I.J. Modern Education and Computer Science, **2014, 10, 29-39**
Published Online October 2014 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijmecs.2014.10.05

A Novel Image Encryption Scheme Based on Multi-orbit Hybrid of Discrete Dynamical System

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

Huiqing Huang
School of Mathematics, Jiaying University, Meizhou, Guangdong, 514015, China

Xiangbo Tan
Department of Mathematics, Shantou University, Shantou, Guangdong, 515063, China

Abstract—A multi-orbit hybrid image encryption scheme based on discrete chaotic dynamical systems is proposed. One generalized Arnold map is adopted to generate three orbits for three initial conditions. Another chaotic dynamical system, tent map, is applied to generate one pseudo-random sequence to determine the hybrid orbit points from which one of the three orbits of generalized Arnold map. The hybrid orbit sequence is then utilized to shuffle the pixels' positions of plain-image so as to get one permuted image. To enhance the encryption security, two rounds of pixel gray values' diffusion is employed as well. The proposed encryption scheme is simple and easy to manipulate. 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, 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—Chaotic dynamical system, generalized Arnold map, tent map, shuffling, diffusion

I. INTRODUCTION

Chaos refers to a kind of pseudo-random irregular movement occurring in a certain dynamical system. Chaotic phenomenon was found by Lorenz, an American meteorologist, in the study of weather problems. Lorenz found the so-called butterfly effect, i.e., the properties of sensitivity to initial conditions in the study of weather forecast through numerical experiments over a long period of time. Loren is now called father of chaos thanks to his contribution to the study of chaotic motion in the deterministic system. Chaotic system is a complex nonlinear dynamic system, which has some fantastic characteristics, such as orbit inscrutability, sensitivity to initial conditions and control parameters, pseudo-randomness, topological transitivity, etc. Chaotic system has been widely applied in many disciplines, such as mathematics, physics, biology, computer, finance and even arts. Especially chaotic system has become a very important tool in the field of information security. It has been successfully introduced to modern cryptography thanks to its fantastic chaotic features meeting the fundamental requirements such as mixing and diffusion in the sense of cryptography. Meanwhile, digital multimedia data is being stored on different media, increasingly shared and communicated over the Internet and wireless networks nowadays. Protection of digital information against illegal usage becomes extremely necessary and urgent. It is well known that digital images possess some intrinsic features, such as bulk data capacity, high correlation among adjacent pixels, and human visual properties. As a result, traditional encryption algorithms, such as DES, RSA [1], are thereby not suitable for practical digital image encryption due to the weakness of low-level efficiency while encrypting images. All these factors make chaotic system a potential candidate for constructing cryptosystems, and thereby many chaos-based image cryptosystems have been proposed [2-15].

In this paper, we propose an image encryption scheme based on hybrid orbit of discrete dynamical chaotic system. The adopting of hybrid orbit of chaotic system can enlarge the key space greatly and therefore enhance the security compared with the conventional image encryption based on single orbit of dynamical system. Given three initial states, the generalized Arnold map is used to generate three orbits. Tent map is applied to generate one pseudo-random sequence to determine the hybrid orbit points from which one of the three yielded orbits. Based on the hybrid sequences derived by the hybrid orbit, we design an image encryption scheme with plain-image dependent key stream. The proposed scheme applies different key streams when encrypting different plain-images (even with the same hybrid chaotic sequences). To make the proposed scheme resist differential analysis attack, we perform one diffusion process with two rounds of diffusion operation which depends on both the cipher keys and the plain-image. The diffusion process can modify the pixel values and break the correlations between adjacent pixels of an image simultaneously. The security and performance analysis of the proposed image encryption are carried out using the histograms, correlation coefficients, information entropy, key sensitivity analysis, differential analysis, key space analysis, etc. All the experimental results show that the proposed image encryption scheme is highly secure and excellent performance, which makes it suitable for practical application.

The rest of the paper is organized as follows. In Section II, we briefly introduce the generalized Arnold map and tent map and discuss their chaotic natures. The hybrid sequence derived from multiple orbits of generalized Arnold map is outlined as well. Section III devotes to designing the image encryption scheme. One shuffling stage and one diffusion stage are presented to encrypt images. In Section IV, we present the results of security and performance analysis of the proposed image encryption scheme using the histograms, correlation coefficients, information entropy, key sensitivity analysis, differential analysis, key space analysis, encryption rate analysis, etc. Section V concludes the paper.

II. Chaotic Dynamical Systems

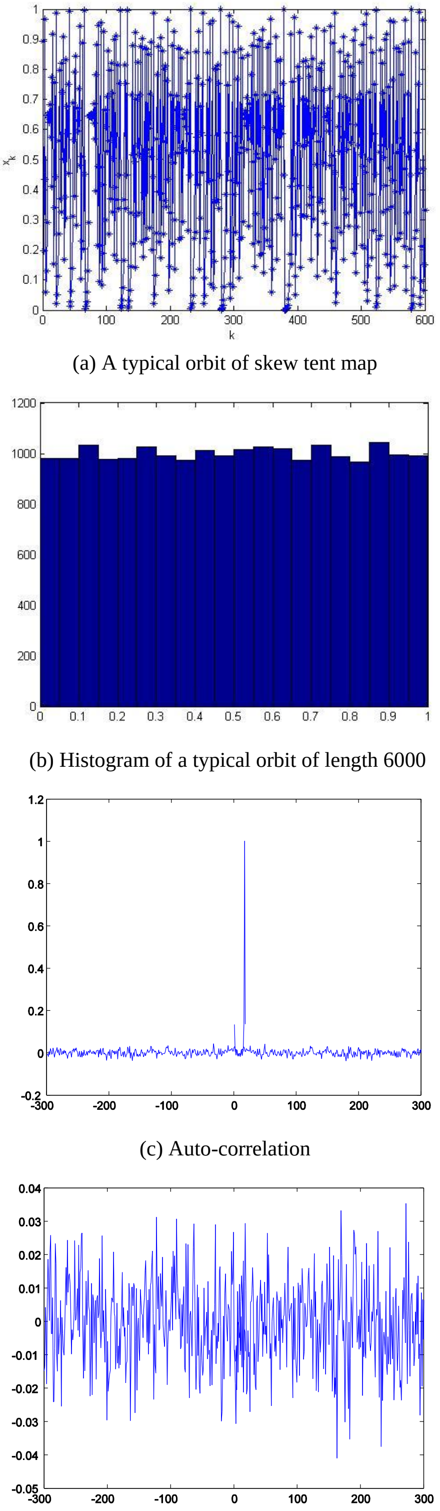
Skew Tent map is defined by

$$z_{n+1}=\begin{cases} z_n/a, & 0\le z_n\le a;\\ (1-z_\mathrm{n})/(1-a), & a<z_n\le 1; \end{cases} \qquad (1)$$

where $a\in(0,1)$ is the control parameter, $z_n, z_{n+1}\in[0,1]$ are the states. It is a noninvertible transformation of the unit interval onto itself. The transformation is continuous and piecewise linear. 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 Fig. 1(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 [16],

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

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 Fig. 1(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, i.e., the auto-correlation function has the characteristics of δ function and the cross-correlation owns the nature of zero function. The iterated trajectories are used to calculate the correlation coefficients, which are shown in Figs. 1(c)-(d) respectively.



(a) A typical orbit of skew tent map

(b) Histogram of a typical orbit of length 6000

(c) Auto-correlation

(d) Cross-correlation

Fig. 1. The chaotic nature of skew tent map

The pseudo-random sequence derived by the skew tent map is processed to generate another pseudo-random integer sequence composed of 1, 2, 3, which will be applied to randomly select orbits of generalized Arnold map. The quantized sequence is calculated by

$$t_n = floor(z_n \times 3)+1,\ t_n \in \{1,2,3\} \tag{2}$$

Arnold map is a two-dimensional invertible chaotic map introduced by Arnold and Avez [17]. It is described by

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod 1 \tag{3}$$

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 classical Arnold map (3) can be generalized to the following form by introducing two positive real control parameters $p>0$ and $q>0$,

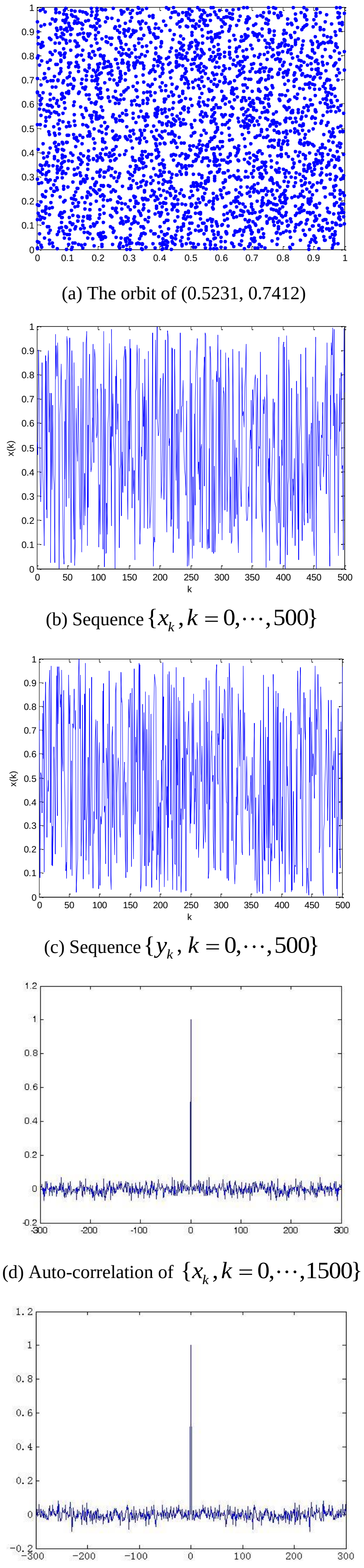
$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & p \\ q & 1+pq \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod 1. \tag{4}$$

The generalized Arnold map (4) has one Lyapunov characteristic exponent $\sigma_1 = 1 + \frac{1+\mathrm{pq}+\sqrt{p^2q^2+4pq}}{2} > 1$, so the map is always chaotic for $p>0$, $q>0$. The extension of p,q from positive integer numbers to positive real numbers is an essential generalization of the control parameters in conventional generalized Arnold maps, which enlarges 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 $p=5.324, q=18.2$, the x-coordinate and the y-coordinate sequences of the orbit are plotted in Fig. 2 (b) and Fig. 2(c) respectively. Some other good dynamical features in the generalized Arnold map, such as desirable auto-correlation and cross-correlation features are demonstrated in Figs. 2(d)-(f). The good chaotic nature makes it can provide excellent random sequence, which is suitable for designing cryptosystem.

To get one hybrid orbit, we define the following generalized Arnold map with three initial states

$$\begin{pmatrix} x_{n+1}^i \\ y_{n+1}^i \end{pmatrix} = \begin{pmatrix} 1 & p \\ q & 1+pq \end{pmatrix} \times \begin{pmatrix} x_n^i \\ y_n^i \end{pmatrix} \bmod 1,\ i=1,2,3, \tag{5}$$

where $(x_n^i, y_n^i) \in [0,1)$, p,q are positive real numbers. Choose three initial state values $(x_0^i, y_0^i), i=1,2,3$ and apply system (5) to generate three orbits, (x_n^i, y_n^i) stands for n th point on the i th orbit. Control parameters p,q and initial values $(x_0^i, y_0^i), i=1,2,3$ can be regarded as cipher keys. Therefore the key space enlarges greatly compared with the single orbit case.



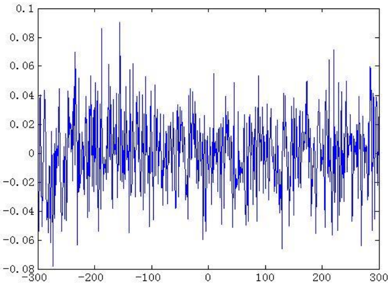
(a) The orbit of (0.5231, 0.7412)

(b) Sequence $\{x_k, k=0,\cdots,500\}$

(c) Sequence $\{y_k, k=0,\cdots,500\}$

(d) Auto-correlation of $\{x_k, k=0,\cdots,1500\}$

(e) Auto-correlation of $\{y_k, k=0,\cdots,1500\}$



(f) Cross-correlation of x_k and y_k sequences

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

III. The Proposed Image Encryption Scheme

The orbit of generalized Arnold map will be ergodic over the unit square $[0,1)^2$ and therefore we can apply it to design shuffling process of cryptosystem. The pseudo-random sequence generated by generalized Arnold map should be quantized to yield integer coordinates (px, py):

$$px = floor\left(x_n \times M\right) + 1, py = floor\left(y_n \times N\right) + 1,$$

where (x_n, y_n) is one of $(x_n^i, y_n^i)(i = 1, 2, 3)$, $floor\left(x\right)$ returns the largest integer not larger than x , which makes px, py belong to $\left[1, 2, ..., M\right]$ and $\left[1, 2, ..., N\right]$ respectively. The pseudo-random sequence $\{t_n\}$ is used to select the t_nth orbit point and to form one hybrid orbit $\{(x_n, y_n), n = 0, 1, \cdots\}$. The hybrid orbit possesses better chaotic natures and will enhance the cryptosystem security.

Suppose the plain-image I is a gray image with 256 gray scale levels and with size $M \times N$. We firstly describe some notations for the variables and their values. The control parameter and initial value for skew tent map are $\alpha = 0.37$, $z_0 = 0.49$ respectively. The parameter and initial values for generalized Arnold map are

$$p = 13.1, q = 33.7 \ ,$$
$$X = (x_0^1, x_0^2, x_0^3) = [0.31, 0.57, 0.86],$$
$$Y = (y_0^1, y_0^2, y_0^3) = [0.61, 0.32, 0.47] .$$

The transient iterated point number is L_0 and the total ergodic orbit point number is N_0 . The corresponding ergodic point number belonging to the ith orbit is denoted by $T(i), i = 1, 2, 3$ with initial values $T(1) = T(2) = T(3) = 0$. $T(i)$ is increased by 1 if the i th orbit is iterated once. The total N_0 ergodic points on the hybrid orbit distribute over the three orbits, therefore $N_0 = T(1) + T(2) + T(3)$ at last. Two vectors $xend, yend$ with length 3 are used to record the x -coordinate and y -coordinate of the three current orbit points, they are temporary variables. k is used to record the point number of the hybrid orbit. Matrix $index$ sized $M \times N$ and initialized to be zero matrix is one index matrix, whose element values are 0 or 1; $index\left(px, py\right) = 1$ if the pixel at position (px, py) is ergodic, and otherwise $index\left(px, py\right) = 0$. Variable $total$ denotes the number of unrepeated ergoic points. Vector IC with length L is employed to place the gray values of shuffled image. Another vector C of length L is used to put the gray values of cipher-image.

A. *The Shuffling Process*

Step 1. Read the plain-image I . Set the values for α , z_0 p, q, X, Y , N_0 L_0 . Iterate (1) to get one vector $\left\{z_n : n = 0, 1, \cdots, N_0 + L_0\right\}$, discard the first L_0 transient points and get $\left\{z_n : n = L_0 + 1, \cdots, N_0 + L_0\right\}$. For the sake of convenience, we still denote it as $\left\{z_n : n = 1, \cdots, N_0\right\}$. Then apply (2) to quantize it to obtain one integer sequence $\left\{t_n : n = 1, \cdots, N_0\right\}$. The generalized Arnold map (5) is utilized to iterate L_0 times for the three orbit and discard these L_0 transient points to get rid of the harmful transient effect of chaotic system. The values of $(x_{L_0}^i, y_{L_0}^i)(i = 1, 2, 3)$ are then set to be the initial values of the three orbit to yield the hybrid orbit and set $xend\left(i\right) = x_{L_0}^i, yend\left(i\right) = y_{L_0}^i$, $k = 1$.

Step 2. Calculate the next point of the t_k th orbit of the system (5). That is, iterate $(x_{L_0 + T(t_k)}^{t_k}, y_{L_0 + T(t_k)}^{t_k})$ = $(xend(t_k), yend(t_k))$ to get $(x_{L_0 + T(t_k) + 1}^{t_k}, y_{L_0 + T(t_k) + 1}^{t_k})$. Set $(x_k, y_k) = (x_{L_0 + T(t_k) + 1}^{t_k}, y_{L_0 + T(t_k) + 1}^{t_k})$, $T(t_k) = T(t_k) + 1$, $k = k + 1$, $(xend(t_k), yend(t_k)) = (x_k, y_k)$, $(px, py) = (floor(xend(t_k) \times M) + 1, floor(yend(t_k) \times N) + 1)$.

If $index\left(px, py\right)$=1, then repeat Step 2, otherwise go to Step 3.

Step 3. Excute

$$total = total + 1, \ index\left(px, py\right) = 1,$$
$$IC\left(total\right) = \mathrm{mod}(I(px, py) + px \times py, 256) .$$

Return to Step 2, until $k = N_0$.

Step 4. Check the remainder pixels which are not ergodic and perform the following code.

If $index(i, j) = 0, i = 1, \cdots, M; j = 1, \cdots$, , then set

$$total = total + 1, \ index\left(px, py\right) = 1,$$

$$IC\left(total\right)=\mathrm{mod}(I(i,j)+i\times j,256).$$

B. The Diffusion Process

Step 5. Quantize the pseudo-random sequence $\{z_n : n=1,\cdots,L\}$ to get one pseudo-random gray value sequence $\{m(i): i=1,\cdots,L\}$, $m(i)=floor(z_i\times 256)$.

Step 6. Set $i=1$ and encrypt the first pixel of shuffled image by

$$C(i)=IC\left(i\right)\oplus(\mathrm{mod}(C0+m(i),256)\oplus m(i)),$$

where $C0$ is a constant and can be regarded as cipher key. In the experiment, we set $C0=139$. Operation "$\oplus$" stands for the bitwise XOR Operation. Function $\mathrm{mod}(x,y)$ represents modular operation.

Step 7. Set $i=i+1$ and calculate the gray value of the i th pixel by

$$C(i)=IC\left(i\right)\oplus(\mathrm{mod}(C(i-1)+m(i),256)\oplus m(i-1))$$

until $i=L$.

Step 8. To get more efficient diffusion effect, we perform the second round of diffusion. Set $i=1$ and execute

$$C(i)=C\left(i\right)\oplus(\mathrm{mod}(C(L)+m(i),256)\oplus m(i)).$$

Step 9. Set $i=i+1$ and calculate

$$C(i)=C\left(i\right)\oplus(\mathrm{mod}(C(i-1)+m(i),256)\oplus m(i-1)),$$

until $i=L$.

Step 10. Convert the vector C to one 2D matrix $I1$ with sized $M\times N$; $I1$ is the cipher-image.

We note that the encryption process is invertible and so the decryption process is just the reverse of the encryption process.

IV. Performance and Security Analysis

An ideal encryption cryptosystem requires sensitivity to cipher keys, i.e., the cipher-text should have high correlation with cipher keys [1]. 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. Experimental results suggest that the proposed image encryption technique is robust and secure and can be used for the secure image and video communication applications.

A. Key Sensitivity Analysis and Key Space Analysis

The key space of an encryption scheme is composed of the total number of different cipher keys that can be used in the encryption procedure. 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.

The cipher keys consist of those keys p,q, x_0^1,x_0^2,x_0^3, y_0^1,y_0^2,y_0^3 in the generalized Arnold map and α,z_0 in the tent map. 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

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

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

$P_s(K)$ 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 tests. The variation ΔK is set to be 10^{-14} for p,q, 10^{-15} for x_0^1,x_0^2,x_0^3 and 10^{-16} for y_0^1,y_0^2,y_0^3, α,z_0. 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 $(10^{14})^2\times(10^{15})^3\times(10^{16})^5=10^{153}$, which is large enough to make brute-force attack infeasible.

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

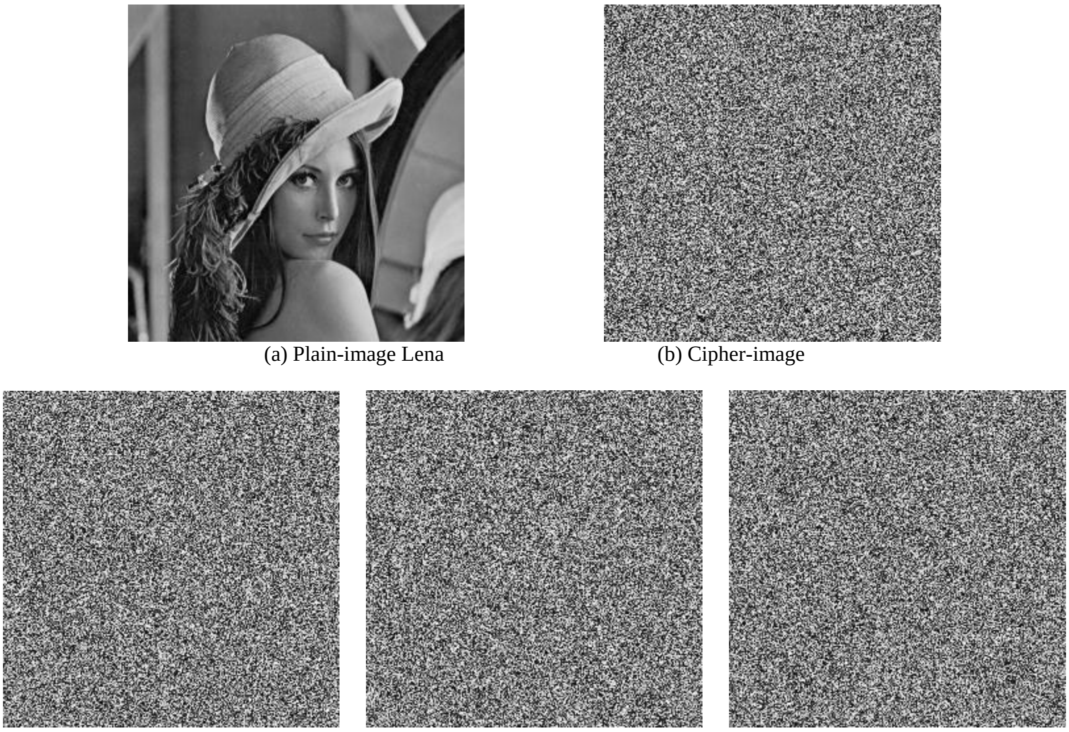
$$\alpha = 0.37,\ z_0 = 0.49,\ p = 13.1, q = 33.7,$$
$$(x_0^1, x_0^2, x_0^3) = (0.31, 0.57, 0.86),$$
$$(y_0^1, y_0^2, y_0^3) = (0.61, 0.32, 0.47).$$

The plain-image and cipher-image are shown in Figs. 3(a)-(b) respectively. Replace z_0=0.49 , q=33.7 , y_0^2=0.32 by $z_0 = 0.49 + 10^{-16}$, q = 33.7+10^{-14} , y_0^2=0.32+10^{-16} respectively, and keep the other cipher keys unchanged, the cipher-images are shown in Figs. 3(c)-(e) respectively. The difference images are Figs. 3(f)-(h).

(ii) Influence of minor change for cipher keys over decryption. Replace $p = 13.1$ by p=13.1+10^{-14} and keep the other cipher keys unchanged, the decrypted image is shown in Fig. 4(a), which has a difference 99.22% from the plain-image Lena. Replace $\alpha = 0.37$ by α=0.37+10^{-16} and keep the other cipher keys unchanged, the decrypted image is shown in Fig. 4(b), which has a difference 99.59% from Lena. If $x_0^1 = 0.31$ is changed to be x_0^1=0.31+10^{-15} , the decrypted image is shown in Fig. 4(c) with a difference 97.84% from Lena.

Table 1. results regarding the sensitivity to cipher keys

Key	p	q	x_0^1	x_0^2	x_0^3
$P_s(K)$	0.9962	0.9958	0.9963	0.9958	0.9961
Key	α	z_0	y_0^1	y_0^2	y_0^3
$P_s(K)$	0.9962	0.9962	0.9962	0.9959	0.9960



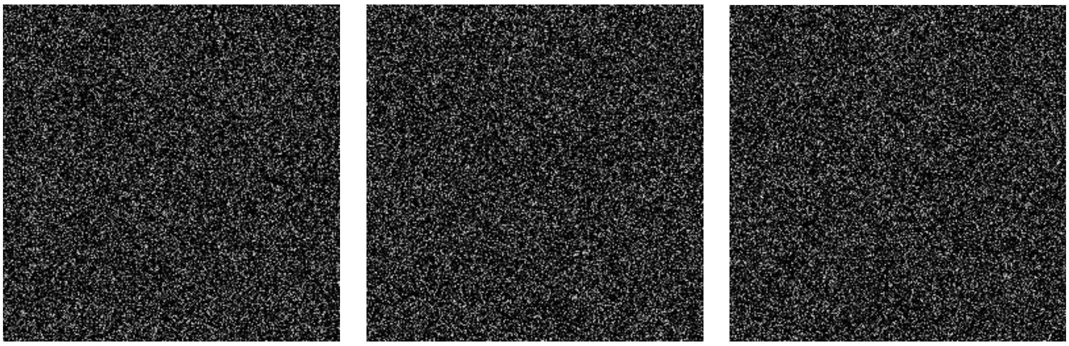
(a) Plain-image Lena

(b) Cipher-image

(c) Cipher-image by $z_0 = 0.49 + 10^{-16}$

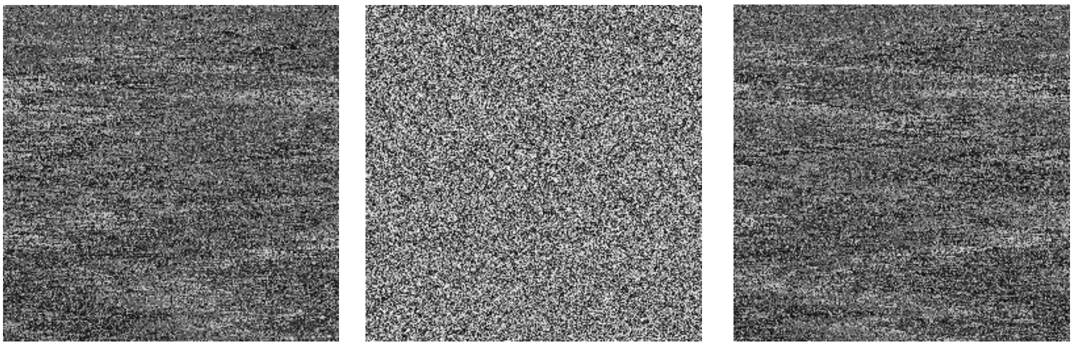
(d)Cipher-image by q = 33.7+10^{-14}

(e)Cipher-image by y_0^2=0.32+10^{-16}



(f) Difference image between (b) and (c) (g) Difference image between (b) and (d) (h) Difference image between (b) and (e)

Fig. 3. Key sensitivity tests I.



(a) Decrypted image by p=13.1+10^{-14} (b) Decrypted image by α=0.37+10^{-16} （c）Decrypted image by x_0^1=0.31+10^{-15}

Fig. 4. Key sensitivity test II.

B. Statistical Analysis

Shannon pointed out the possibility to solve many kinds of ciphers by statistical analysis in his masterpiece [18]. 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 Figs. 5(a)-(b), respectively. Fig. 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.

(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:

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

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

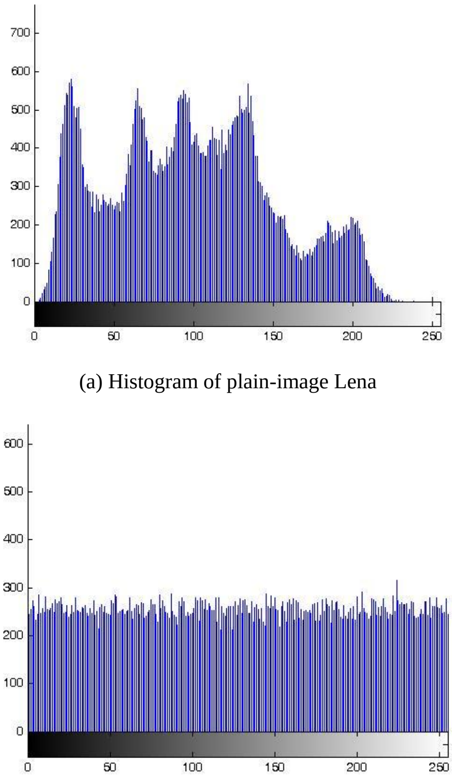
$$E(x) = \frac{1}{T}\sum_{i=1}^{T}x_i, D(x) = \frac{1}{T}\sum_{i=1}^{T}\left(x_i - E(x)\right)^2,$$

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 II. The correlation distribution of two adjacent pixels in the plain-image and that in the cipher-image are shown in Fig. 6.

(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 7.9971 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.



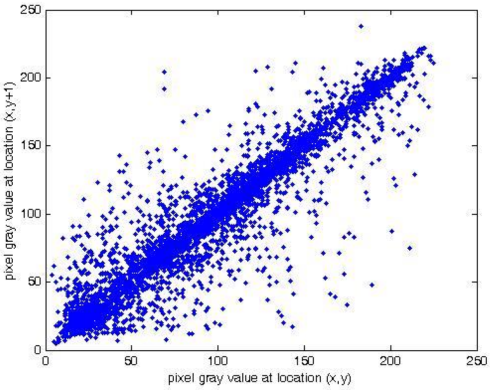
(a) Histogram of plain-image Lena

(b) Histogram of cipher-image

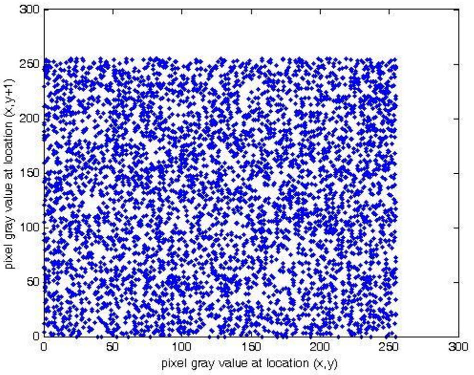
Fig. 5. The histograms of plain-image and cipher-image

Table 2. Correlation coefficients of plain-image and cipher-image.

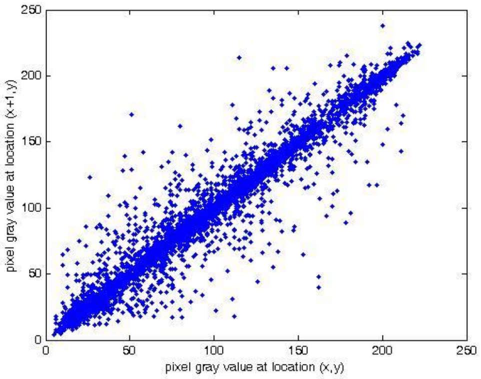
	Horizontal	Vertical	diagonal
Plain-image lena	0.9395	0.9689	0.9184
Cipher-image	0.0052	-0.0042	0.0141



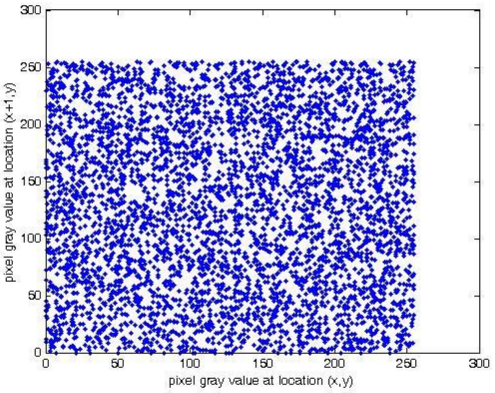
(a)



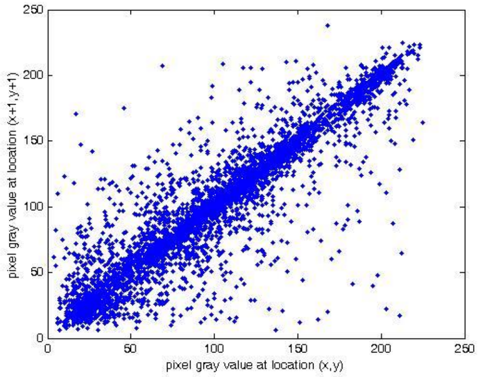
(b)



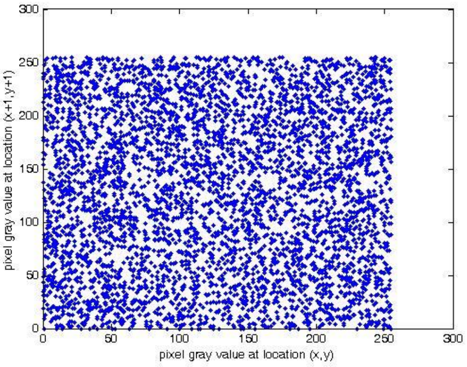
(c)



(d)



(e)



(f)

Fig. 6. 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. Peak Signal-to-noise Ratio Analysis

Another parameter to describe the encryption quality is the peak signal-to-noise ratio (PSNR). This term is described based on that the mean squared error (MSE) is calculated. This criterion provides the error between input image and output image. The MSE value is

$$MSE=\left\{\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left[I_O\left(i,j\right)-I_E\left(i,j\right)\right]^2\right\}^{1/2},$$

where $I_O\left(i,j\right)$ is the pixel value of plain-image, $I_E\left(i,j\right)$ is the pixel value of cipher-image. Thus the PSNR is described by

$$PSNR=20\log\left[\frac{I_{\max}}{MSE}\right]$$

where $I_{\max}$ is the maximum of pixel value of the image. The PSNR should be a low value, which corresponds to great difference between the original image and the encrypted image. To determine the encryption quality, the PSNR for the encryption of Lena is 8.5508. The calculated PSNR value is very low. Therefore, the encryption quality is good in sense of PSNR test.

D. Differential 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 also. As for image cryptosystems, attackers may generally make a slight change (e.g., modify only one pixel) of the plain-image, and compare the two cipher-images (obtained by applying the same cipher key on two plain-images having one pixel difference only) 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 opponents 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 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

$$NPCR=\frac{1}{M\times N}\sum_{i,j}D(i,j)\times 100\%,$$
$$UACI=\frac{1}{M\times N\times 255}\sum_{i,j}\left|C_1(i,j)-C_2(i,j)\right|\times 100\%$$

where C_1 and C_2 are the two cipher-images corresponding to two plain-images with only one pixel difference, and $D(i,j)$ is defined by

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

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.

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

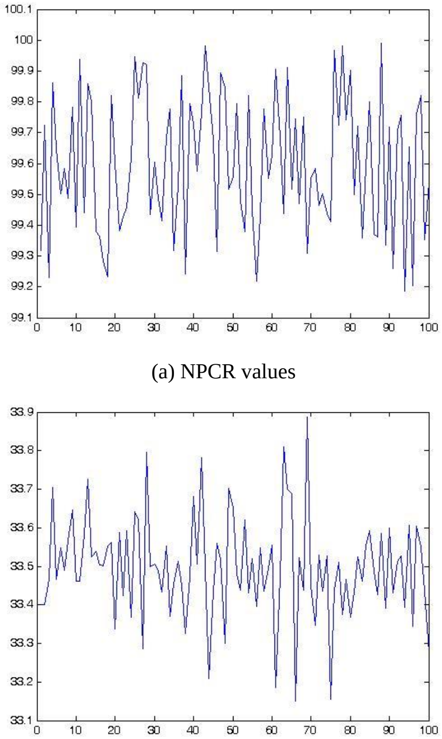
$$\text{NPCR}_{Expected}=(1-2^{-L})\times 100\%,$$

where L is the number of bits used to represent all the gray values of the considered image. For a 8-bit gray scale image L, hence $\text{NPCR}_{Expected}=99.6094\%$. The UACI for two random images, which is an expected estimate for an ideal image cryptosystem, is given by

$$\text{UACI}_{Expected}=\frac{1}{2^{2L}}\cdot\frac{\sum_{i=1}^{2^L-1}i(i+1)}{2^L-1}\times 100\%.$$

For a 8-bit gray image, $\text{UACI}_{Expected}=33.4635\%$.

To resist difference attacks, the values of NPCR and UACI should be close to the expected values. We randomly select 100 pixels and change the gray values with a difference of 1. The numerical results are shown in Fig. 7. The mean values of 100 NPCR and UACI values are 99.6015% and 33.4978% respectively. They are almost the same as the corresponding expected values. We can observe from Fig. 7 that the two measure values are exceptionally good undergoing only one round of encryption.



(a) NPCR values

(b) UACI values

Fig. 7. The differential analysis results.

V. Conclusions

A novel image encryption scheme based on multi-orbit hybrid of chaotic system is proposed in the paper. The proposed encryption scheme enhances the security compared with conventional image encryption schemes based on singe orbit in the sense that multi-orbit hybrid can enlarge the cipher key space greatly. The proposed image encryption scheme consists of one shuffling stage and one diffusion stage. The shuffling process utilizes the ergodicity of chaotic system and gets good shuffling effect. The diffusion process adopts two rounds of diffusion operation to achieve efficient diffusion effect. 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.

Acknowledgment

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

References

[1] B. Schiener. Applied Cryptography: Protocols, Algorithms and Source Code in C[M], John Wiley and sons, New York, 1996.

[2] J. Fridrich, Symmetric ciphers based on two-dimension chaotic map [J]. International Journal of Bifurcation and chaos, 1998, 8(6):1259-1284.

[3] F. Huang, Z.-H. Guan, A modified method of a class of recently presented cryptosystems, Chaos, Solitons and Fractals, 23(2005), 1893–1899.

[4] R. Ye, A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism, Optics Communications, 284(2011), 5290–5298.

[5] N. K. Pareek, V. Patidar, K. K. Sud, Image encryption using chaotic logistic map, Image and Vision Computing, 24(2006), 926-934.

[6] N. Masuda, K. Aihara, Cryptosystems with discretized chaotic maps, IEEE Trans. Circuits Syst. I, 49(2002), 28–40.

[7] H. Liu, X. Wang, Color image encryption using spatial bit-level permutation and high-dimension chaotic system, Optics Communications, 284(2011), 3895–3903.

[8] S. Behnia, A. Akhshani, S. Ahadpour, H. Mahmodi, A. Akhavan, A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps, Phys. Lett. A, 366(2007), 391–396.

[9] 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.

[10] V. Patidar, N. K. Pareek, K. K. Sud, A new substitution–diffusion based image cipher using chaotic standard and logistic maps, Communications in Nonlinear Science and Numerical Simulation, 14 (2009), 3056–3075.

[11] N. Masuda, K. Aihara, Cryptosystems with discretized chaotic maps, IEEE Trans. Circuits Syst. I, 49(2002), 28–40.

[12] S. Behnia, A. Akhshani, S. Ahadpour, H. Mahmodi, A. Akhavan, A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps, Phys. Lett. A, 366(2007), 391–396.

[13] 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.

[14] L. Kocarev, Chaos-based cryptography: a brief overview, IEEE Circuits and Systems Magazine, 1(2001), 6–21.

[15] C. Zhu, A novel image encryption scheme based on improved hyperchaotic sequences [J]. Opt. Commun., 2012, 285:29-37.

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

[17] V. Arnold, A. Avez, Ergodic problems in classical mechanics [M], Benjamin, New York, 1968.

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

Prof. Ruisong Ye 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.

Huiqing Huang was born in 1981 and received the Master degree in Applied Mathematics in 2009 from Shantou University, Shantou, Guangdong, China. He is now a lecturer, at School of Mathematics, Jiaying University, Meizhou, Guangdong, 514015, China. His research field is fractal, chaos and their applications in information security.

Xiangbo Tan: graduate student at department of mathematics in Shantou University, His research field is chaotic dynamical system and its application in information security.