encrypted by the cipher keys x_0 =0.49, a =0.45, y_0=0.6191 , z_0=0.2617 , w_0=0.43 , b=1.16 , $c = 5.93, d = 0.3638$, the cipher-image is shown in figure 1(c). Replace y_0 , a , b by y_0=0.6191+10^{-16} , a = 0.45+10^{-16} , b=1.16+10^{-15} respectively, and keep the other cipher keys unchanged, the cipher-images are shown in figures 3(a)-(c) respectively. The difference images are figures 3(d)-(f).

(ii) Influence of minor change for cipher keys over decryption. Replace y_0 by y_0=0.6191+10^{-16} and keep the other cipher keys unchanged, the decrypted image is shown in figure 4(a), which has a difference 99.53% from the plain-image Lena. Replace a by a=0.45+10^{-16} and keep the other cipher keys unchanged, the decrypted image is shown in figure 4(b), which has a difference 99.16% from Lena. If b is changed to be b=1.16+10^{-15}, the decrypted image is shown in figure 4(c) with a difference 99.59% from Lena.

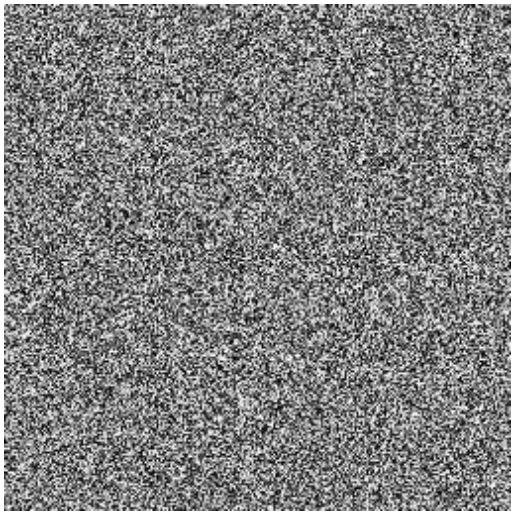


Fig. 3: (a) Cipher-image by y_0=0.6191+10^{-16}

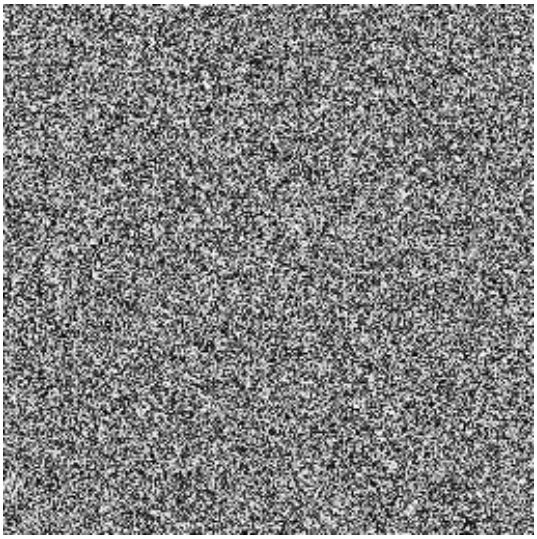


Fig. 3: (b) Cipher-image by a = 0.45+10^{-16}

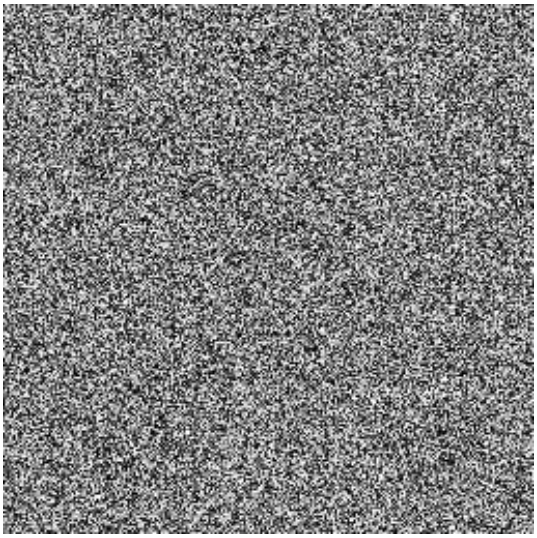


Fig. 3: (c) Cipher-image by b=1.16+10^{-15}

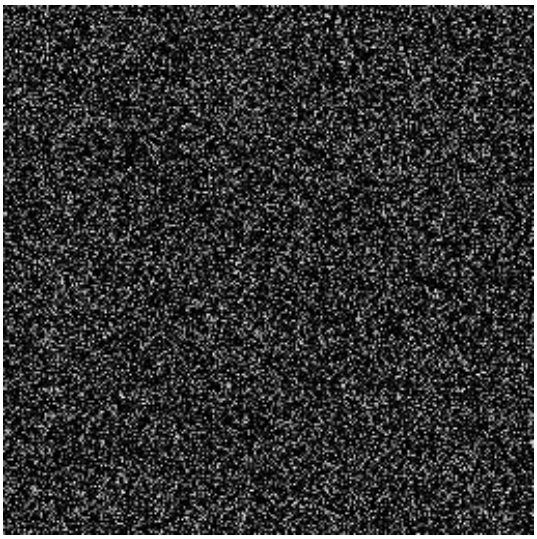


Fig. 3: (d) Difference image between Fig.3 (a) and Fig. 1(c)

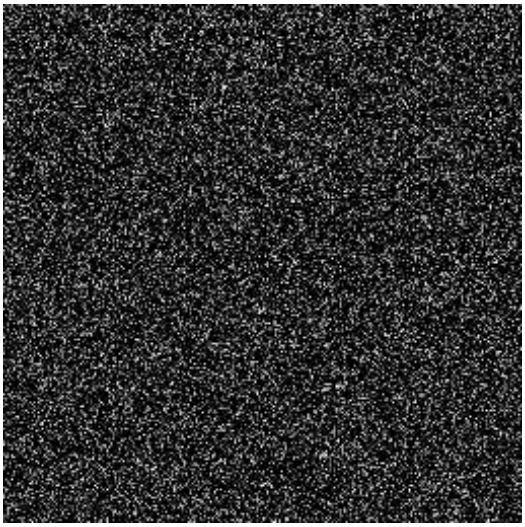


Fig. 3: (e) Difference image between Fig.3 (b) and Fig.1(c)

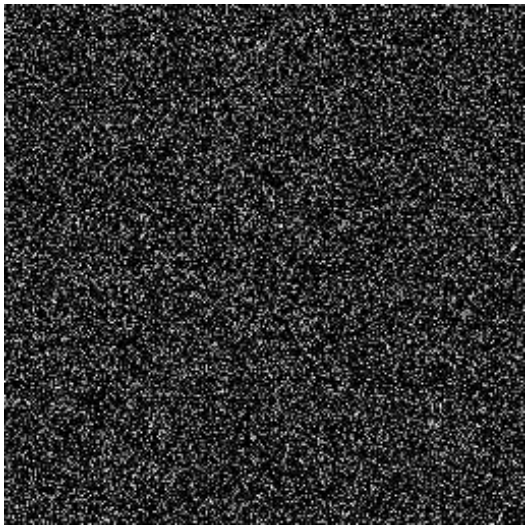


Fig. 3: (f) Difference image between Fig.3 (c) and Fig. 1(c)

Fig. 3: Key sensitivity test I

3.2 Statistical Analysis

Shannon pointed out in his masterpiece[18] the possibility to solve many kinds of ciphers by statistical analysis. Therefore, passing the statistical analysis on cipher-image is of crucial importance for a cryptosystem. Indeed, an ideal cryptosystem should be robust against any statistical attack. In order to prove the security of the proposed encryption scheme, the following statistical tests are performed.

(i) Histogram. Encrypt the plain-image Lena one round, and then plot the histograms of plain-image and cipher-image as shown in figures 5(a)-(b), respectively. figure 5(b) shows that the histogram of the cipher-image is fairly uniform and significantly different from the histogram of the original plain-image and hence it does not provide any useful information for the opponents to perform any statistical analysis attack on the encrypted image.

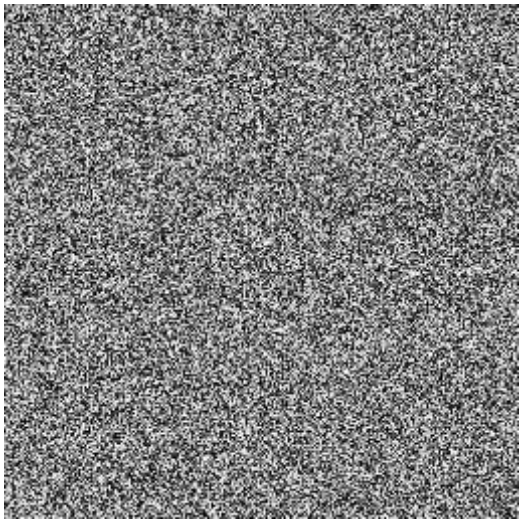


Fig. 4: (a) Decrypted image by y_0=0.6191+10^{-16}

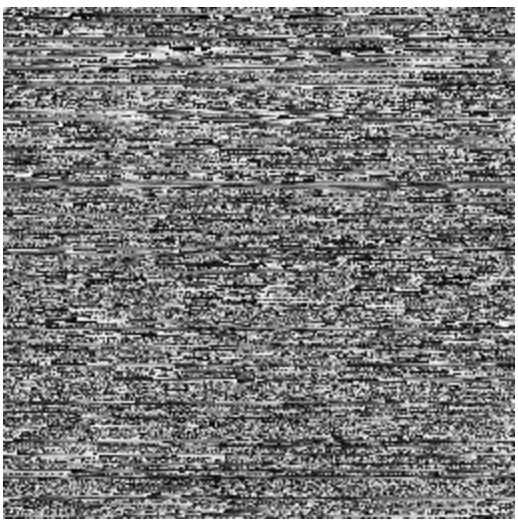


Fig. 4: (b) Decrypted image by a=0.45+10^{-16}

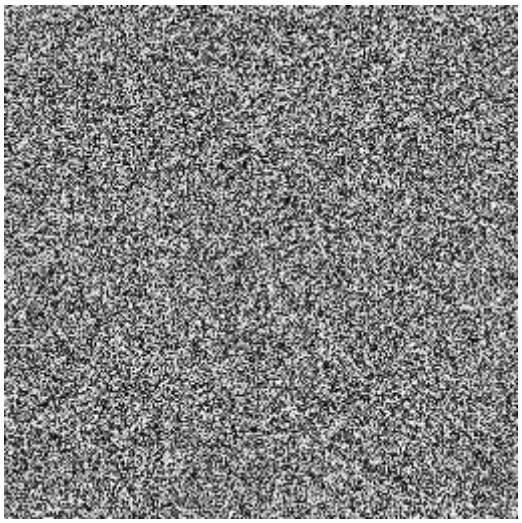


Fig. 4: (c) Decrypted image by b=1.16+10^{-15}

Fig. 4: Key sensitivity test II

(ii) Correlation of adjacent pixels. To test the correlation between two adjacent pixels, the following performances are carried out. First, we select 3000 pairs of two adjacent pixels randomly from coefficient of the selected pairs using the following formulae:

$$Cr = \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)D(y)}},$$

$$\operatorname{cov}(x,y) = \frac{1}{T}\sum_{i=1}^{T}\left(x_i - E(x)\right)\left(y_i - E(y)\right),$$

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

where x, y are the gray-scale values of two adjacent pixels in the image and T is the total pairs of pixels randomly selected from the image. The correlations of two adjacent pixels in the plain-image and in the cipher-image are shown in table 2. The correlation distribution of two adjacent pixels in the plain-image and that in the cipher-image are shown in figure 6.

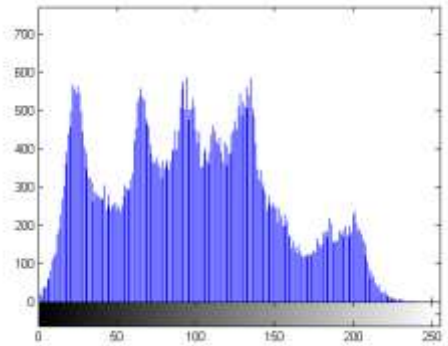


Fig. 5: (a) The histogram of plain-image

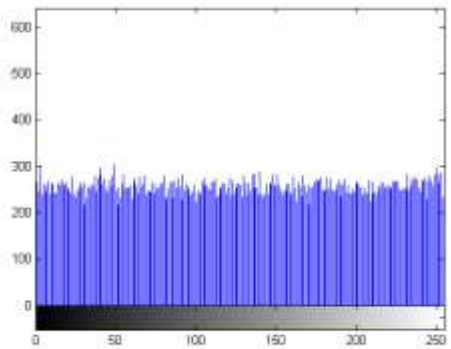


Fig. 5: (b) The histogram of cipher-image

Fig. 5: The histograms of plain-image and cipher-image

(iii) Information entropy analysis. The entropy is the most outstanding feature of randomness. Therefore, it is generally used to measure the strength of the cryptosystem. The entropy $H(m)$ of a message source can be measured by

$$H(m) = -\sum_{i=0}^{L-1} p(m_i)\log\left(p(m_i)\right)$$

where L is the total number of symbols m, $p(m_i)$ represents the probability of occurrence of symbol m_i and log denotes the base 2 logarithm so that the entropy is expressed in bits. Considering a random source with 256 outcomes, sharing equal probability, its entropy is equal to 8. Under the proposed cryptosystem, the entropy of encrypted image of Lena is 7.9974 bits while the entropy of plain-image Lena is 7.3507. According to this result, the cipher-image is close to a random source and the proposed algorithm is secure against the entropy attack.

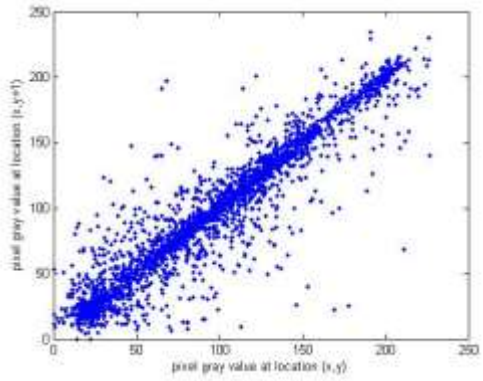


Fig. 6: (a)

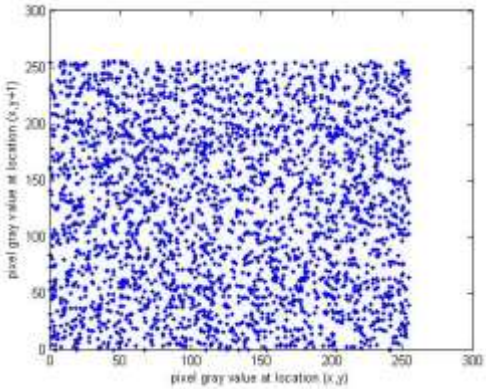


Fig. 6: (b)

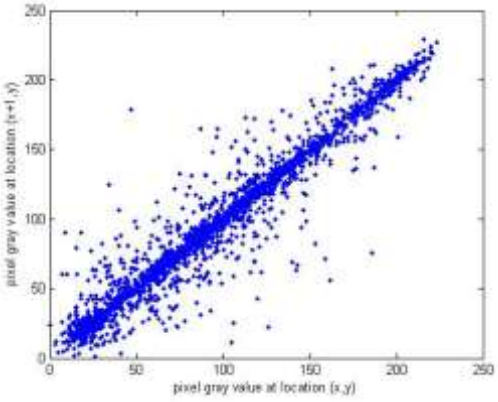


Fig. 6: (c)

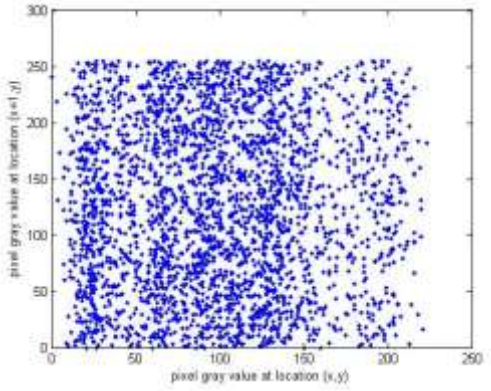


Fig. 6: (d)

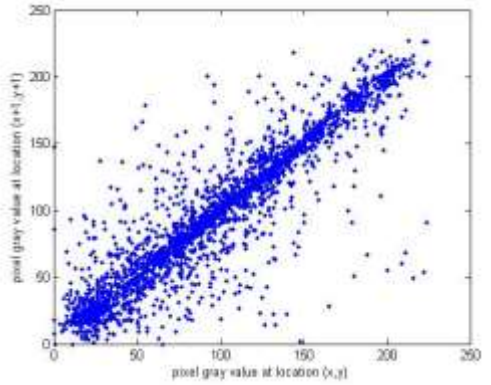


Fig. 6: (e)

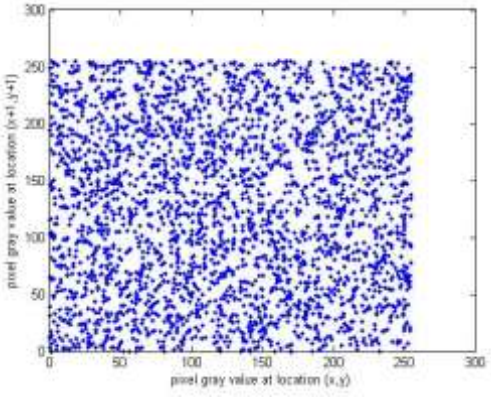


Fig. 6: (f)

Fig. 6: **C**orrelations of two adjacent pixels in the plain-image and in the cipher-image: (a), (c), (e) are for the plain-image; (b),(d),(f) are for the cipher-image

3.3 Differential Attack

In general, attackers may make a slight change (e.g., modify only one pixel) of the plain-image to find out some meaningful relationships between the plain-image and the cipher-image. If one minor change in the plain-image will cause a significant change in the cipher-image, then the encryption scheme will resist the differential attack efficiently. To test the influence of only one-pixel changed in the plain-image over the whole cipher-image, two common measures, namely number of pixels change rate (NPCR) and unified average changing intensity (UACI), are evaluated by (2) and (3) respectively.

$$\mathrm{NPCR}(C_1, C_2) = \frac{1}{M \times N} \sum_{i,j} D(i, j) \times 100\%, \tag{2}$$

$$\mathrm{UACI}(C_1, C_2) = \frac{100}{M \times N \times 255} \sum_{i,j} \left| C_1(i, j) - C_2(i, j) \right|, \tag{3}$$

NPCR measures the percentage of different pixels numbers between the two cipher-images whose plain-images only have one-pixel difference; UACI measures the average intensity of differences between the two cipher-images. They indicate the sensitivity of the cipher-images to the minor change of plain-image. To resist difference attacks, the values of NPCR and UACI should be large enough. We randomly select 10 pixels and change the gray values with a difference of 1, for example, we replace the gray value 137 of the pixel at position (164,200) by 138, and get NPCR=99.83%, UACI=43.32%. The numerical results are shown in table 3. The mean values of the ten NPCR and UACI values are 99.83% and 37.79% respectively. We observe from table 3 that the two measure values are exceptionally good undergoing only one round of encryption.

Table 2: Correlation coefficients of two adjacent pixels

	plain-image	**cipher-image**
horizontal	0.9435	-0.0069
vertical	0.9696	0.0347
diagonal	0.9194	0.0200

Table 3: Results of NPCR and UACI tests of Lena

Position	**(164,200)**	**(186,7)**	**(232,180)**	**(24,133)**	**(18,83)**
NPCR(%)	99.83	99.75	99.67	99.94	99.93
UACI(%)	43.32	27.01	37.10	15.98	47.10
Position	**(123,48)**	**(10,236)**	**(98,210)**	**(250,100)**	**(198,120)**
NPCR(%)	99.92	99.96	99.78	99.65	99.85
UACI(%)	46.40	49.14	41.63	32.42	28.55

IV. Conclusion

An efficient image encryption scheme based on chaotic systems and gray value scrambling-diffusion is proposed in the paper. The proposed encryption scheme utilizes one tent map to generate a pseudo-random sequence and then shift the bits of the expanding 0-1 image circularly so as to achieve the shuffling effect of gray values. Generalized Arnold maps and Bernoulli shift maps are also applied to produce two pseudo-random gray value sequences and then diffuse the gray values bi-directionally in the diffusion stage. Security analyses including key sensitivity analysis, key space analysis, statistical analysis, differential analysis and information entropy analysis are performed. All the experimental results demonstrate that the proposed image encryption scheme possesses large key space to frustrate brute-force attack efficiently and can resist statistical attack, differential attack, etc.

Acknowledgement

This research is supported by Innovation and Entrepreneurship Training Program of Guangdong Colleges.

References

[1] B. Schneier. Cryptography: Theory and Practice. Boca Raton: CRC Press, 1995.

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

[3] G. R. Chen, Y. B. Mao, C. K. Chui. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons and Fractals, 21(2004), 749--761.

[4] Y.B. Mao, G. Chen, S. G. Lian. A novel fast image encryption scheme based on the 3D chaotic Baker map. International Journal of Bifurcation and Chaos, 14(2004), 613--3624.

[5] Z.-H. Guan, F. Huang, W. Guan, Chaos-based image encryption algorithm, Physics Letters A, 346 (2005), 153--157.

[6] S. Lian, J. Sun, Z. Wang, A block cipher based on a suitable use of the chaotic standard map, Chaos, Solitons and Fractals, 26 (2005), 117--129.

[7] V. Patidar, N. K. Pareek, K. K. Sud, A new substitution–diffusion based image cipher using chaotic standard and logistic maps, Commun. Nonlinear Sci. Numer. Simulat., 14 (2009) 3056--3075.

[8] R. Ye, H. Huang, Application of the Chaotic Ergodicity of Standard Map in Image Encryption and Watermarking, I. J. Image, Graphics and Signal Processing, 1(2010), 19--29.

[9] X. Wang, X. Wang, J. Zhao, Z. Zhang, Chaotic encryption algorithm based on alternant of stream cipher and block cipher, Nonlinear Dynamics, 63(2011), 587--597.

[10] R. Ye. A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism. Opt. Commun., 284(2011), 5290--5298.

[11] G. Chen, W. A. Halang. Cryptanalysis of an image encryption scheme based on a compound chaotic sequence. Image and Vision Computing, 27(2009), 1035--1039.

[12] D. Xiao, X. Liao, P. Wei. Analysis and improvement of a chaos-based image encryption algorithm. Chaos, Solitons and Fractals, 2009, 40: 2191--2199.

[13] X. Wang, G. He. Cryptanalysis on a novel image encryption method based on total shuffling scheme. Opt. Commun.,284(2011), 5804--5807

[14] G. J. Zhang, Q. Liu. A novel image encryption method based on total shuffling scheme. Opt. Commun., 284(2011), 2775--2780.

[15] Z.-L. Zhu, W. Zhang, K.-W. Wong, H. Yu, A chaos-based symmetric image encryption scheme using a bit-level permutation, Information Sciences, 181(2011), 1171--1186.

[16] L. Teng, X. Wang, A bit-level image encryption algorithm based on spatiotemporal chaotic system and self-adaptive, Opt. Commun., 285(2012), 4048--4054.

[17] M. Hasler and Y. L. Maistrenko, An introduction to the synchronization of chaotic systems: Coupled skew tent map, IEEE Transactions on Circuits and Systems, 44(1997), 856--866.

[18] C. E. Shannon. Communication theory of secrecy system. Bell Syst. Tech. J, 28(1949), 656--715.

Authors' Profiles

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.

Shaojun Zeng: Undergraduate student at department of mathematics in Shantou University.

Peiqian Lung: Undergraduate student at department of mathematics in Shantou University.

Junming Ma: Undergraduate student at department of mathematics in Shantou University.

Chuting Lai: Undergraduate student at department of mathematics in Shantou University.

How to cite this paper: Ruisong Ye, Shaojun Zeng, Peiqian Lun, Junming Ma, Chuting Lai,"An Image Encryption Scheme Based on Bit Circular Shift and Bi-directional Diffusion", International Journal of Information Technology and Computer Science(IJITCS), vol.6, no.1, pp.82-92, 2014. DOI: 10.5815/ijitcs.2014.01.10

