

# A Chaos-based Pseudorandom Permutation and Bilateral Diffusion Scheme for Image Encryption

Weichuang Guo, Junqin Zhao and Ruisong Ye\*

Department of Mathematics, Shantou University, Shantou, Guangdong, 515063, P. R. China

\*Corresponding author, e-mail: rsye@stu.edu.cn

**Abstract**—A great many chaos-based image encryption schemes have been proposed in the past decades. Most of them use the permutation-diffusion architecture in pixel level, which has been proved insecure enough as they are not dependent on plain-images and so cannot resist chosen/known plain-image attack usually. In this paper, we propose a novel image encryption scheme comprising of one permutation process and one diffusion process. In the permutation process, the image sized  $M \times N$  is expanded to one sized  $M \times 2N$  by dividing the plain-image into two parts: one consisting of the higher 4bits and one consisting of the lower 4bits. The permutation operations are done row-by-row and column-by-column to increase the speed of permutation process. The chaotic cat map is utilized to generate chaotic sequences, which are quantized to shuffle the expanded image. The chaotic sequence for permutation process is dependent on plain-image and cipher keys, resulting in good key sensitivity and plain-image sensitivity. To achieve more avalanche effect and larger key space, a chaotic Bernoulli shift map based bilateral (i.e., horizontal and vertical) diffusion function is applied as well. The security and performance of the proposed image encryption have been analyzed, including histograms, correlation coefficients, information entropy, key sensitivity analysis, key space analysis, differential analysis, encryption rate analysis etc. All the experimental results suggest that the proposed image encryption scheme is robust and secure and can be used for secure image and video communication applications.

**Index Terms**—Chaos, cat map, Bernoulli shift map, image encryption, permutation-diffusion architecture.

## I. INTRODUCTION

Thanks to the rapid growth of computer networks and the fast development in digital multimedia processing, more and more digital multimedia applications have covered most sectors of the society, such as education, communication, military, medical-care, etc. Especially, digital images are transmitted and shared in open networks due to their easy-understanding and attractive presentation natures. Digital information has become an indispensable resource and has changed people's life totally. Some image information resources may contain valuable and highly sensitive message related to

government public security or personal commercial interests. Therefore protection of digital image information against illegal copying and distribution has become extremely urgent. Encryption is a directly classical and efficient way to protect the digital information from unauthorized eavesdropping. In 1949, Shannon explained the encryption issue in his masterpiece [1], implying that the modern cryptology has been built. Since then, DES, IDEA, AES etc. were developed and became the typical data encryption standards [2]. However it has been shown that these ciphers are unfit for digital image information due to their special characteristics such as bulk data, high correlation among pixels, visual characteristics, etc [3].

Chaotic systems have many fantastic natures, such as ergodicity, good sensitivity to control parameters and initial values, pseudo-randomness, orbit inscrutability, which are in accordance with the fundamental requirements of cryptography. Therefore chaotic systems are suitable for constructing image encryption algorithms and chaos-based cryptosystems have attracted many researchers' attention. As a matter of fact, 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. In 1998, Fridrich firstly proposed one permutation-diffusion architecture based on different chaotic systems [3]. The proposed architecture is composed of two processes generally: chaotic confusion of pixel positions by permutation process and diffusion of pixel gray values by diffusion process, where the former permutes the plain-image pixel positions governed by a 2D chaotic map, while the latter changes the pixel gray values sequentially controlled by a 1D chaotic map, so that a tiny change for one pixel can spread out to almost all pixels in the whole image. The Fridrich architecture has become the most popular structure adopted in a great number of chaos-based image encryption algorithms subsequently proposed [4-8]. The existing chaos-based cryptosystems can be classified into two categories usually. The basic permutation units are pixel-level and bit-level for the first and second category respectively. So far, most of the cryptosystems fall into the first category. For example, Patidar et al. [7] proposed a secure and robust chaos-based pseudorandom permutation substitution scheme to

encrypt color image. The proposed scheme contains three processes: preliminary permutation, substitution and main permutation. It demonstrates strong robustness and great security. All the three processes are done row-by-row and column-by-column instead of pixel-by-pixel to improve the speed of encryption. To yield excellent key sensitivity and plaintext sensitivity, both preliminary permutation and main permutation are designed to be dependent on the plain-image and controlled through the pseudo random number sequences (PRNS) generated from the chaotic standard map. The substitution process is initialized with the initial vectors generated via the cipher keys and chaotic standard map, and then the pixel gray values of row and column pixels of input 2D matrix are bitwise exclusive OR with the PRNS generated from the standard map. Ye and Guo [8] employed chaotic multimodal skew tent maps to design a chaos-based image encryption scheme with an efficient permutation-diffusion mechanism, in which permutation of the positions of image pixels incorporates with changing the gray values of image pixels by a two-way diffusion process to confuse the relationship between cipher-image and plain-image. All pixel-level ciphers suffer from a problem that the modifications to pixel gray values are all or almost dependent on the diffusion operations. However, diffusion operations usually consume more execution time than the confusion operations [9]. As for the second category, each pixel is divided into 8 bits for 256 gray-scale images. Since each bit of a pixel contains different percentage of the pixel information, the situation of performing confusion at bit-level is quite different from pixel-level case. The bit-level permutation not only relocates the pixel positions, but also alters the pixel gray values [10, 11]. Therefore certain diffusion effect has been introduced in the confusion stage with a bit-level permutation. Thanks to the superior characteristics of bit-level operations and the intrinsic bit features of images, Zhang et al. proposed a novel image encryption scheme using lightweight bit-level confusion and cascade cross circular diffusion in [12]. They also applied an expand-and-shrink strategy at bit-level to shuffle the image with reconstructed permuting plane [13]. All the proposed image encryption schemes show good performances compared with the traditional permutation-diffusion structure operating at pixel-level. However, there exists one flaw in all bit-level based image encryption schemes. Although the bit-level confusion operations can change the pixel gray values, they consume much execution time to get the eight bit planes.

A good permutation process should show good shuffling effect and a good diffusion process should cause great modification over the cipher-image even if only a minor change for one pixel in the plain-image. However it has been pointed out that the proposed permutation-diffusion architecture with fixed parameters has one fatal flaw in [14], that is, the two processes will become independent if the plain-image is a homogeneous one with identical pixel gray value. Therefore, such a kind of encryption algorithms can be attacked by the following steps: (1) a homogeneous image is adopted to

eliminate the confusion effect; (2) the keystream of the diffusion process is obtained via known-plaintext or chosen plaintext attacks; (3) the remaining cipher-image can be regarded as the output of a kind of permutation-only cipher, which has been shown insecure and can be cryptanalyzed by known-plaintext or chosen plaintext attacks [15, 16]. As a matter of fact, many existing chaos-based image encryption schemes with the permutation-diffusion architecture have been cryptanalyzed and have been found to be insecure due to the keystreams are nothing with the plain-images [17-21]. As a result, attackers can apply chosen/known plaintext attacks to break the ciphers easily. An ideal permutation-diffusion architecture should rely on the plain-images to be encrypted and thereby owns the one-time key effect.

In this paper, a robust and secure chaos-based image encryption scheme is proposed. The proposed image encryption scheme comprises of one permutation process and one diffusion process. To overcome the drawback of consuming much execution time to get the eight bit planes, we adopt a strategy to get the tradeoff between the workload and the security, that is, 4bits derived from the pixel gray value is regarded as one unit. In the permutation process, the image sized  $M \times N$  is expanded to one of size  $M \times 2N$  by dividing the plain-image into two parts: one consisting of the higher 4bits and one consisting of the lower 4bits. To improve the speed of permutation process, another confusion operation is applied, that is, the permutation operations are done row-by-row and column-by-column instead of pixel-by-pixel or bit-by-bit. The chaotic cat map is utilized to generate chaotic sequences, which are quantized to shuffle the expanded image. The chaotic sequence for permutation process is designed to be not only dependent on cipher keys, but also dependent on plain-images, resulting in good key sensitivity and plain-image sensitivity. To achieve more avalanche effect and larger key space, a chaotic Bernoulli shift map based bilateral (i.e., horizontal and vertical) diffusion function is applied as well. The security and performance of the proposed image encryption scheme have been analyzed, including histograms, correlation coefficients, information entropy, key sensitivity analysis, key space analysis, differential analysis, encryption rate analysis etc. All the experimental results suggest that the proposed image encryption scheme is robust and secure and can be used for secure image and video communication applications.

The rest of the paper is organized as follows. In Section II, we first briefly introduce the 2D chaotic cat map and discuss its chaotic natures. Then we devote to designing the image encryption scheme. One permutation process and one bilateral diffusion process are presented to encrypt plain-images. In Section III, we present the results of security and performance analysis of the proposed image encryption scheme using histograms, correlation coefficients, information entropy, key sensitivity analysis, differential analysis, key space analysis, encryption rate analysis, etc. Section IV draws some conclusions for the paper.

II. THE PROPOSED SCHEME

A. Chaotic cat map

Chaotic cat map is also called Arnold cat map. It is a two-dimensional invertible chaotic map introduced by Arnold and Avez [22]. The classical cat map is described by

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \text{ mod } 1 \quad (1)$$

where “ $x \text{ mod } 1$ ” means the fractional part of a real number  $x$  by adding or subtracting an appropriate integer such that its result belongs to  $[0,1)$ . 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 stretched by the linear transform matrix and then folded back to the unit square by the modulo operation.

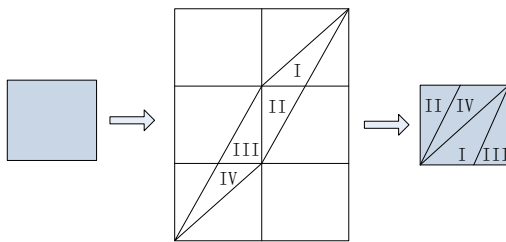
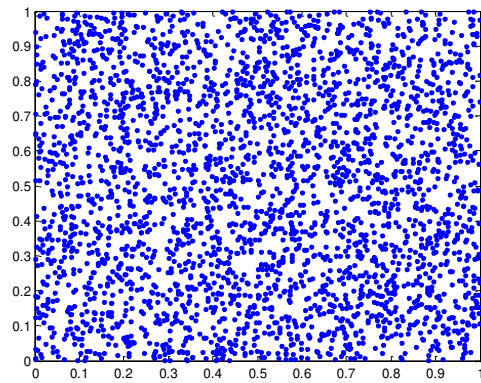


Fig.1 The chaotic cat map

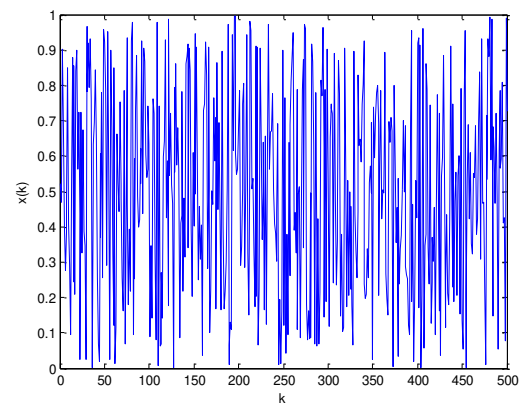
The above 2D cat map (1) can be generalized to the following form by introducing two real control parameters  $p > 0$  and  $q > 0$  [8]

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & p \\ q & 1 + pq \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \text{ mod } 1. \quad (2)$$

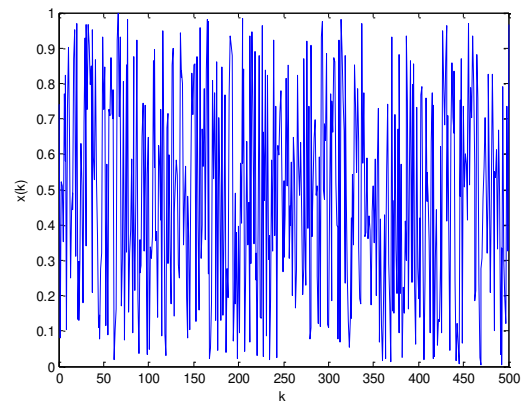
The generalized cat map (2) has one Lyapunov characteristic exponent  $\sigma_1 = 1 + \frac{1 + pq + \sqrt{p^2 q^2 + 4pq}}{2}$  larger than one, so the map is always chaotic for  $p > 0, q > 0$  [23]. The real control parameters in the generalized cat map results in enlarging the cipher key space for image encryption scheme significantly. It has good chaotic natures such as ergodicity, high sensitivity to control parameters and initial values, pseudo-randomness, orbit inscrutability, etc. 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  $p = 5.324, q = 18.2$ , the  $x$ -coordinate sequence and the  $y$ -coordinate sequence of the orbit are plotted in Fig. 2 (b) and Fig. 2(c) respectively. Meanwhile, the sequences  $\{x_k\}, \{y_k\}$  have good randomness as well. Figs. 2(d)-(f) illustrate the pseudo-randomness of the yielded chaotic sequences.



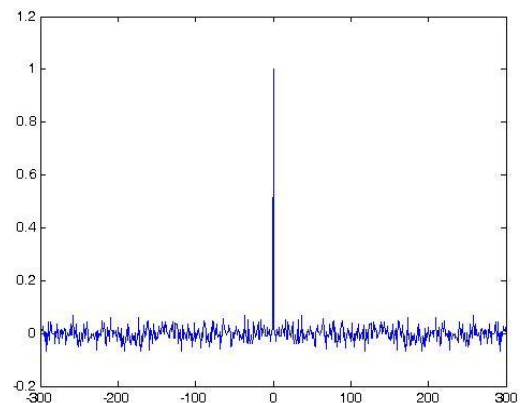
(a) The orbit of (0.5231, 0.7412)



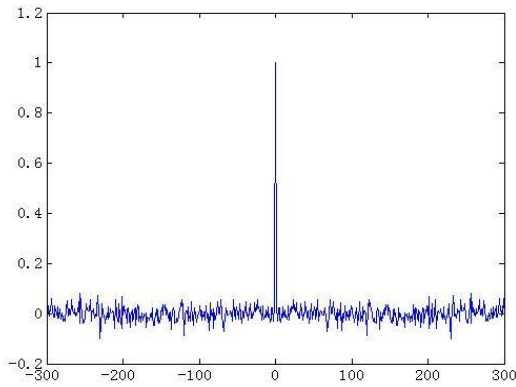
(b)  $x$ -coordinate sequence



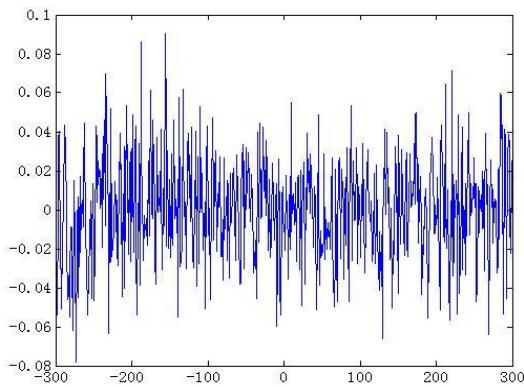
(c)  $y$ -coordinate sequence



(d) The auto-correlation of  $x$ -coordinate sequence



(e) The auto-correlation of y- coordinate sequence



(f) The cross-correlation of between x- coordinate sequence and y- coordinate sequence

Fig.2. Chaotic natures of the generalized Arnold map with  $p=5.324$ ,  $q=18.2$ .

**B. Permutation process**

In this stage, 2D generalized chaotic cat map (2) is employed to generate pseudorandom sequences, which are quantized and then utilized to shuffle the plain-image. We discuss the detailed permutation process step-by-step. Through the paper, we assume the plain-image to be encrypted is of size  $M \times N = 512 \times 512$ .

**Step 1.** Read a 256 gray-scale level plain-image with size  $M \times N$ , then expand this plain-image to a new image with size  $M \times 2N$  and 16 gray-scale level. The expansion strategy is as follow. The plain-image is divided into 2 parts, the higher 4 bits are treated as one part and the lower 4 bits are integrated into the second part. Therefore 8bits of each pixel can be divided into 2 groups as shown in Fig. 3.

(1) The higher 4 bits are extracted to form a new pixel set; each pixel gray value contains 4 bits, which are originally the 8th, 7th, 6th, and 5th bit in the plain-image with corresponding weights  $\frac{128}{256}$ ,  $\frac{64}{256}$ ,  $\frac{32}{256}$ ,  $\frac{16}{256}$  respectively. The higher 4 bits of each pixel carry  $\frac{128}{256} + \frac{64}{256} + \frac{32}{256} + \frac{16}{256} = 94.125\%$  of the pixel information. Regarding one plain-image with size  $M \times N$ , all the

higher four bits are extracted to form part I of size  $M \times N$  as well.

(2) The lower 4 bits are extracted to form another new pixel set shown as part II in Fig. 3. We note that the lower 4 bits of each pixel contains only 5.875% of the total information of the considered pixel.

The two subsets then form a new plain-image  $NP$  with size  $M \times 2N$  and gray-scale level 16.

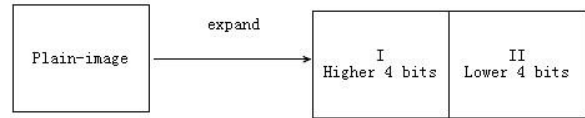


Fig.3. The expansion of plain-image

**Step 2.** We shuffle the expanded plain-image using a strategy via row-by-row, column-by-column instead of pixel-by-pixel, resulting in the improvement of execution efficiency. In traditional chaos-based image encryption schemes, the keystreams generated by the cipher keys are nothing with the plain-images, and therefore they fail to provide sufficient security and can be cryptanalyzed by known/chosen plaintext attacks. To enhance such a kind of security, we adopt an improved strategy. The chaotic sequences for permutation process are made to be dependent on both plain-image and cipher keys, and thereby get excellent key sensitivity and plaintext sensitivity. First, we calculate the number  $N_1$  of iterations for generalized cat map by Eq. (3). Then we iterate the generalized cat map  $N_1$  times starting with the initial conditions  $(x_0, y_0)$  and get  $(x_{N_1}, y_{N_1})$ .

$$N_1 = \{NP(1,1) + NP(1,2) + L + NP(1,2N) + NP(2,1) + L + NP(M,2N)\} \text{ mod } 256. \quad (3)$$

For simplicity, we still denote  $(x_{N_1}, y_{N_1})$  as  $(x, y)$ . The generalized cat map is then applied to generate four chaotic sequences. The pseudo code is outlined as follows.

```

for i=1 to max (M,2N) step 1
    x' = (x + p × y) mod 1
    y' = (q × x + (1 + p × q) × y) mod 1
    PR1(i) = 1 + floor(x' × M)
    PC1(i) = 1 + floor(y' × 2N)
    x = (x' + p × y') mod 1
    y = (q × x' + (1 + p × q) × y') mod 1
    PR2(i) = 1 + floor(x × M)
    PC2(i) = 1 + floor(y × 2N)
end

for i=1 to M step 1
    interchange NP(PR1(i,:),) and NP(PC2(i,:),)
end

for i=1 to 2N step 1
    
```

interchange  $NP(:,PC1(i))$  and  $NP(:,PC2(i))$   
end

where  $NP(i,:)$  and  $NP(:,j)$  represent all the elements of  $i$ th row and  $j$ th column of  $NP$  respectively; function  $\text{floor}(x)$  rounds  $x$  to the nearest integers towards minus infinity. interchange  $NP(PR1(i,:))$  and  $NP(PR2(i,:))$  stands for exchanging the  $PR1(i)$ th row and  $PR2(i)$ th row. In this process, the generalized cat map is iterated with randomly selected control parameters and initial conditions

$$(p, q) = (102.456789321, 92.234569217),$$

$$(x_0, y_0) = (0.123456789, 0.234567891).$$

### C. Diffusion process

In the diffusion stage, in order to enhance the resistance to statistical attacks and differential attacks efficiently, we design a bilateral diffusion with horizontal and vertical direction as shown in Fig. 4. After this process, the histogram of the cipher-image is extremely uniform and completely different from that of plain-image. The diffusion process is outlined as follows.

**Step 3.** After the permutation process, we get a shuffled image  $B$  with size  $M \times 2N$ . In this step, we shrink image  $B$  into image  $C$  with size  $M \times N$ , which is actually the reverse procedure of the expansion procedure. The pixel values locating in part I will become the 8th, 7th, 6th, 5th bit of the corresponding pixel of the shrunk image  $C$ . The pixel values locating in part II will become the 4th, 3rd, 2nd, 1st bit of the corresponding pixel of image  $C$ . We depict the procedure in Fig. 5.

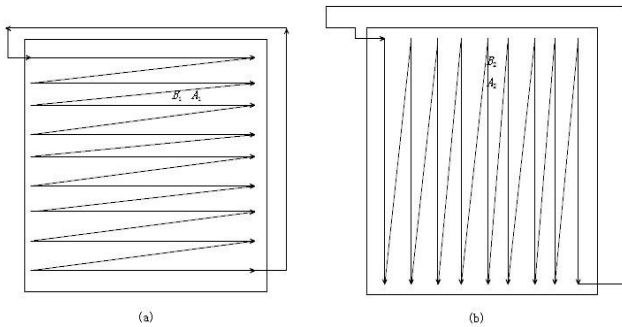


Fig.4. The bilateral diffusion diagram.

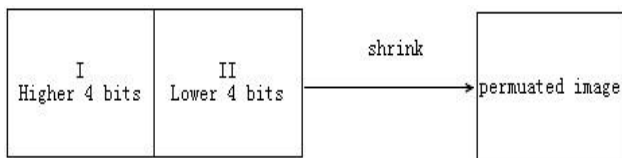


Fig.5. The shrinkage process.

**Step 4.** Generate two random positions  $A_1 = (p_{1x}, p_{1y})$ ,  $A_2 = (p_{2x}, p_{2y})$  as the start pixels of the diffusion operation in two different directions by the chaotic cat map. The motive is to enhance the security and randomness. They are calculated by

$$p_{1x} = (\text{floor}(bsm_1(100) \times 10^9)) \bmod M,$$

$$p_{1y} = (\text{floor}(bsm_2(100) \times 10^9)) \bmod N,$$

$$p_{2x} = (\text{floor}(bsm_1(101) \times 10^9)) \bmod M,$$

$$p_{2y} = (\text{floor}(bsm_2(101) \times 10^9)) \bmod N,$$
(4)

where  $bsm_1(s)$ ,  $bsm_2(s)$  are respectively the  $s$ th pseudorandom number of the chaotic sequences generated by Bernoulli shift map [24]

$$bsm_k(i+1) = (bsm_k(i) / c) \bmod 1, k = 1, 2 \quad (5)$$

with two initial values and one same control parameter

$$bsm_1(0) = 0.12345432167893,$$

$$bsm_2(0) = 0.88765432123456, c = 0.56789.$$

**Step 5.** The 2D gray value matrix  $C$  is first transformed to one vector  $V_1$ . Starting from the initial position  $A_1$  to the end position  $B_1 = (p_{1x}, p_{1y} - 1)$ , the first diffusion round is performed orderly according to the horizontal direction shown as Fig. 4(a). The diffusion is governed by

$$t_1(i) = [c_1(i) / (1000 \times c)] \bmod 1,$$

$$l_1(i+1) = (\text{floor}(t_1(i) \times 1000) + R(i+1)) \bmod 256, \quad (6)$$

$$c_1(i+1) = V_1(i+1) \oplus l_1(i+1),$$

where  $c_1(i)$  and  $c_1(i+1)$  are the previous and current gray value of the  $i$ th pixel and  $i+1$ th pixel of the output encrypted image,  $V_1(i)$  is the value of the  $i$ th element of vector  $V_1$ .  $t_1(i)$  and  $l_1(i)$  are temporary variables. The initial condition  $c_1(0)$  should be set one value to make the diffusion function definite, which can be regarded as part of cipher keys and defined here by

$$c_1(0) = \text{floor}([(Key1 / c) \bmod 1] \times 10^9) \bmod 256.$$

With  $Key1 = 0.5678912342321$  and the same control parameter  $c = 0.56789$ . Chaotic sequence  $\{R(i)\}$  is generated by

$$R(i) = \text{floor}(l(i) \times 10^9) \bmod 256, \quad (7)$$

where  $l(i)$  is the output sequence of the Bernoulli shift map

$$l(i+1) = (l(i) / c) \bmod 1 \quad (8)$$

with initial value  $l(0) = 0.25673548982132$  and control parameter  $c$ , respectively.

**Step 6.** In the second diffusion round, the diffusion direction is illustrated in Fig. 4(b) where we start from the

pixel  $A_2$  to the end pixel  $B_2 = (p_{2x} - 1, p_{2y})$ . The second diffusion round is performed as follows.

$$\begin{aligned} t_2(i) &= [c_2(i) / (1000 \times c)] \bmod 1, \\ l_2(i+1) &= (\text{floor}(t_2(i) \times 1000) + R'(i+1)) \bmod 256, \\ c_2(i+1) &= c_1(i+1) \oplus l_2(i+1), \end{aligned} \quad (9)$$

where  $c_1(i)$  is one-dimensional vector obtained by the first diffusion round in Step 5,  $c_2(i)$  and  $c_2(i+1)$  are the previous and current gray value of the  $i$ th pixel and  $i+1$ th pixel of the output cipher-image at the second diffusion round,  $t_2(i)$  and  $l_2(i)$  are temporary variables and the initial condition  $c_2(0)$  is set to be

$$c_2(0) = \{[(Key2 / c) \bmod 1] \times 10^9\} \bmod 256$$

where  $Key2=0.33792252345612$ . The sequence  $\{R'(i)\}$  is generated by

$$R'(i) = \text{floor}(l'(i) \times 10^9) \bmod 256 \quad (10)$$

where  $l'(i)$  is the output sequence of Bernoulli shift map

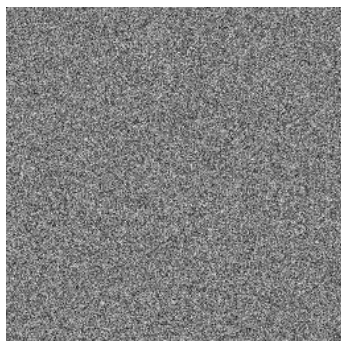
$$l'(i+1) = (l'(i) / c) \bmod 1 \quad (11)$$

with initial value  $l'(0)=0.48982132256735$  and control parameter  $c$ , respectively.

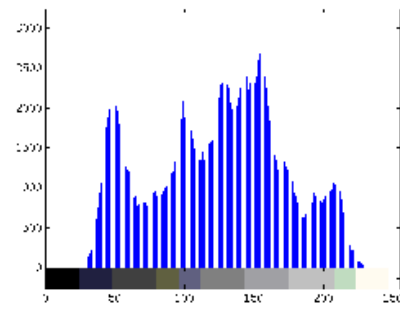
The complete image encryption scheme is composed of the permutation process and the bilateral diffusion process. The plain-image Lena with size 512X512 and its cipher-image are shown in Fig. 5(a), (b) respectively.



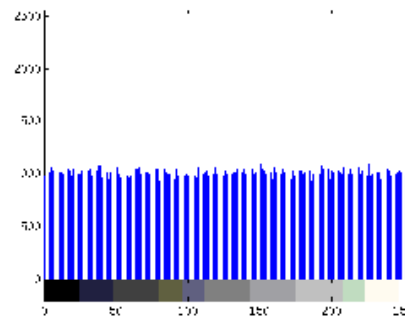
(a) Plain-image of Lena



(b) Cipher-image of Lena



(c) Histogram of plain-image



(d) Histogram of cipher-image

Fig. 6. The encrypted results.

### III. SECURITY AND PERFORMANCE ANALYSIS

In this section, security and performance analysis for the proposed image encryption scheme have been carried out, including histograms, correlation coefficients, information entropy, key sensitivity analysis, key space analysis, differential analysis, encryption rate analysis. Some comparisons with two other existing algorithms are done as well. Two comparable schemes proposed in [2] are Traditional Chaos-based Image Encryption Architecture (TCIEA) and Lightweight Bit-level Confusion and Cascade Cross Circular Diffusion Encryption Scheme (LBCCC).

#### A. Histogram analysis

Histogram analysis is a visual test which reveals the distribution information of pixel gray values. A good encrypted image should have a uniform and completely different histogram in comparison with that of the plain-image. As shown in Figs. 6(c)-(d), the histogram of the cipher-image obtained by the proposed image encryption scheme is fairly uniform and is significantly different from that of the plain-image. Therefore, the proposed image encryption scheme does not provide any useful information for the opponents to perform any effective statistical analysis attack on the cipher-image.

#### B. Correlation analysis

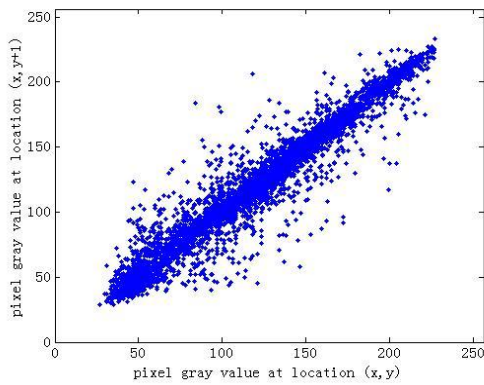
It is common sense that for an ordinary nature image having definite visual content, each pixel is highly correlated with its adjacent pixels either in horizontal, vertical or diagonal direction. An ideal encryption

technique should produce cipher-images with less correlation in the adjacent pixels. To quantify and compare the horizontal, vertical and diagonal correlations of adjacent pixels in the plain and cipher images, we calculate the correlation coefficients for all the pairs of horizontally, vertically and diagonally adjacent pixels respectively. First, we select 6000 pairs of two adjacent pixels randomly from an image, and then calculate the correlation coefficient by the following formulae

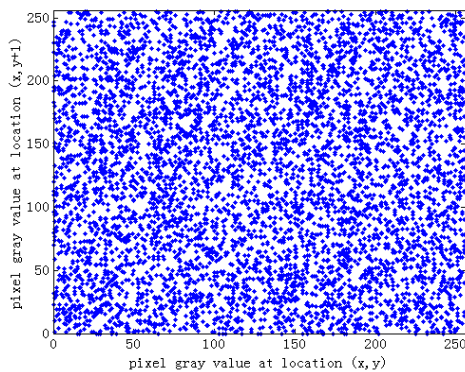
$$\rho_{X,Y} = \frac{E\{[X - E(X)][Y - E(Y)]\}}{\sqrt{D(X)}\sqrt{D(Y)}},$$

$$E(X) = \frac{1}{T} \sum_{i=1}^T x_i, \quad D(X) = \frac{1}{T} \sum_{i=1}^T [x_i - E(X)]^2, \quad (12)$$

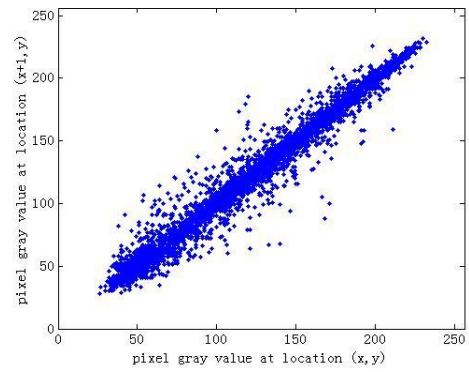
where  $X = (x_1, \dots, x_T)$ ,  $Y = (y_1, \dots, y_T)$  are the gray values of two adjacent pixel pairs.  $T$  is the total pair number,  $E(X), D(X)$  are the expectation and variance of  $X$ , respectively. In the simulations, two test images Lena and couple are used. The correlation coefficients for two test images derived from the proposed scheme and two comparable schemes are listed in Table 1. The correlation distributions of two adjacent pixels in the plain-image Lena and that in its corresponding cipher-image are show in Fig. 7. We can conclude that the correlation between adjacent pixels is greatly reduced in the cipher-image.



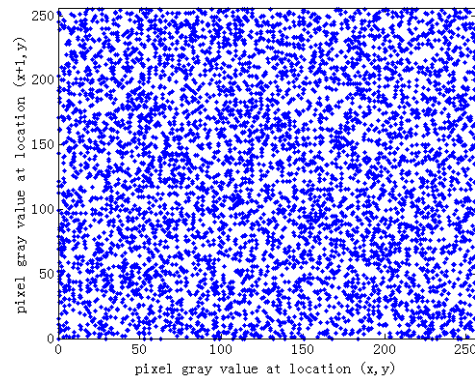
(a)



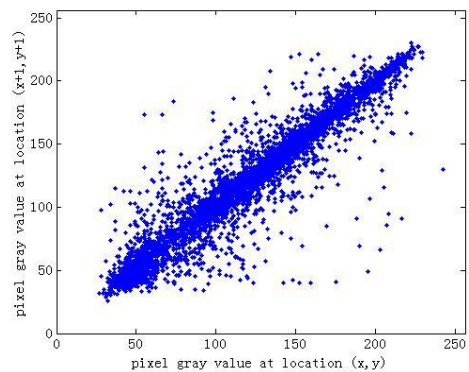
(b)



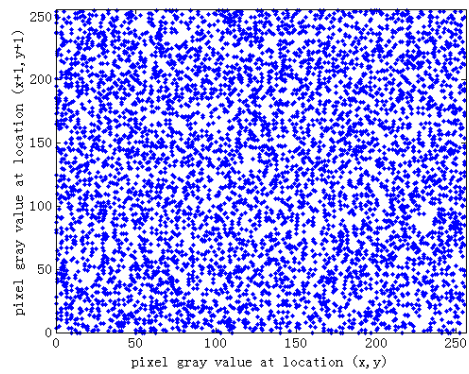
(c)



(d)



(e)



(f)

Fig.7. Correlations 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.

C. Differential attack analysis

The differential cryptanalysis of a block cipher is the study of how differences in a plaintext can affect the resultant differences in the ciphertext with the same cipher key. It is usually done by implementing the chosen plaintext attack but now there are extensions which use known plaintext as well as ciphertext attacks as well. As for image cryptosystems, attackers may generally make a minor change (e.g., modify only one pixel) of the plain-image and encrypt the original plain-image and the modified plain-image using the same cipher keys, then compare the two cipher-images to find out some meaningful relationships between the plain-image and the cipher-image. If a meaningful relationship between plain-image and cipher-image can be found in such analysis, which may further facilitate the attackers to determine the cipher key. If one minor change in the plain-image will cause significant, random and unpredictable changes in the cipher-image, then the encryption scheme will resist differential attack efficiently. To test the robustness of image cryptosystems against the differential cryptanalysis, two most common measures NPCR (number of pixel change rate) and UACI (unified average changing intensity) are used. NPCR is used to measure the percentage number of pixels in difference in two cipher-images obtained by applying the same cipher key on two plain-images having one pixel difference only.

NPCR for a cryptosystem is defined by

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

$$D(i, j) = \begin{cases} 1, & C_1(i, j) \neq C_2(i, j), \\ 0, & otherwise, \end{cases} \quad (13)$$

where  $M, N$  are the height and width of the considered image;  $C_1$  and  $C_2$  are the two cipher-images corresponding two plain-images with only one pixel difference.

The NPCR for two random images, which is an expected estimate for an ideal image cryptosystem, is given by

$$NPCR_{Expected} = (1 - 2^{-L}) \times 100\% , \quad (14)$$

where  $L$  is the number of bits used to represent all the intensity levels. For a 8-bit gray-scale image,  $L = 8$ , hence  $NPCR_{Expected} = 99.6094\%$ .

UACI, the average intensity difference between two cipher-images  $C_1$  and  $C_2$ , is calculated by

$$UACI = \frac{1}{M \times N} \left[ \sum_{i,j} \frac{|C_1(i, j) - C_2(i, j)|}{255} \right] \times 100\% . \quad (15)$$

The UACI for two random images, which is an expected estimate for an ideal image cryptosystem, is given by

$$UACI_{Expected} = \frac{1}{2^{2L}} \cdot \frac{\sum_{i=1}^{2^L-1} i(i+1)}{2^L - 1} \times 100\% . \quad (16)$$

For a 8-bit gray-scale image,  $UACI_{Expected} = 33.4635\%$ .

We randomly choose 10 pixels and calculate the corresponding NPCR and UACI values using the proposed image encryption scheme and two comparable schemes TCIEA and LBCCC. The experimental results are listed in Tables 2-3.

Table 1. Correlation coefficients of the proposed and comparable schemes.

Test image	Direction	Plain-image	TCIEA	LBCCC	Proposed scheme
Lena	Horizontal	0.9725	-0.0096	0.00032795	0.0079
	Vertical	0.9857	-0.0015	0.0085	-0.0063
	Diagonal	0.9571	0.0099	-0.0145	0.0114
Couple	Horizontal	0.9509	-0.0011	-0.0256	0.0036
	Vertical	0.9595	-0.0100	-0.0136	-0.0167
	Diagonal	0.9144	0.0035	0.0066	-0.0093

Table 2. NPCR and UACI performance with one round encryption.

(a) Proposed Scheme										
position	(27,461)	(340,158)	(72,504)	(69,380)	(450,246)	(307,303)	(57,468)	(152,288)	(62,295)	(325,19)
NPCR(%)	75.4379	76.1227	75.0801	75.7126	27.8019	74.6811	74.4827	39.0640	3.7609	28.7197
UACI(%)	25.1066	25.3403	25.0485	25.1682	9.3086	24.8565	24.7459	12.9700	1.2586	9.5515



(b) TCIEA

position	(27,461)	(340,158)	(72,504)	(69,380)	(450,246)	(307,303)	(57,468)	(152,288)	(62,295)	(325,19)
NPCR(%)	0.1171	0.3582	0.0488	0.0095	0.3418	0.0290	0.0366	0.4185	0.0214	0.1217
UACI(%)	0.0386	0.1222	0.0168	0.0033	0.1162	0.0099	0.0128	0.1426	0.0073	0.0404

(c) LBCCC

position	(27,461)	(340,158)	(72,504)	(69,380)	(450,246)	(307,303)	(57,468)	(152,288)	(62,295)	(325,19)
NPCR(%)	57.8312	10.3382	54.4086	37.4802	57.7965	53.2101	54.3964	23.5035	2.1427	35.9169
UACI(%)	19.4888	3.4672	18.2960	12.6269	19.4928	17.9483	18.3201	7.9558	0.7384	12.1110

Table 3. NPCR and UACI performance with two rounds encryption.

(a) Proposed Scheme

position	(27,461)	(340,158)	(72,504)	(69,380)	(450,246)	(307,303)	(57,468)	(152,288)	(62,295)	(325,19)
NPCR(%)	99.5922	99.6113	99.6231	99.5888	99.6078	99.6078	99.5876	99.6201	99.5991	99.6101
UACI(%)	33.4768	33.4530	33.5106	33.4430	33.5070	33.4600	33.4473	33.4362	33.4421	33.4023

(b) TCIEA

position	(27,461)	(340,158)	(72,504)	(69,380)	(450,246)	(307,303)	(57,468)	(152,288)	(62,295)	(325,19)
NPCR(%)	34.7233	67.2276	17.3740	2.5234	65.9348	10.4897	12.0281	68.7874	8.9283	37.0251
UACI(%)	11.7293	22.6670	5.8478	0.8333	22.1911	3.5486	4.1126	23.2377	3.0118	12.4871

(c) LBCCC

position	(27,461)	(340,158)	(72,504)	(69,380)	(450,246)	(307,303)	(57,468)	(152,288)	(62,295)	(325,19)
NPCR(%)	99.6078	99.5956	99.5979	99.5926	99.6090	99.6178	99.6304	99.6124	99.5934	99.5937
UACI(%)	33.4520	33.3745	33.4841	33.5222	33.4765	33.4651	33.4371	33.5834	33.3996	33.4644

#### D. Information entropy analysis

Information entropy is a measure of the uncertainty associated with a random variable and can also be a measure of disorder and randomness. It quantifies the amount of information contained in data, usually in bits/symbol. Two extremely cases are: a long sequence of repeating characters and a truly random sequence. The former has entropy of 0 since every character is predictable, and the latter has maximum entropy since there is no way to predict the next character in the sequence. Regarding image, it can be used to measure the uniformity of image histograms and the randomness of image information. The entropy of a message source  $m$  can be measured by

$$H(m) = \sum_{i=0}^{2^L-1} p(m_i) \log \frac{1}{p(m_i)}, \quad (17)$$

where  $L$  is the number of bits required to represent a symbol in the message  $m$ ,  $p(m_i)$  represents the probability of occurrence of symbol  $m_i$  and  $\log$  denotes the base 2 logarithm so that the entropy is expressed in

bits. For a random source emitting 256 symbols, its entropy is  $H(m) = 8$  bits. The best expected value of information entropy for an 8-bit cipher-image is 8, indicating the cipher-image can be considered as random one. We have calculated the information entropy for plain-images Lena, couple and their corresponding cipher-images. The results are shown in Table 4. The information entropy data produced using two comparable cryptosystems are listed as well.

#### E. Key space analysis

A good image encryption scheme should be extremely sensitive to cipher keys, which is an essential feature for any good cryptosystem in the sense that it can effectively make brute-force attacks infeasible. The key sensitivity of a cryptosystem can be observed in two ways: (i) the cipher-image derived from the cryptosystem should be extraordinarily sensitive to cipher keys, i.e., if we use two slightly different cipher keys to encrypt the same plain-image, then two produced cipher-images should be almost different and possess negligible correlation; (ii) the cipher-image cannot be decrypted correctly although there is a slight difference between the encryption and decryption keys. In the proposed scheme, the key space is

composed of all possible choices of  $p, q, x_0, y_0, bsm_1(0), bsm_2(0), c, l(0), l'(0), Key1$  and  $Key2$ .

To test the sensitivity of cipher key parameter  $k$ , the original plain-image Lena is encrypted with  $k, k - \Delta\delta, k + \Delta\delta$  respectively while keeping the other cipher key parameters unchanged. The key sensitivity coefficient is calculated by

$$p'_s(k) = \sum [N_s(I_1(i, j), I_2(i, j)) + N_s(I_1(i, j), I_3(i, j))]$$

$$p_s(k) = \frac{p'_s(k)}{2 \times M \times N} \times 100\%, N_s(x, y) = \begin{cases} 1, & x \neq y, \\ 0, & x = y, \end{cases} \quad (18)$$

where  $I_1, I_2, I_3$  are the encrypted images respectively, and  $\Delta\delta$  is the perturbing value. The test results are shown in Table 5. We have also test the sensitivity of  $Key1$  and  $Key2$ . As  $\Delta\delta = 10^{-7}$ , the corresponding  $p_s(k)$  are only 0.6681 and 0.6680 respectively. The experimental results show that these two keys are of low sensitivity and therefore cannot be considered to be cipher keys. The other parameters are all strongly sensitive and can be regarded as cipher keys. The key space is therefore larger than  $(10^{14})^7 \times (10^{13})^2 = 10^{124}$ . Such a key space is large enough to stand brute-force attacks. The sensitivity test can also be demonstrated visually, for example, see Fig. 8.

Table 4. Information entropy of the proposed and two comparable schemes.

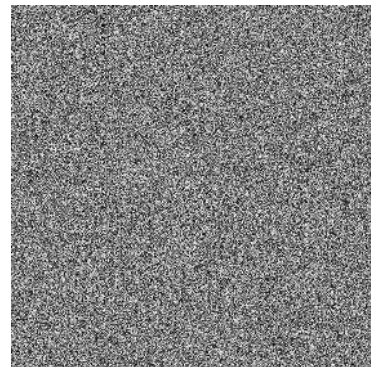
Test image	Proposed scheme	TCIEA	LBCCC
Lena	7.99930930933	7.9992544486	7.9992049214
Couple	7.99701882136	7.9972668082	7.9974865480

Table 5. Result of the sensitivity test ( $\Delta\delta = 10^{-13}$  for  $p, q$  and  $\Delta\delta = 10^{-13}$  for the other cipher keys).

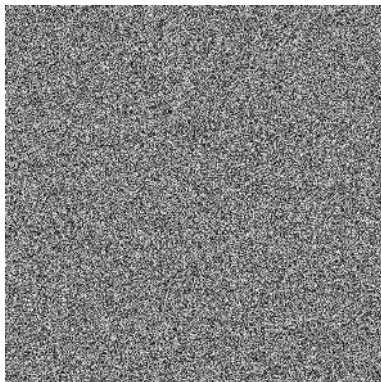
$k$	$bsm_1(0)$	$bsm_2(0)$	$x_0$	$y_0$	$c$	$l(0)$	$l'(0)$	$p$	$q$
$p_s(k)$	0.9962	0.9961	0.9960	0.9962	0.9962	0.9960	0.9961	0.9963	0.9960



(a) Original image



(c) Encrypted image with  $x_0 = 0.123456789 + 10^{-14}$



(b) Encrypted image with  $x_0 = 0.123456789$



(d) Original image

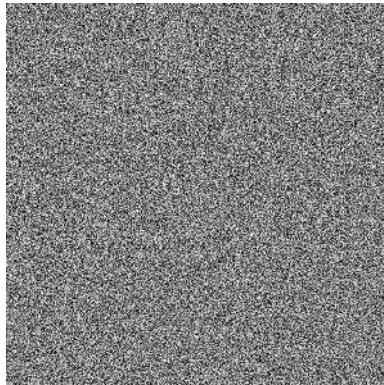
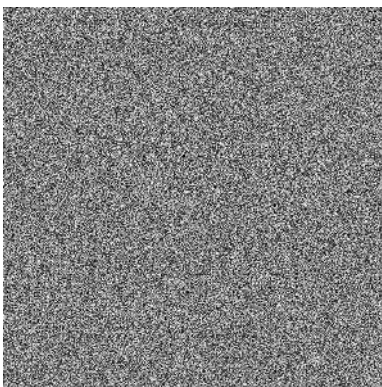
(e) Encrypted image with  $c=0.56789$ (f) Decrypted image with  $c=0.56789$ (g) Decrypted image with  $c=0.56789+10^{-14}$ 

Fig. 8. Key sensitive test.

#### F. Resistance to known-plaintext and chosen plaintext attacks.

In the permutation process, we calculate the number  $N_1$  and then iterate the chaotic cat map  $N_1$  times to get  $(x_{N_1}, y_{N_1})$  to generate chaotic sequences for permuting the plain-image. Since  $N_1$  depends on all the values of  $NP(i, j), 1 \leq i \leq M, 1 \leq j \leq 2N$ ,  $(x_{N_1}, y_{N_1})$  are then related to the plain-image and consequently the yielded chaotic pseudorandom sequences for permutation rely on the plain-image as well. When different plain-images are encrypted, the corresponding chaotic sequences applied to permute the plain-images will be different, resulting in different cipher-images. The attackers cannot find useful information by encrypting some special images. The

proposed image scheme can resist the known/chosen plaintext attacks efficiently.

#### G. Speed performance analysis

We have also estimated the encryption rate of the proposed image encryption scheme. An encryption round of the proposed image encryption scheme is composed of one confusion process and one bilateral diffusion process. Two comparable image encryption schemes are performed as well on a computer with Intel Core 2GHZ CPU and 1 GB RAM. The operating system is windows XP and the simulation software is MATLAB 7.2 programming. In Table 6, all the execution time for three image encryption schemes is listed.

Table 6. Execution time comparison.

Scheme	Time (s)
Proposed	0.957
TCIEA	0.656
LBCCC	1.041

From Table 6, we can know that the execution time of proposed scheme is shorter than the LBCCC's. Although the TCIEA scheme execution time is shortest, its NPCR and UACI values cannot achieved the ideal values even at the second encryption round. Therefore, we can be concluded that the proposed scheme have higher efficiency.

## IV. CONCLUSIONS

A novel chaos-based pseudorandom permutation and bilateral diffusion scheme for image encryption has been proposed. The pseudorandom number sequences produced via 2D chaotic cat map and generalized Bernoulli shift map have been used in an effective way to achieve the desired level of confusion and diffusion in the encryption process. The permutation process has been made to be dependent on the plain-images as well as cipher keys, which produce an excellent combination of plain-image sensitivity and key sensitivity in the encryption technique. The performance and security of the proposed image encryption technique, including histograms, correlation coefficients, information entropy, key sensitivity analysis, key space analysis, differential analysis, encryption rate analysis. etc. have been tested thoroughly using rigorous security analysis tools commonly used in the image processing as well as chaos-based cryptosystems. The results are perfect as required for any secure image and video communication application.

#### ACKNOWLEDGMENT

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

#### REFERENCES

- [1] C.E. Shannon, Communication theory of secrecy system.

- Bell Syst. Tech. J, 28(1949), 656-715.
- [2] B. Schiener, Applied Cryptography: Protocols, Algorithms and Source Code in C. John Wiley and sons, New York, 1996.
- [3] J. Fridrich, Symmetric cipher based on two dimensional chaotic maps. International Journal of Bifurcation and chaos, 8: 6 (1998), 1259-1284.
- [4] L. Kocarev, Chaos-based cryptography: a brief overview. IEEE Circuits and Systems Magazine, 1(2001), 6-21.
- [5] N. K. Pareek, V. Patidar, K. K. Sud, Image encryption using chaotic logistic map. Image and Vision Computing, 24(2006), 926-934.
- [6] R. Ye, A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism. Optics Communications, 284(2011), 5290-5298.
- [7] Vinod Patidar, N. K. Pareek. G. Purohit, K. K. Sud, A robust and secure chaotic standard map based pseudorandom permutation substitution scheme for image encryption. Optics Communications, 284 (2011) 4331-4339.
- [8] R. Ye, W. Guo, A chaos-based image encryption scheme using multi modal skew tent maps. Journal of Emerging Trends in Computing and Information Sciences, 4:10 (2013), 800-810.
- [9] K.-W. Wong, S.-H. Kwok, W.-S. Law, A fast image encryption scheme based on chaotic standard map. Physics Letter A, 372:15(2006), 2645-52.
- [10] 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.
- [11] L. Teng, X. Wang, A bit-level image encryption algorithm based on spatiotemporal chaotic system and self-adaptive, Optics Communications, 285(2012), 4048-4054.
- [12] W. Zhang, K.-W. Wong, H. Yu, Z.-L. Zhu, An image encryption scheme using lightweight bit-level confusion and cascade cross circular diffusion. Optics Communications, 285 (2012), 2343- 2354.
- [13] W. Zhang, K.-W. Wong, H. Yu, Z.-L. Zhu, A symmetric color image encryption algorithm using the intrinsic features of bit distributions. Commun. Nonlinear Sci. Numer. Simulat., 18 (2013), 584-600.
- [14] Y. Wang, K.W. Wong, X. F. Liao, T. Xiang, G. R. Chen, A chaos-based image encryption algorithm with variable control parameters. Chaos, Solitons and Fractals, 41(2009), 1773-1783.
- [15] S. J. Li, C. Q. Li, G. R. Chen, N. G. Bourbakis, K. T. Lo, A general quantitative cryptanalysis of permutation-only multimedia ciphers against plain-image attacks. Signal Process. Image Commun., 23(2009), 212-223.
- [16] C. Q. Li, S. J. Li, G. R. Chen, G. Chen, L. Hu, Cryptanalysis of a new signal security system for multimedia data transmission. EURASIP J. Appl. Signal Process., 8(2005), 1277-1288.
- [17] G. Alvarez, S. Li, Breaking an encryption scheme based on chaotic baker map, Physics Letters A, 352(2006), 78-82.
- [18] D. Xiao, X. Liao, P. Wei, Analysis and improvement of a chaos-based image encryption algorithm, Chaos, Solitons and Fractals, 40 (2009), 2191-2199.
- [19] J. M. Liu, Q. Qu, Cryptanalysis of a substitution-diffusion based on cipher using chaotic standard and logistic map, in: Third International Symposium on Information Processing, 2010, pp. 67-69.
- [20] R. Rhouma, E. Solak, S. Belghith, Cryptanalysis of a new substitution-diffusion based image cipher, Commun. Nonlinear Sci. Numer. Simulat., 15 (2010), 1887-1892.
- [21] X. Wang, G. He, Cryptanalysis on a novel image encryption method based on total shuffling scheme, Optics Communications, 284 (2011), 5804-5807.
- [22] V. Arnold, A. Avez, Ergodic problems in classical mechanics, Benjamin, New York, 1968.
- [23] C. Robinson, An Introduction to Dynamical Systems, Continuous and Discrete, Prentice Hall, 2004.
- [24] R. Ye, H. Zhao, An efficient chaos-based image encryption scheme using affine modular maps, I. J. Computer Network and Information Security, 4:7(2012), 41-50.

#### AUTHOR PROFILES

**Weichuang Guo**, male, is a master degree candidate at department of mathematics in Shantou University.

**Junqin Zhao**, female, is a master degree candidate at department of mathematics in Shantou University.

**Ruisong Ye**, male, was 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.