Image Encryption Scheme Based on Amplitude Modulation of Chaotic Signals

Chunlai Li [1,2,3*], Wenhua Hai [1,2*]

[1] Department of Physics and Key Laboratory of Low-dimensional Quantum Structures and Quantum Control of Ministry of Education, Hunan Normal University, Changsha, 410081, China.

[2] Synergetic Innovation Center for Quantum Effects and Applications, Hunan Normal University, Changsha, 410081, China.

[3] College of Physics and Electronics, Hunan Institute of Science and Technology, Yueyang, 414006, China.

* Corresponding author. Email: hnistlichl@163.com.

Manuscript submitted May 20, 2018; accepted June 8, 2018.

doi: 10.17706/jsw.13.8.421-436

Abstract: We introduce a three-dimensional chaotic system and reveal the relation between signal amplitude and the system parameters which can enrich the key for a cryptosystem. To study application of the relation to multi-media security, we propose an image encryption scheme based on the permutation-diffusion architecture. Security of immunity to known-plaintext attack and chosen-plaintext attack is ensured by adopting plaintext sequence and amplitude parameter to generate key stream with the ideology of one-time pad. Numerical experiments are implemented and prominent advantage of the theoretical scheme is confirmed.

Key words: Amplitude modulation, chaotic system, one-time pad, image encryption.

1. Introduction

With the rapid development of information technology and multimedia industry, digital image has been increasingly acquired, stored and transmitted. Consequently, the secure communication of confidential digital images over open channels has become vital and urgent requirement [1], [2]. Several traditional encryption schemes, such as DES (data encryption standard), AES (advanced encryption standard) and RSA (Rivest-Shamir-Adleman), are introduced for textual information based on confusion and diffusion principles [2]. In view of the theory by Shannon, practical cryptographic characteristics for image encryption include not only the bit confusion and diffusion, but also the computational unpredictability, and the sensitivity to keys and plain text [3], which can be commendably catered by the fundamental features of a chaotic system. Therefore, chaos can be thought of as a suitable candidate for image encryption [4-9].

In 1998, Fridrich introduced chaos-based image encryption with permutation-diffusion procedure at the first time [10]. Under this scheme, the position of image pixels is firstly changed to erase the high correlation between adjacent pixels; then the pixel values are modified sequentially using pseudorandom sequences, so that a tiny change in a pixel can spread out to as many pixels in the whole image as possible, and the correlations of adjacent pixels are broken simultaneously. Subsequently, the permutation-diffusion schemes and their extension, such as bit-level permutation approach [11], [12], plain-image confusion [13], enhanced key stream generator [1], [5], transform domain scheme are proposed [4], [14], [15]. Recently,

some chaos-based image encryption algorithms with permutation-diffusion architecture are found to be insecure against different attacks, and have been subsequently broken [16]-[21]. The common weaknesses of these insecure schemes are summarized as below: (a) The algorithms for encryption/decryption are insensitive to the variations of the plain-image, and the key streams are independent of the plain-image, which favor known-plaintext attack and chosen-plaintext attack. (b) The chaotic sequences for permutation and diffusion are generated from different systems, and the procedures of permutation and diffusion are independent. Accordingly, the change of one of secret keys will only affect the permutation module or the diffusion procedure. (c) The schemes do not conform to the idea of one-time pad (OTP) since the key is unchanged in the procedure of encryption, which can't ensure perfect security.

In cryptography, OTP is the only known unbreakable cipher, and was proven mathematically to be perfectly secure by Shannon [22]. For OTP scheme, the private key is required to not only be perfectly random, but also be used only once, thus it must be as long as the message with an executed difficulty. In spite of the practical shortcomings, OTP continues to be used in DNA cryptography [23], quantum cryptography [24] and even in classical cryptography [25], when high security is desired. The amplitude parameter of a chaotic system is defined as that enabling modulating signal amplitude. If the amplitude parameter of a chaotic system is regarded as encryption key and changes with encryption process for every pixel, it can provide the private key as long as the message and result in possible realization of OTP.

In this paper, we present a practicable image encryption scheme for both combining permutation and diffusion and addressing the existed problems (weaknesses) mentioned above. Firstly, we propose a three-dimensional chaotic system with five linear terms and two quadratic product terms. Basic dynamical properties including the amplitude modulation are analyzed carefully. And the chaotic sequences are modified to obtain a chaotic key stream suiting for diffusion. Then the idea of OTP realized by correlating the parameter secret key and plain-image, is employed to shuffle the pixels. Security analyses and experiment results show the proposed scheme has high key sensitivity, high plaintext sensitivity and resistance to different attacks.

2. The Chaotic System

2.1. System Description

The introduced three-dimensional chaotic system holds five linear terms and two quadratic terms, as below

$$\begin{cases} \dot{x}_1 = -ax_1 + bx_2 \\ \dot{x}_2 = cx_1 + dx_3 - ex_1x_3 \\ \dot{x}_3 = fx_1^2 - gx_3 \end{cases} \tag{1}$$

Here, x_1, x_2, x_3 are state variables and a, b, c, d, e, f, g are positive parameters. Similar to the ordinary chaotic systems, system (1) exhibits complex dynamical behaviors but different properties of amplitude modulation by varying some parameter.

By considering the condition $\dot{x}_1 = 0$, $\dot{x}_2 = 0$, $\dot{x}_3 = 0$, we get three equilibrium points, depicted by

$$E_0(0,0,0),\ E_1\left(x_+, \frac{a}{b}x_+, \frac{f}{g}x_+^2\right),\ E_2\left(x_-, \frac{a}{b}x_-, \frac{f}{g}x_-^2\right) \text{ with } x_\pm = \frac{d}{2e} \pm \sqrt{\frac{d^2}{4e^2} + \frac{gc}{ef}}.$$

The corresponding characteristic equation can be deduced as

$$\Phi(\lambda) = -\lambda^3 - (a+g)\lambda^2 + (-ag + b(c - ex_3))\lambda + 2bfx_1(d - ex_1) + bg(c - ex_3) \tag{2}$$

Throughout this manuscript, we consider the parameter set

$$S = \{a, b, c, d, e, f, g\} = \{10, 6, 28, 1, 1, 0.1, 5\}$$

Unless explicitly stated otherwise. Thus the nonzero equilibrium points read $E_1(37.9199, 63.1999, 28.7584)$, $E_2(-36.9199, -61.5332, 27.2616)$. The characteristic roots corresponding to the equilibrium points are

$$E_0 : \lambda_1 = -28, \lambda_2 = 20, \lambda_3 = -3.$$

$$E_1 : \lambda_1 = -17.4608, \lambda_2 = 1.2304 + 9.7982i, \lambda_3 = 1.2304 - 9.7982i.$$

$$E_2 : \lambda_1 = -17.7118, \lambda_2 = 1.3559 + 9.5793i, \lambda_3 = 1.3559 - 9.5793i.$$

For the equilibrium points E_0, λ_1 and λ_3 are negative real number, λ_2 is positive real number. As a consequence, E_0 is a saddle-node of index 1. But for the equilibrium points E_1 and E_2, λ_1 is a negative real number, λ_2 and λ_3 become a pair of complex conjugate roots with positive real parts, meaning saddle-focus points of index 2. The Lyapunov exponents of system (1) are calculated as $0.869,\ 0.0,\ -22.51012$ for the parameter set S, and the corresponding Kaplan-Yorke dimension is 2.0386, denoting a fractional feature. Therefore, system (1) is chaotic, as depicted in Fig.1.

It deserves to be mentioned that system (1) holds two asymmetrical nonzero equilibrium points which is different from those of the similar systems [26-30], therefore, they are not topological equivalent, though all have similar attractors.

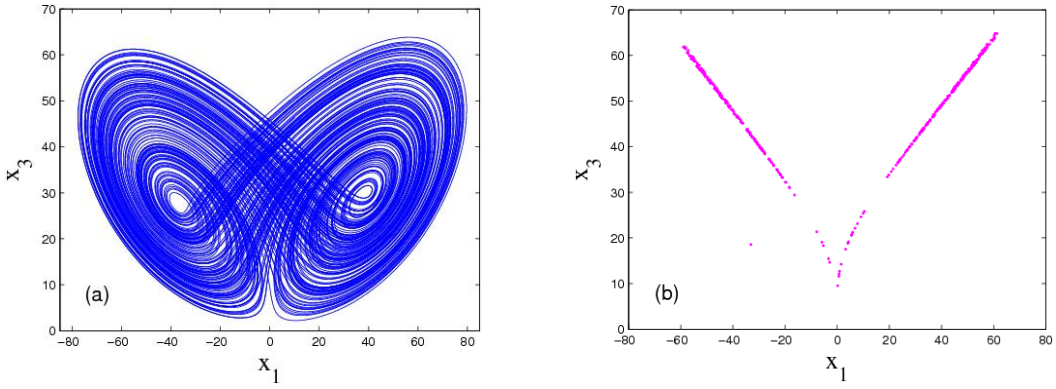

Fig. 1. x_1-x_3 phase portrait (a) and poincaré map (b) with x_2=0 and the parameter set $S = \{a, b, c, d, e, f, g\} = \{10, 6, 28, 1, 1, 0.1, 5\}$.

2.2. Phase Modulation of Chaotic Signals

In system (1), coefficient d can control the phase of signals x_1 and x_2 simultaneously, which can be seen from the invariance with the transformation

$$(x_1, x_2, x_3, a, b, c, d, e, f, g) \to (-x_1, -x_2, x_3, a, b, c, -d, e, f, g).$$

The bifurcation diagrams for variables x_1 and x_2 are reverse symmetrical about d =0, which further confirms that the sign variation of d can change the polarity of x_1 and x_2, regardless of the dynamics behavior, as described in Fig. 2.

2.3. Amplitude Modulation of Chaotic Signals

It is known from Refs. [31]-[33] that, for the quadratic chaotic systems, the coefficients of quadratic terms can control the signal amplitude partially or totally. Here we define such coefficients of a chaotic system as *amplitude parameters*. We will use the amplitude parameters to study the amplitude modulation of Eq. (1) for both the cases $f \neq e$ and $f = e$ as follows.

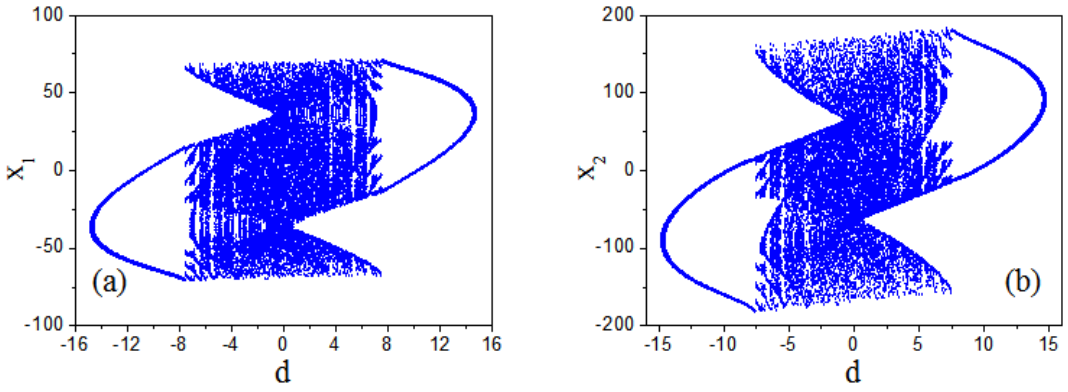

Fig. 2. Bifurcation diagram versus *d* with the parameter set *S* except for *d*.

Case $f \neq e$. The bifurcation diagram of system (1) with $e \in [0,\ 10]$ is depicted in Fig.3 (a). Superficially, the coefficient *e* can control the amplitude of signal x_1 nonlinearly. But one can see that there emerges visible period doubling bifurcation or periodic window from the enlarged view, as shown in Fig.3 (b). The bifurcation diagram versus coefficient *f* further demonstrates that not all coefficients of quadratic terms can modulate the signal amplitude, seen in Fig.3 (c).

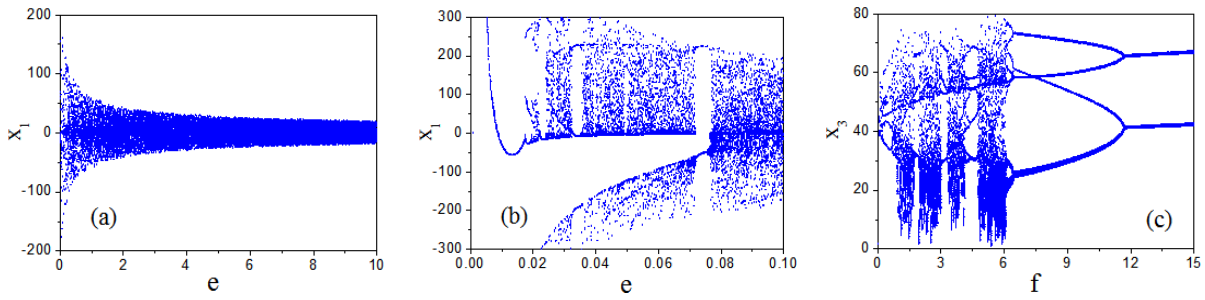

Fig. 3. (a), (b) Bifurcation diagram versus *e* with the parameter set *S* except for *e*;
(c) Bifurcation diagram versus *f* with the parameter set *S* except for *f*.

Spontaneously, when considering the property of amplitude modulation for chaotic system, we raise a puzzled yet worth to be explored question "what's the necessary condition for possibly modulating signal amplitude of chaotic system?" It's known that the equilibrium point of dynamical system denotes the equilibrium position of unstable motion with zero velocity, and the nonzero equilibrium points will accordingly deviate from the original position when rescaling the trajectory of chaotic attractor. Therefore, for the chaotic system with multiple equilibrium points, the possible prerequisite for amplitude modulation of chaotic signals can be summarized as: (a) in the mathematical expression of nonzero equilibrium point, the amplitude parameter is symmetrical about some axis; (b) and the amplitude parameter can modulate the location of the nonzero equilibrium point in coordinate plane.

Case $f=e$. Considering the expression of nonzero equilibrium point of system (1) for the case $f\neq e$, any one of parameters e and f of nonlinear term can't modulate the location of equilibrium point E_1 or E_2. Consequently, parameter e or f can't execute amplitude modulation. Now we introduce a unified parameter e for nonlinear term x_1x_3 and x_1^2, resulting in the new case $f=e$ of Eq. (1) and the nonzero equilibrium points

$$E_1\left(\frac{1}{e}\left(\frac{d}{2}+\sqrt{\frac{d^2}{4}+gc}\right),\ \frac{1}{e}\left(\frac{ad}{2b}+\frac{a}{b}\sqrt{\frac{d^2}{4}+gc}\right),\ \frac{1}{e}\left(\frac{d^2}{2g}+c+\frac{d}{2g}\sqrt{\frac{d^2}{4}+gc}\right)\right),$$
$$E_2\left(\frac{1}{e}\left(\frac{d}{2}-\sqrt{\frac{d^2}{4}+gc}\right),\ \frac{1}{e}\left(\frac{ad}{2b}-\frac{a}{b}\sqrt{\frac{d^2}{4}+gc}\right),\ \frac{1}{e}\left(\frac{d^2}{2g}+c-\frac{d}{2g}\sqrt{\frac{d^2}{4}+gc}\right)\right). \quad (3)$$

The set of symmetrical axis for points E_1 and E_2 is $\left(\frac{d}{2e},\ \frac{ad}{2be},\ \frac{d^2}{2eg}+\frac{c}{e}\right)$. In addition, the unified parameter e can modulate the location of the nonzero equilibrium points according to $\frac{1}{e}$ respectively. As a result, the parameter e can execute amplitude modulation for signal x_1, x_2, x_3 according to $\frac{1}{e}$. The corresponding signal amplitude and Lyapunov exponent spectrum versus e are depicted in Fig.4.

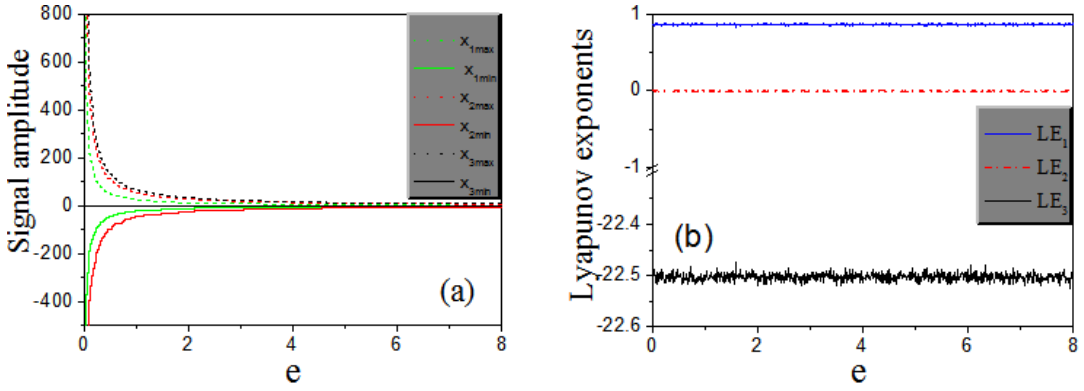

Fig. 4. Signal amplitude (a) and Lyapunov exponent spectrum (b) versus e with the parameter set S except for e and f.

3. Image Encryption Scheme Based on Amplitude Modulation of Chaotic Signals

3.1. Improved Chaotic Sequences

The Logistic map is a simple chaotic system with one-dimensional dynamical equation yet complex behavior, expressed as

$$x(n+1)=\alpha x(n)\left(1-x(n)\right) \quad (4)$$

When the parameter is selected as $\alpha\in(3.9,4]$, the system (4) is chaotic and the sequence $x(n)$ is between 0 and 1 [5, 7].

Based on Golomb's theory [1], three properties should hold for an ideal pseudo-random sequence: (a) the AC (autocorrelation) is the delta function; (b) the CC (cross correlation) is zero; (c) uniform distribution. Experimental results show that the sequences x_1, x_2, x_3 generated by new system (1) with $f = e$ and the sequence x generated by system (4) are not the ideal pseudo-random sequences, which need to be modified, see Figs.5 (a), (c) and Figs.6 (a). In the encryption scheme, we make the pretreatment for these sequences, as below:

$$\begin{aligned} h_1 &= x_1 \times 10^2 - round(x_1 \times 10^2) \\ h_2 &= x_2 \times 10^2 - round(x_2 \times 10^2) \\ h_3 &= x_3 \times 10^2 - round(x_3 \times 10^2) \\ h_4 &= x \times 10^2 - round(x \times 10^2) \end{aligned} \tag{5}$$

In (5), round (*) stands for rounding * to the nearest integer. As shown in Fig.5 (b), (c), the autocorrelations of sequences h_1 to h_4 verge on the ideal delta function. And the cross correlation between sequences h_1 and h_2 is close to zero, depicted as Fig.6 (b). Further, we know that the modified sequences hold uniform distribution between –0.5 and 0.5. Therefore, the modified sequences in (5) have better performance for image encryption.

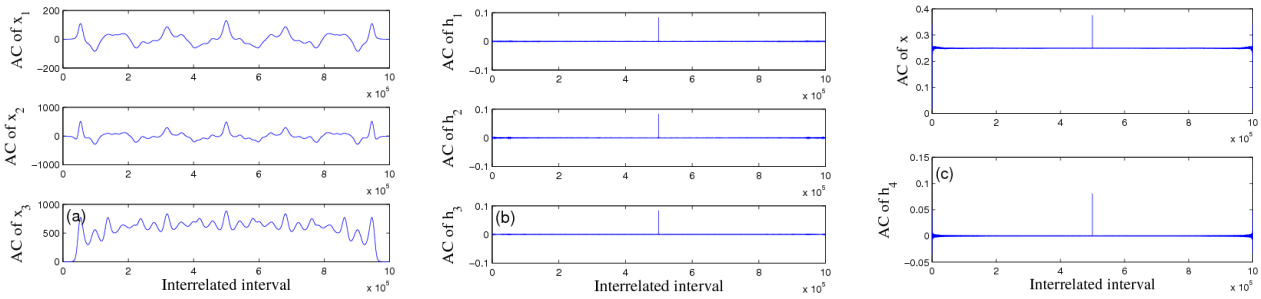

Fig. 5. Autocorrelation series for the pseudo-random sequences and the modified forms.

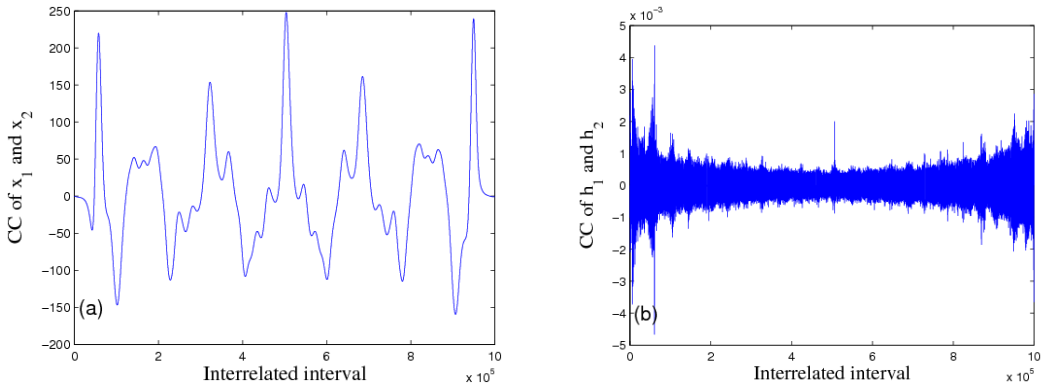

Fig. 6. Cross correlation series for x_1, x_2 and h_1, h_2.

3.2. Image Encryption Scheme

The block diagram of the suggested image encryption scheme is shown in Fig.7. This scheme can ensure high security for holding the following features: (a) The chaotic sequences for permutation and diffusion are simultaneously generated from Logistic map and new chaotic system, thus the change of one of secret keys will affect both the permutation module and the diffusion procedure. (b) The

plaintext sequence and amplitude parameter are adopted to generate key stream based on the idea of OTP, which can effectively fend off known-plaintext attack and chosen-plaintext attack. (c) The chaotic key stream is modified for diffusion process based on the properties of ideal pseudo-random sequence. (d) There exists a big key space to ensure a high security level. The encryption procedure is described as follows.

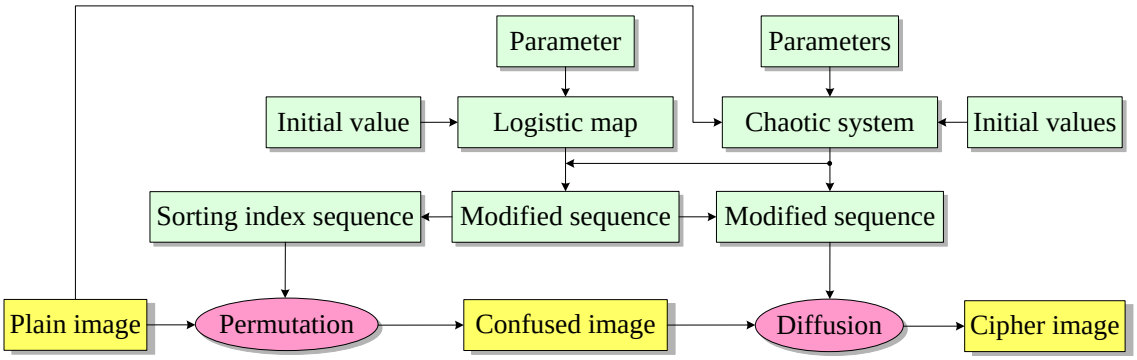

Fig. 7. Block diagram of the suggested image encryption scheme.

Step 1. Input the original image I with size $L=M\times N$. The L pixels are arranged as a one-dimensional array from the upper left to the lower right, which is represented by $P=(P_0, P_1, \dots, P_{L-1})$.

Step 2. Generate chaotic sequence $x=(x_1, x_2, \dots, x_L)$ by Logistic map (4) with parameter $\alpha \in (3.9, 4]$ and initial value x_0.

Step 3. Generate chaotic sequences $x_1=(x_{11}, x_{12}, \dots, x_{1L})$, $x_2=(x_{21}, x_{22}, \dots, x_{2L})$ and $x_3=(x_{31}, x_{32}, \dots, x_{3L})$ by the modified chaotic system (6) with parameter set (a, b, c, d, e, g) and initial condition (x_{10}, x_{20}, x_{30}).

$$\begin{cases} \dot{x}_1 = -ax_1 + bx_2 \\ \dot{x}_2 = cx_1 + dx_3 - (e+k)x_1x_3 \\ \dot{x}_3 = (e+k)x_1^2 - gx_3 \end{cases} \tag{6}$$

with $k=(k_1, k_2, \cdots, k_L)$, $k_i = \mathrm{mod}\left(\frac{P_i}{256\pi}\times 10^8,\ 256\right) \Big/ 256$.

Step 4. Generate chaotic sequences $y_1=(y_{11}, y_{12}, \dots, y_{1L})$, $y_2=(y_{21}, y_{22}, \dots, y_{2L})$ by

$$\begin{aligned} y_1 &= \tanh(e^x + x + x_1) \\ y_2 &= \mathrm{mod}\left((y_1 - abs(y_1))\times 10^{15},\ 256\right) \end{aligned} \tag{7}$$

Step 5. Sort sequence y_2 by ascending order to get the corresponding index sequence. According to the index sequence, number the one-dimensional pixels P and adjust pixel positions sequentially. Rearrange the scrambled pixels from left to right and top to bottom to get the confused image I_c.

Step 6. The chaotic sequences of system (6) are modified according to Golomb's theory, and obtain h_1, h_2, h_3.

Step 7. Generate one-dimensional chaotic key stream S with size L for diffusion process by the formulas

$$H = \mathrm{mod}\left((h_1 + h_2 - abs(h_1 + h_2))\times 10^{14} + (h_3 - abs(h_3))\times 10^{15} + (h_4 - abs(h_4))\times 10^{16},\ 256\right) \tag{8}$$

$$S = \mathrm{mod}\left(floor(H) \times 2^{16},\ 256 \right) \tag{9}$$

Step 8. Modify the pixel values of the confused image by performing forward diffusion and reverse diffusion, as below

$$I_d(i) = I_d(i-1) S(i) \oplus I_c(i) \tag{10}$$

$$I_d(i) = I_d(i+1) S(i) \oplus I_c(i) \tag{11}$$

The pixel values of image I_c are completely diffused by two round diffusions with the key stream S, thus we get the ciphered image I_d via the exclusive OR operation.

The decryption procedure is an inverse process of encryption procedure.

4. Experimental Results and Security Analysis

In this section, by adopting different standard images with 8-bit grayscale and size of 512×512, a series of numerical experiments have been conducted to check the security of the introduced cryptosystem. The initial value and parameter of Logistic map are chosen as α=4, x_0=0.02. The initial conditions and parameters of system (6) are fixed as x_{10}=0.02, x_{20}=0.1, x_{30}=0.03, a=10, b=6, c=28, d=1, e=1, g=5.

The experimental results for Lena image are shown in Fig.8. And several tests will be discussed to analyze the security level of the proposed encryption algorithm in the following subsections.

4.1. Key Space Analysis

Kerckhoff pointed out that the information system should be of security even if the system is publicly available except the key [34]. Therefore, a good encryption scheme should provide a large enough key space against any brute force attacks. In this encryption technique, the four initial values x_0, x_{10}, x_{20}, x_{30} and seven parameter values α, a, b, c, d, e, g for systems' setup can be viewed as secret keys. Accordingly, if the computational precision is 10^{-15}, the total key space size is bigger than $10^{15\times11}=10^{165}$, which is large enough to ensure a high security against brute-force attacks.

4.2. Sensitivity Analysis

A good encryption algorithm should be sensitive to the mismatches with respect to the original images or any secret keys on the whole cipher-image, for this reason, two common types of sensitivity analysis are executed in the following experiments.

4.2.1. Key sensitivity

The key sensitivity (KS) can be measured by calculating the Number of Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI), as the following formulas

$$NPCR = \frac{1}{L} \sum_{i=1}^{M} \sum_{j=1}^{N} Dif(i, j) \times 100\% \tag{12}$$

$$UACI = \frac{1}{L(2^Q - 1)} \sum_{i=1}^{M} \sum_{j=1}^{N} \left| I_{d1}(i, j) - I_{d2}(i, j) \right| \times 100\% \tag{13}$$

where $L=M\times N$ is the size of the cipher-image; Q is the number of bits, for images holding allocations of 8 bits/pixel of gray-scale, $2^Q-1=255$; I_{d1} and I_{d2} are two cipher-images corresponding to the right and mismatched keys; $Dif(i, j)$ denotes the difference between I_{d1} and I_{d2}.

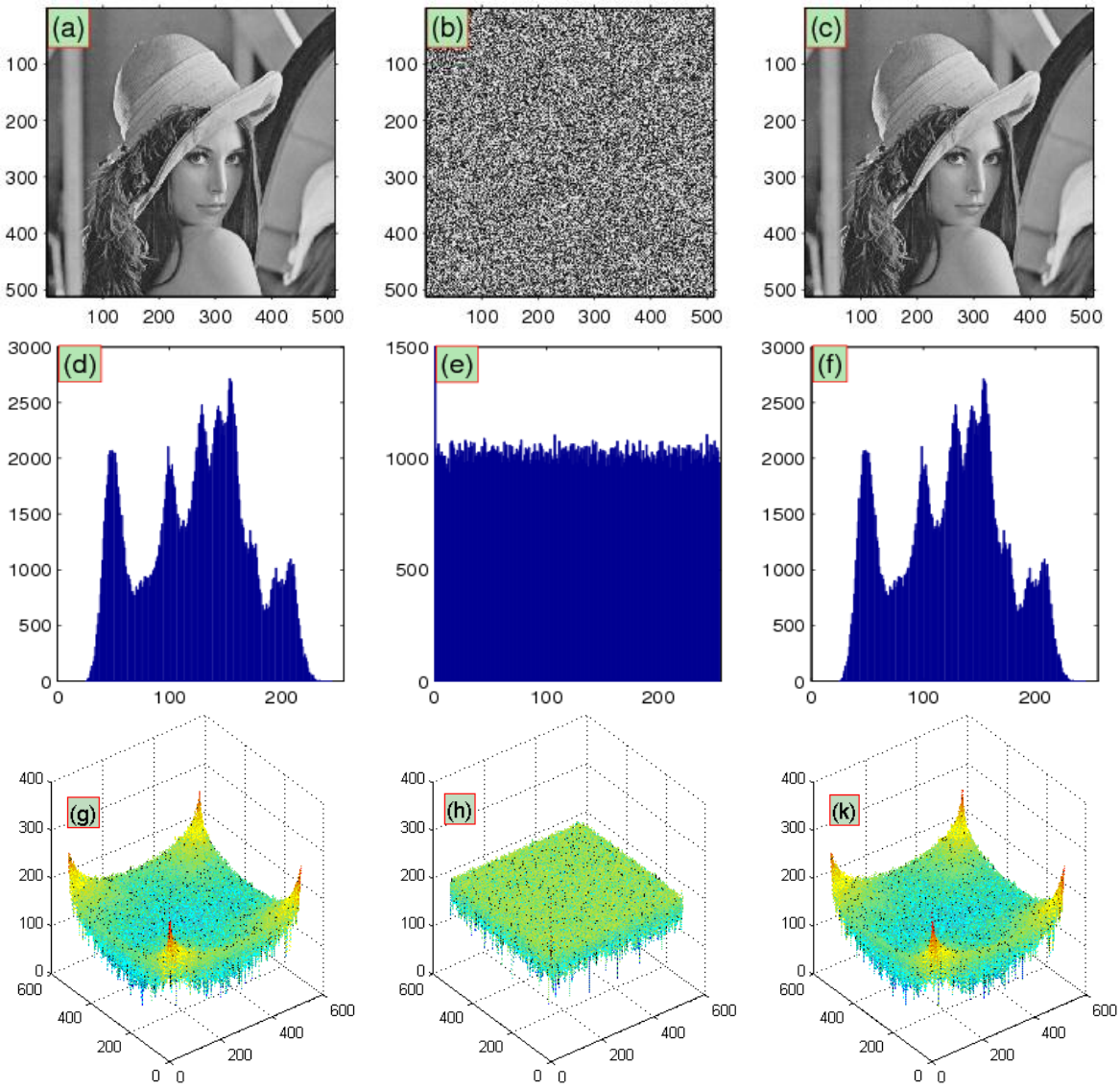

Fig. 8. (a) original Lena image; (b) Encrypted image; (c) Decrypted image; (d) Histogram of Lena image; (e) Histogram of the encrypted image; (f) Histogram of the decrypted image; (g) Amplitude spectrum of Lena image; (h) Amplitude spectrum of encrypted image; (k) Amplitude spectrum of decrypted image.

We first encrypt the standard images Lena, Scenery and Girla, using the right keys $\alpha=4, x_0=0.02$, $x_{10}=0.02, x_{20}=0.1, x_{30}=0.03$, $a=10, b=6, c=28, d=1, e=1, g=5$. Then we encrypt the same images with tiny change of keys. For all cryptographic systems, the idea results of NPCR and UACI are 100% and 33.33%, respectively. Therefore, experimental results of the proposed encryption are close to the expected estimate, as listed in Table 1. Thus, a high sensitivity of key is provided by the proposed scheme.

Table 1. Key Sensitivity for Different Standard Images

Slight changes of keys										Measures					
Logistic Map		The introduced chaotic system								NPCR/%			UACI/%		
$\Delta\alpha$	Δx_0	Δa	Δb	Δc	Δg	Δe	Δx_{10}	Δx_{20}	Δx_{30}	Lena	Scenery	Girla	Lena	Scenery	Girla
10^{-15}	0	0	0	0	0	0	0	0	0	99.6029	99.6071	99.6136	33.2705	33.5786	33.5705
0	10^{-15}	0	0	0	0	0	0	0	0	99.6235	99.5941	99.5964	33.4416	33.4426	33.5246
0	0	0.01	0	0	0	0	0	0	0	99.6254	99.6014	99.6178	33.2859	33.4857	33.5330
0	0	0	10^{-12}	0	0	0	0	0	0	99.6067	99.6048	99.5941	33.4125	33.5360	33.5056
0	0	0	0	0.01	0	0	0	0	0	99.6117	99.5880	99.5945	33.4434	33.3556	33.4177
0	0	0	0	0	10^{-12}	0	0	0	0	99.6109	99.6082	99.5861	33.4224	33.6465	33.4880
0	0	0	0	0	0	10^{-10}	0	0	0	99.6143	99.6456	99.5945	33.2362	33.4934	33.4980
0	0	0	0	0	0	0	10^{-15}	0	0	99.6315	99.6185	99.6067	33.5187	33.4595	33.6973
0	0	0	0	0	0	0	0	10^{-15}		99.5811	99.6075	99.6010	33.3366	33.3245	33.5061
0	0	0	0	0	0	0	0	0	10^{-15}	99.6277	99.5998	99.6155	33.2998	33.5342	33.6493

4.2.2. Plaintext sensitivity

The encryption technique can effectively resist differential attack if that a slight change in the plain-image makes the cipher-image vary greatly, which can also be tested by calculating the values of NPCR and UACI. For the plaintext sensitivity (PS), I_{d1} and I_{d2} are respectively the cipher-image before and after the change of one pixel of the plain image. The experimental results for the standard images Lena, Scenery and Girla are depicted in Table 2. It is clear that the values of NPCR and UACI remain in the vicinity of the expected values, thus the proposed scheme is extreme sensitive with respect to the little change of plain-image and can effectively resist differential attack.

Table 2. Plaintext Sensitivity for Different Standard Images

NPCR/%			UACI/%		
Lena	Scenery	Girla	Lena	Scenery	Girla
99.6174	99.6044	99.6361	33.4027	33.5370	33.5818

4.3. Statistical Analysis

According to Shannon's theory, the encryption process should prevent the cipher-image from suffering any statistical attack [3], [22]. There is strong correlation among adjacent pixels for plain images. Statistical analysis is mainly to observe the confusion and diffusion properties of the encrypted image and the difference with the original image. In order to prove the security of the proposed cryptographic scheme, several statistical tests such as histogram, spectrum, information entropy, correlation are performed in this subsection.

4.3.1. Histograms of image

The histogram reveals the statistical characteristics of image and the distribution information of pixel values. Histograms of the original Lena image and its encrypted and decrypted images are shown in Fig. 8 (d-f). It's known that the histogram of encrypted image distributes nearly uniform and completely differ from the histograms of the original and decrypted images. Hence, the histogram of encrypted image does not reveal any statistical information of the original image. Thus, it is difficult for attackers to recover the plain image from statistical feature of ciphered image.

4.3.2. Spectrums of image

Similar to the histogram of image, the spectrum also reflects the distribution of the corresponding image in frequency domain. The distributions of the amplitude spectrum for the original Lena image and the corresponding encrypted and decrypted images are shown in Fig. 8 (g-k). It can be seen that there exists ridges and valleys in Fig. 8 (g) and Fig. 8 (k), but the amplitude spectrum of the encrypted image in Fig. 8 (h) is fairly uniform in the whole frequency distribution. What's more, the amplitude spectrum of the decrypted image is almost equivalent to the original one. Therefore, the proposed technique is strong enough to resist any statistical attack.

4.3.3. Information entropy

Information entropy is an important measure of the uncertainty of randomness. Let $p(s_i)$ be the probability of information source s_i, and N is the number of bits for each information symbol s_i. The information entropy can be calculated as

$$H(s) = -\sum_{i=1}^{2^N-1} p(s_i)\log_2 p(s_i) \tag{12}$$

The entropy of experimental result for the standard images Lena, Scenery and Girla are 7.9972, 7.9973, 7.9973, respectively. Compared with the algorithms from Refs. [1, 4], the obtained result for the cipher-image Lena is more close to the ideal value 8. Therefore, the probability of information leakage of the proposed scheme is very little and the ciphered image is secure against any kind of entropy attack.

4.3.4. Correlations of two adjacent pixels

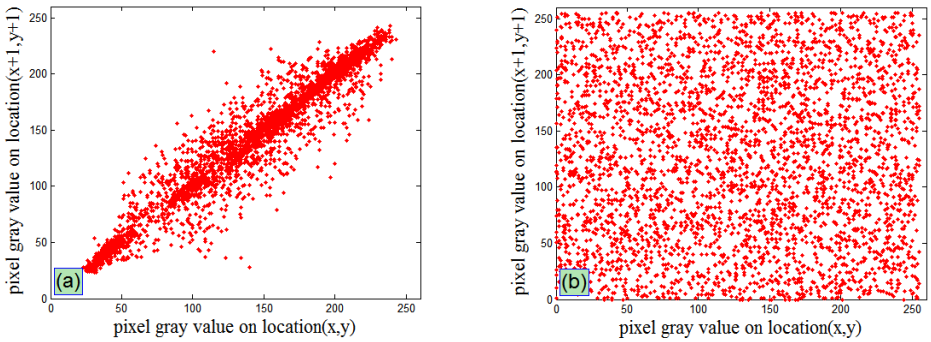

Fig. 9. (a) Correlations in the plain-image Lena; (b) Correlations in the cipher-image Lena.

A secure encryption scheme should reduce the correlation between adjacent image pixels to withstand statistical attack. Thus, we randomly select 10,000 pairs of two adjacent pixels in horizontal,

vertical and diagonal directions from the original image and the cipher-image to test the correlation. The correlation coefficient R_{xy} will be calculated by using the following equation

$$R_{xy} = \mathrm{cov}(x, y) / \sqrt{D(x)D(y)} \tag{13}$$

with $\mathrm{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)\left(y_i - E(y)\right)$, $D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2$, $E(x) = \frac{1}{N}\sum_{i=1}^{N}x_i$, where x and y are gray-scale values of the adjacent pixels in the image.

Fig. 9 shows the correlation distribution of two diagonally adjacent pixels in the original Lena image and that in the ciphered image, with the corresponding correlation coefficients 0.9739 and 0.0014. The test results for different standard images are concluded in Table 3. From Table 3, it can be seen that the proposed scheme approximates zero correlation, revealing high-level security.

Table 3. Correlation Coefficients for the Standard Images Girla, Scenery and Lena

Direction	Plain-image			Cipher-image		
	Lena	Scenery	Girla	Lena	Scenery	Girla
Horizontal	0.9858	0.9690	0.9686	–0.0090	0.0011	–0.0035
Vertical	0.9904	0.9832	0.9889	–0.0019	–0.0012	0.0036
Diagonal	0.9739	0.9759	0.9544	0.0014	0.0012	0.00004

4.4. Noise Attack Analysis

Fig. 10. Decrypted images disturbed by salt-and-pepper noise with (a) R=0.1 and (b) R=0.4; decrypted images disturbed by Gaussian noise with (c) R=0.1 and (d) R=0.4.

The image is often corrupted by different noises in processing and transmission. To analyze the immunity to different noise of this scheme, we add the salt-and-pepper noise and Gaussian noise to the ciphered image of Lena in the way: $I'_d(x, y) = I_d(x, y)(1+RN(x, y))$, in which $I_d(x, y)$ and $I'_d(x, y)$ denote the ciphertext and the noise-disturbed ciphertext respectively, $N(x, y)$ is the salt-and-pepper noise or

Gaussian noise, *R* denotes the noise strength. The decryption process is performed with correct keys except that the ciphertext is disturbed by different noises. Fig. 10 (a) and (b) show the results of decrypting ciphertext disturbed by salt-and-pepper noise when *R* is set to 0.1 and 0.4. Fig. 10 (c) and (d) show the results of decrypting ciphertext disturbed by Gaussian noise when *R* is set to 0.1 and 0.4. As we know that the decrypted plain images become more fuzzy with a larger strength *R*, but the main information of the plain images can be recognized. Therefore, the proposed encryption scheme can resist noise attack to some extent.

4.5. Occlusion Attack Analysis

The image is mostly also damaged by occlusion in processing and transmission. We perform the decryption process with all correct keys except that the encrypted image is occluded partly. Fig. 11 (a) displays the occluded ciphertext which is cut by 25% at the central and Fig. 11(b) depicts the recovered plain image. Fig. 11(c) displays the occluded ciphertext cut by 50% at the lower-left corner and top-right corner, and Fig. 11 (d) shows the decrypted image. From the recovered images, it's found that the content of the original image can be identified visually. Therefore, the introduced encryption scheme is proved to be immune to occlusion attack.

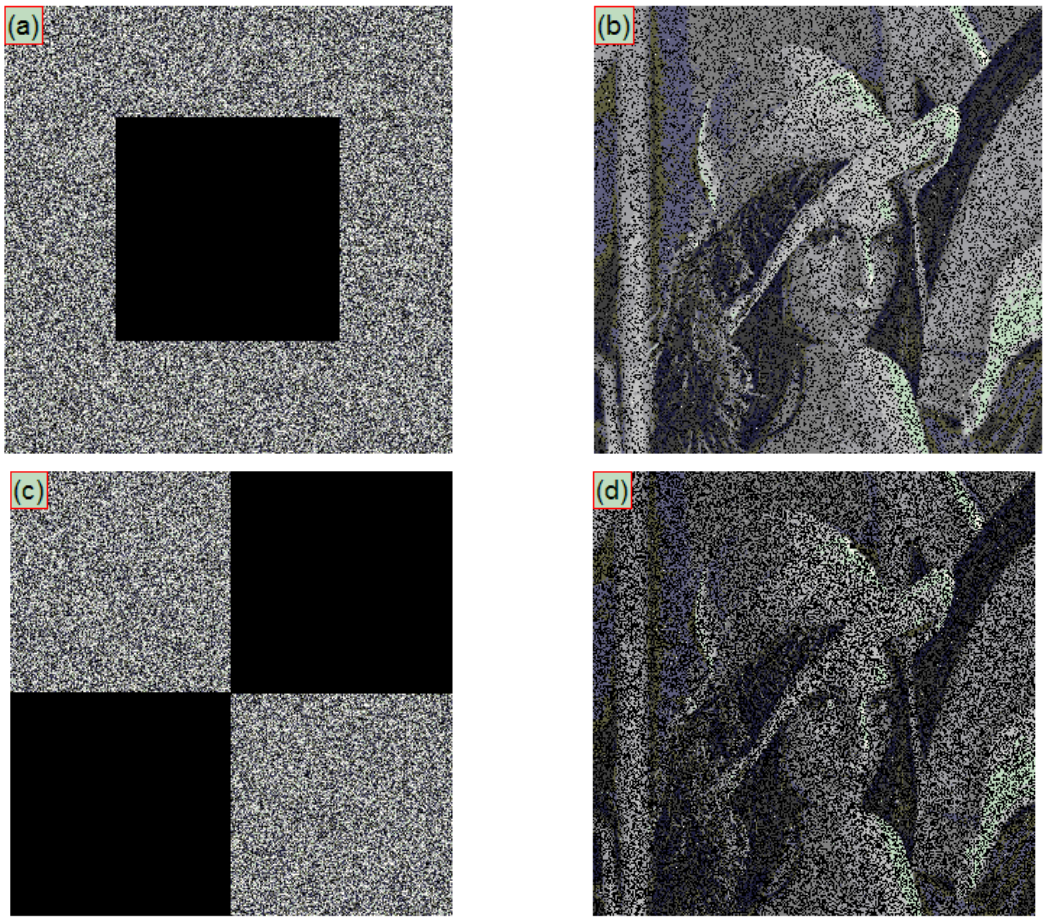

Fig. 11. (a) Ciphertext with 25% occlusion and (b) the corresponding decrypted image; (c) ciphertext with 50% occlusion and (d) the corresponding decrypted image.

5. Discussion and Conclusion

A practical scheme for image encryption includes not only bit confusion and diffusion, but also computational unpredictability and sensitivity to keys and plain text, which can be commendably catered by chaotic systems. And the chaotic system with amplitude parameter can execute a possible realization for one-time pad since it can provide enough key than the message. In this paper, we introduce a three-dimensional chaotic system by analyzing basic dynamical properties, particularly including amplitude modulation. And to study its application in multi-media security, an image encryption scheme is presented based on the permutation-diffusion architecture. The proposed cryptosystem can ensure high security by mainly employing the following two innovations: (a) The chaotic sequences for permutation and diffusion are simultaneously generated from Logistic map and new chaotic system, thus the change of one of secret keys will affect both the permutation module and the diffusion procedure. Moreover, the chaotic key stream for diffusion process is modified based on the properties of ideal pseudo-random sequence. (b) The plaintext sequence and amplitude parameter are employed to generate key stream based on the idea of OTP, which will cause a significant variation in the key stream if we choose different pixel of plain-image, different parameter or different initial condition of chaotic systems. Therefore, this procedure can effectively resist known-plaintext attack and chosen-plaintext attack. And, consequently, it can also withstand other conventional attacks. Finally, we have carried out key space analysis, key sensitivity analysis and statistical analysis to demonstrate the security of the introduced image encryption scheme.

Acknowledgment

This research was supported by the NNSF of China under Grant No. 11475060; the Research Foundation of Education Bureau of Hunan Province of China under Grant No. 16B113; the China Postdoctoral Science Foundation under Grant No. 2016M590745 and Hunan Provincial Natural Science Foundation of China under Grant 2016JJ4036.

References

[1] Zhu C. (2012). A novel image encryption scheme based on improved hyperchaotic sequences. *Opt Commun*, *285*, 29-37.

[2] Del, R. A. M., & Sánchez, G. R. (2015). An image encryption algorithm based on 3D cellular automata and chaotic maps. *Int J Mod Phys C*.

[3] Alvarez, G., & Li, S. (2006). Some basic cryptographic requirements for chaos-based cryptosystems. *Int J Bifur Chaos*.

[4] Luo, Y., Du, M., & Liu, J. (2015). A symmetrical image encryption scheme in wavelet and time domain. *Commun Nonlinear Sci Numer Simul*.

[5] Zhou, Y., Bao, L., & Chen, C. L. P. (2014). A new 1D chaotic system for image encryption. *Signal Process*, *97*, 172-182.

[6] Wang, X. Y., Gu, S. X., & Zhang, Y. Q. (2015). Novel image encryption algorithm based on cycle shift and chaotic system, *Opt Laser Eng*, *68*, 126-134.

[7] Liu, S., Guo, C., & Sheridan, J. T. (2014). A review of optical image encryption techniques. *Opt Laser Technol*, *57*, 327-342.

[8] Muthukumar, P., Balasubramaniam, P., & Ratnavelu, K. (2014). Synchronization and an application of a novel fractional order King Cobra chaotic system. *Chaos*.

[9] Yao, W., Zhang, X., Zheng, Z., & Qiu, W. (2015). A colour image encryption algorithm using 4-pixel Feistel structure and multiple chaotic systems. *Nonlinear Dyn*, *81*, 151-168.

[10] Fridrich, J. (1998). Symmetric ciphers based on two-dimensional chaotic maps. *Int J Bifur Chaos*.

[11] Zhang, W., Wong, K., Yu, H., & Zhu, Z. (2013).A symmetric color image encryption algorithm using the intrinsic features of bit distributions. *Commun Nonlinear Sci Numer Simul*.

[12] Zhang, Y., & Xiao, D. (2014). An image encryption scheme based on rotation matrix bit-level permutation and block diffusion. *Commun Nonlinear Sci Numer Simul.*

[13] Lin, Z. S., Yu, S. M., Lü, J. H., Cai, S. T., & Chen, G. R. (2014). Design and Arm-embedded implementation of a chaotic map-based real-time secure video communication system. *IEEE Trans. Circuits Syst. Video Technol*, *99*, 1051-8215.

[14] Kong, D., & Shen, X. (2014). Multiple-image encryption based on optical wavelet transform and multichannel fractional Fourier transform. *Opt Laser Technol*, *57*, 343-349.

[15] Zhong, Z., Chang, J., Shan, M. G., & Hao, B. G. (2012). Fractional fourier-domain random encoding and pixel scrambling technique for double image encryption. *Opt Commun*.

[16] Xiang, T., Wong, K., & Liao, X. (2007). Selective image encryption using a spatiotemporal chaotic system. *Chaos*.

[17] Solak, E., Cokal, C., Yildiz, O., & Biyikoglu T. (2010). Cryptanalysis of Fridrich's chaotic image encryption. *Int J Bifur Chaos*.

[18] Rhouma, R., & Safya, B. (2017). On the security of a spatiotemporal chaotic cryptosystem. *Chaos*, *17*, 033117.

[19] Cokal, C., & Solak, E. (2009). Cryptanalysis of a chaos-based image encryption algorithm. *Phys Lett A*, 373, 1357-1360.

[20] Zhang, Y., & Xiao, D. (2013). Cryptanalysis of S-box-only chaotic image ciphers against chosen plaintext *attack. Nonlinear Dyn*, 72, 751-756.

[21] Zhu, C., Xu, S., & Hu, Y., *et al.* (2014). Breaking a novel image encryption scheme based on Brownian motion and PWLCM chaotic system. *Nonlinear Dyn*, *79*, 1511-1518.

[22] Shannon, C. E. (1948). A mathematical theory of communication. *Bell Syst Tech J*., *27*, 379-423.

[23] Gehani, A., Labean, T., & Reif, J. (2003). DNA-based cryptography. *Lecture Notes in Computer Science*, *2950*, 233-249.

[24] Brandão, F., & Oppenheim, J. (2012).Quantum one-time pad in the presence of an eavesdropper. *Phys Rev Lett*, *108*, 040504.

[25] Nagaraj, N. (2012). One-time pad as a nonlinear dynamical system. *Commun Nonlinear Sci Numer Simul*, *17*, 4029-4036.

[26] Yang, Q., Zhang, K., & Chen, G. (2009). A modified generalized Lorenz-type system and its canonical form. *Int J Bifur Chaos*, *19*, 1931-1949.

[27] Chen, G., & Ueta, T. (1999). Yet another chaotic attractor. *Int J Bifur Chaos*, *9*, 1465-1466.

[28] Lainscsek, C. (2012). A class of Lorenz-like systems. *Chaos*, *22*, 013126.

[29] Lü, J., & Chen, G. (2002). A new chaotic attractor coined. *Int J Bifur Chaos*, *12*, 659-661.

[30] Wei, Z. (2011).Dynamical behaviors of a chaotic system with no equilibria. *Phys Lett A*, *376*, 102-108.

[31] Li, C., Wu, L., Li, H. M., & Tong, Y. N. (2013). A novel chaotic system and its topological horseshoe. *Nonlinear Anal Model Control*, *18*, 66-77.

[32] Li, C., Su, K., & Wu, L. (2013). Adaptive sliding mode control for synchronization of a fractional-order chaotic system. *J Comput Nonlinear Dynam*, *8*, 031005.

[33] Li, C., & Zhang, J. (2016). Synchronization of a fractional-order chaotic system using finite time input-to-state stability. *Int J Syst Sci*., *47(10)*, 2440-2448.

[34] Kerckhoffs, A. (1978). *La Cryptographie Militaire*. University Microfilms.

Chunlai Li received his master of engineering from the College of Electronic Engineering, Guangxi Normal University, Guilin, China in 2006. He gained his PhD from the College of Automation, Guangdong University of Technology, Guangzhou, China in 2012. He is currently a professor in the College of Physics and Electronics at Hunan Institute of Science and Technology. His current research interests include stable operation of power system, chaos control, chaos dynamics and chaos application.

Wenhua Hai started the college physics teaching and research work from January 1982 and was promoted to professor in 1994. He was a doctoral supervisor since 2001 in Hunan Normal University. He is the author of more than 140 papers in SCI journals, including 32 papers published in the international authoritative journal Phys. Rev. His current research interests include chaos dynamics and chaos control in classical chaotic system, the atomic and molecular system and the condensed matter.