IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 17, 2019, accepted August 15, 2019, date of publication August 23, 2019, date of current version September 5, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2937126

Dynamical Analysis of a Novel Complex Chaotic System and Application in Image Diffusion

FEIFEI YANG[1], JUN MOU[1], HUIZHEN YAN[1], AND JINHUA HU[2]
[1]School of Information Science and Engineering, Dalian Polytechnic University, Dalian 116034, China
[2]Liaoning Provincial Key Laboratory of Ecological Textiles, National Supercritical Fluid Waterless Dyeing Technology Research and Development Center, Dalian Polytechnic University, Dalian 116034, China

Corresponding author: Jun Mou (moujun@csu.edu.cn)

This work was supported in part by the Basic Scientific Research Projects of Colleges and Universities of Liaoning Province under Grant 2017J045, and in part by the Provincial Natural Science Foundation of Liaoning under Grant 20170540060.

ABSTRACT In this paper, a novel complex chaotic system is constructed. The characteristics of new complex chaotic system are analyzed by symmetric, dissipative and stability, then dynamical performances studied using bifurcation diagram, Lyapunov exponent spectrum and complexity. On the basis of this, an image diffusion algorithm is proposed based on the model of law of gravity. Security performances of the proposed algorithm are researched through the key space, statistics, information entropy, noise attack. The experimental results illustrates that the novel complex chaotic system has abundant dynamical behaviors and large parameters range, the security analysis shows that the proposed image encryption algorithm possess higher security features. Therefore, the research will provide theoretical guidance and experimental basis for chaotic secure communication and information security.

INDEX TERMS Novel complex chaotic system, image diffusion, model of law of gravity.

I. INTRODUCTION

At present, the research of chaos system mainly includes the most basic chaotic system model, the unknown parameter chaotic system, fractional-order chaotic system, time delay chaotic system, pulsed chaotic system and complex chaotic system model etc. Specially, the development of complex chaotic system started relatively late. In 1982, Fowler et al. [1], [2], [3] proposed Lorenz complex chaotic equations. Since then, the characteristics of complex chaotic systems have attracted the attention of scholars.

In recent years, the study of complex chaotic systems has been growing [4]–[15]. For example, Mahmoud *et al.* [4] presented a complex hyperchaotic Chen system and analyzed its dynamical performances. Dynamic characteristics and synchronization of complex Lorenz system is analyzed in [5]. Synchronization and control of hyperchaotic complex Lorenz systems were studied by Mahmoud and Mahmoud [6]. Luo *et al.* [7] analyzed the dynamic characteristics and synchronization algorithm of the fractional-order complex system. Liu and Zhang [8] proposed a synchronization algorithm of complex chaotic based on complex function projective. A new hyperchaotic complex Lü-like system based on generalized combination complex synchronization algorithm was analyzed by Jiang and Liu [9]. Liu *et al.* [10] presented a synchronization of complex chaotic systems with uncertain complex parameters by adaptive complex modified projective. Based on the above research background, a new complex chaotic system is constructed in this paper and it is implemented in image encryption algorithm.

Image encryption is an important aspect of chaos application. Up to now, a variety of image encryption algorithms based on chaotic system are proposed [16]–[42]. Such as, A new image encryption algorithm by complex chaotic map was designed by Liu *et al.* [16]. Wang *et al.* [17] designed a novel color image encryption scheme based on two complex chaotic systems. Complex chaotic system was used to color image encryption schemes in [18], [19]. Chai *et al.* [21], [20] proposed image encryption algorithm through chaotic system and DNA. A new image encryption scheme based on chaotic map was presented by Wu *et al.* [22]. Zhu and Sun [23] analyzed and improved an image encryption algorithm by using chaotic mat map. Medical image encryption scheme through quantum chaotic was proposed in [24]. Zhang and Wang [25] introduced a novel image encryption algorithm through chaotic system and elliptical curve. An image encryption scheme based on 2D chaotic map and Hash function was studied in [26]. Wang and his research team proposed [27] a novel

The associate editor coordinating the review of this article and approving it for publication was Di He.

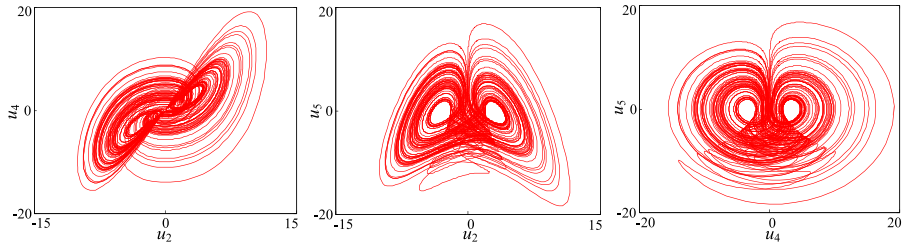


FIGURE 1. Phase portraits of complex chaotic system: (a) u_2-u_4 plane; (b) u_2-u_5 plane; (c) u_4-u_5 plane.

fast image encryption scheme by chaotic system. In addition, there are some other image encryption algorithms. For instance, image encryption algorithm based on hash function diffusion operation in [28]. Wang *et al.* [29] described a new image encryption algorithm based on hash function and cyclic shift. An novel image encryption scheme through bit-level was presented in [30]. In view of the image encryption algorithm [27]–[30] has low security performances. Therefore, on the basis of above research background, in this paper, a new complex chaotic system is constructed, and propose a novel image diffusion algorithm based on complex chaotic system and the model of law of gravity.

The rest of this paper is organized as follows. Mathematical model of the novel complex chaotic system is constructed in section 2. In section 3, dynamical characteristics of the novel complex chaotic system are analyzed. In section 4, a new image diffusion algorithm based on complex chaotic and the model of law of gravity is given. Performances of the proposed algorithm are analyzed in section 5. Finally, some main conclusions are summarized in section 6.

II. MATHEMATICAL MODEL OF THE NOVEL COMPLEX CHAOTIC SYSTEM

Recently, a new 4D chaotic system based on Sprott B system was proposed by Long and Mei [43]. The dynamical equation of new 4D chaotic system is

$$\begin{cases} \dot{x} = a(y - x) + w \\ \dot{y} = xz \\ \dot{z} = b - xy \\ \dot{w} = -cw + xz, \end{cases} \tag{1}$$

when $a = 4$, $b = 9$, $c = 5$, the new 4D system have four Lyapunov exponent, but only has a positive. Therefore, the system (1) is chaotic system.

In this paper, on the basis of the 4D chaotic system (1), a new complex chaotic system is obtained, and its forms are as follows:

$$\begin{cases} \dot{x} = a(y - x) + w \\ \dot{y} = xz \\ \dot{z} = b - \frac{1}{2}(\bar{x}y + x\bar{y}) \\ \dot{w} = -cw + \frac{1}{2}(\bar{x}z + x\bar{z}), \end{cases} \tag{2}$$

where a, b and c represent the system parameters. $x = u_1 + iu_2$ and $y = u_3 + iu_4$ are complex variable, i is imaginary unit. $z = u_5$ and $w = u_6$ means real variable. The real form for the complex chaotic system (2) is obtained by separate the imaginary part from complex system. In this case, the system (2) is expressed as

$$\begin{cases} \dot{u}_1 = a(u_3 - u_1) + u_6 \\ \dot{u}_2 = a(u_4 - u_2) \\ \dot{u}_3 = u_1u_5 \\ \dot{u}_4 = u_2u_5 \\ \dot{u}_5 = b - u_1u_3 - u_2u_4 \\ \dot{u}_6 = -cu_6 + u_1u_5, \end{cases} \tag{3}$$

where a, b and c represent the system parameters. $u_1 \ldots u_6$ are state variable.

Setting the system parameters $a = 4$, $b = 9$, $c = 5$, initial values $x = 1 + i$, $y = 1 + i$, $z = 1$ and $w = 1$. The phase portraits of complex chaotic system (3) through means of the numerical simulation are shown in Fig. 1. The Lyapunov exponents are obtained through Wolf method, here, $L_1 = 0.5264$, $L_2 = 0$, $L_3 = -0.0903$, $L_4 = -3.9910$, $L_5 = -4.4889$, $L_6 = -4.9593$. In addition, the Lyapunov dimension of the system is $D_L = 4.8341$. Therefore the system is chaotic.

III. CHARACTERISTIC ANALYSIS OF THE NOVEL COMPLEX CHAOTIC SYSTEM

A. SYMMETRY AND INVARIANCE

The system (3) is symmetric and invariant under transformation $(u_1, u_2, u_3, u_4, u_5, u_6) \rightarrow (-u_1, -u_2, -u_3, -u_4, u_5, -u_6)$. Therefore, the system (3) is symmetric about u_5-axis. In addition, the symmetry is true for all system parameters a, b and c.

B. DISSIPATION

According to system (3), we get

$$\nabla V = \frac{\partial \dot{u}_1}{u_1} + \frac{\partial \dot{u}_2}{u_2} + \frac{\partial \dot{u}_3}{u_3} + \frac{\partial \dot{u}_4}{u_4} + \frac{\partial \dot{u}_5}{u_5} + \frac{\partial \dot{u}_6}{u_6} = -2a - c \tag{4}$$

Hence, when system parameter $a > 0$ and $c > 0$, the system is dissipative.

C. EQUILIBRIUM AND STABILITY

Setting $a(u_3\text{-}u_1)+u_6=0, a(u_4\text{-}u_2)=0, u_5u_1=0, u_5u_2=0, b\text{-}u_1u_3\text{-}u_4u_2=0, -cu_6+u_5u_1=0$. The equilibrium points of system (3) is

$$\begin{cases} E_{1,2}=(\alpha, \pm\sqrt{-\alpha^2+b}, \alpha, \pm\sqrt{-\alpha^2+b}, 0, 0) \\ E_{3,4}=(\pm\sqrt{b}, 0, \pm\sqrt{b}, 0, 0, 0) \\ E_{5,6}=(0, \pm\sqrt{b}, 0, \pm\sqrt{b}, 0, 0) \end{cases} \tag{5}$$

where α is any real number. Hence, the system (3) has an infinite of equilibrium points. The system (3) is linearized near the equilibrium points, and then Jacobian matrix of system (3) is obtained as

$$J=\begin{bmatrix} -a & 0 & a & 0 & 0 & 1 \\ 0 & -a & 0 & a & 0 & 0 \\ u_5 & 0 & 0 & 0 & u_1 & 0 \\ 0 & u_5 & 0 & 0 & u_2 & 0 \\ -u_3 & -u_4 & -u_1 & -u_2 & 0 & 0 \\ u_5 & 0 & 0 & 0 & u_1 & -c \end{bmatrix} \tag{6}$$

For the equilibrium point E_1, the corresponding Jacobian matrix $J\ (E_1)$ is

$$J(E_1)=\begin{bmatrix} -a & 0 & a & 0 & 0 & 1 \\ 0 & -a & 0 & a & 0 & 0 \\ 0 & 0 & 0 & 0 & \alpha & 0 \\ 0 & 0 & 0 & 0 & \sqrt{-\alpha^2+b} & 0 \\ -\alpha & -\sqrt{-\alpha^2+b} & -\alpha & -\sqrt{-\alpha^2+b} & 0 & 0 \\ 0 & 0 & 0 & 0 & \alpha & -c \end{bmatrix} \tag{7}$$

Eq. (7) parameters are assumed $\alpha=2, a=4, b=9, c=5$. The eigenvalues are obtained by calculation, here, $\lambda_1=0.3593+2.8977i$, $\lambda_2=-0.3593-2.8977i$, $\lambda_3=-5.2545$, $\lambda_4=-4$, $\lambda_5=-4.4663$, $\lambda_6=0$.

The corresponding Jacobian matrix $J\ (E_2)$ of the equilibrium point E_2 as

$$J(E_2)=\begin{bmatrix} -a & 0 & a & 0 & 0 & 1 \\ 0 & -a & 0 & a & 0 & 0 \\ 0 & 0 & 0 & 0 & \alpha & 0 \\ 0 & 0 & 0 & 0 & -\sqrt{-\alpha^2+b} & 0 \\ -\alpha & \sqrt{-\alpha^2+b} & -\alpha & \sqrt{-\alpha^2+b} & 0 & 0 \\ 0 & 0 & 0 & 0 & \alpha & -c \end{bmatrix} \tag{8}$$

Setting Eq. (8) parameters $\alpha=2, a=4, b=9, c=5$. The eigenvalues are $\lambda_1=0.5120+3.7854i$, $\lambda_2=-0.5120-3.7854i$, $\lambda_3=-5.6890$, $\lambda_4=-4$, $\lambda_5=-4.3430$, $\lambda_6=0$.

For the equilibrium point E_3, the corresponding Jacobian matrix $J\ (E_3)$ is expressed by

$$J(E_3)=\begin{bmatrix} -a & 0 & a & 0 & 0 & 1 \\ 0 & -a & 0 & a & 0 & 0 \\ 0 & 0 & 0 & 0 & \sqrt{b} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ -\sqrt{b} & 0 & -\sqrt{b} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \sqrt{b} & -c \end{bmatrix} \tag{9}$$

For the Eq. (9), when $a=4, b=9, c=5$. The eigenvalues are obtained by calculation, here $\lambda_1=0.5+3.8406i$, $\lambda_2=0.5-3.8406i$, $\lambda_3=-6$, $\lambda_4=-4$, $\lambda_5=-4$, $\lambda_6=0$.

Similarly, Jacobian matrix $J\ (E_4)$ of the equilibrium point E_4 is

$$J(E_4)=\begin{bmatrix} -a & 0 & a & 0 & 0 & 1 \\ 0 & -a & 0 & a & 0 & 0 \\ 0 & 0 & 0 & 0 & -\sqrt{b} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ \sqrt{b} & 0 & \sqrt{b} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -\sqrt{b} & -c \end{bmatrix} \tag{10}$$

Assumption $a=4, b=9, c=5$. Get the eigenvalues are $\lambda_1=0.5+3.8406i$, $\lambda_2=0.5-3.8406i$, $\lambda_3=-6$, $\lambda_4=-4$, $\lambda_5=-4$, $\lambda_6=0$.

For the equilibrium point E_5, the corresponding Jacobian matrix $J\ (E_5)$ as

$$J(E_5)=\begin{bmatrix} -a & 0 & a & 0 & 0 & 1 \\ 0 & -a & 0 & a & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \sqrt{b} & 0 \\ 0 & -\sqrt{b} & 0 & -\sqrt{b} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -c \end{bmatrix} \tag{11}$$

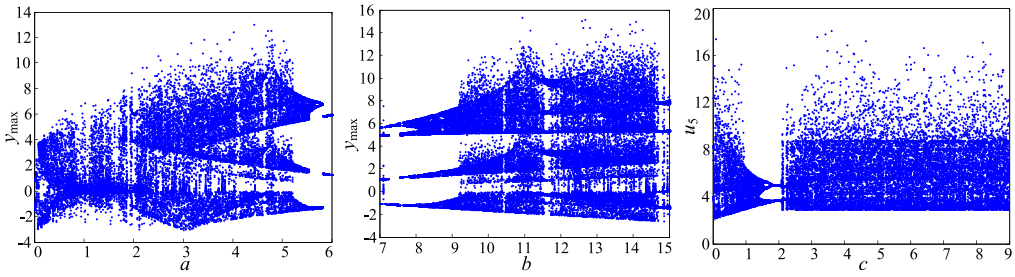
In the same way $a=4, b=9, c=5$. The eigenvalues are obtained by calculation, where $\lambda_1=0.5225+3.7415i$, $\lambda_2=0.5225-3.7415i$, $\lambda_3=-5.0049$, $\lambda_4=-4$, $\lambda_5=0$, $\lambda_6=-5$.

The corresponding Jacobian matrix $J\ (E_6)$ of the equilibrium point E_6 is expressed by

$$J(E_6)=\begin{bmatrix} -a & 0 & a & 0 & 0 & 1 \\ 0 & -a & 0 & a & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -\sqrt{b} & 0 \\ 0 & \sqrt{b} & 0 & \sqrt{b} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -c \end{bmatrix} \tag{12}$$

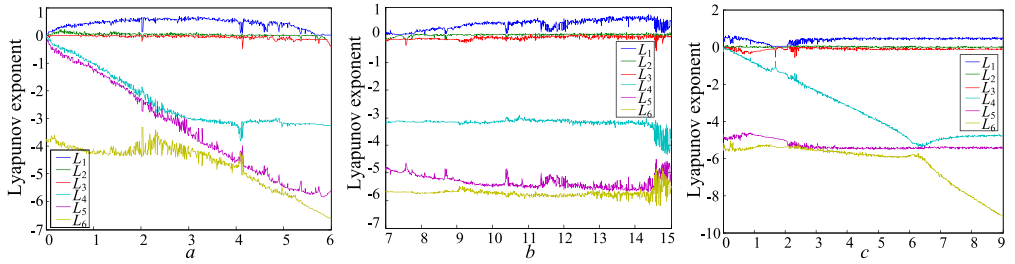
Jacobian matrix $J\ (E_6)$ parameters $a=4, b=9, c=5$. The corresponding eigenvalues are $\lambda_1=0.5225+3.7415i$, $\lambda_2=0.5225-3.7415i$, $\lambda_3=-5.0049$, $\lambda_4=-4$, $\lambda_5=0$, $\lambda_6=-5$.

Therefore, the system (6) for all the equilibrium points is unstable under $a=4, b=9, c=5$ by the above analysis.



(a) (b) (c)

FIGURE 2. Bifurcation diagrams with different parameters: (a) $b = 9$, $c = 5$, $a \in [0,6]$; (b) $a = 4$, $c = 5$, $b \in [7,15]$; (c) $b = 9$, $a = 4$, $c \in [0,9]$.



(a) (b) (c)

FIGURE 3. Lyapunov exponent spectrums with different parameters: (a) $b = 9$, $c = 5$, $a \in [0,6]$; (b) $a = 4$, $c = 5$, $b \in [7,15]$; (c) $b = 9$, $a = 4$, $c \in [0,9]$.

IV. DYNAMICAL ANALYSIS OF THE NOVEL COMPLEX CHAOTIC SYSTEM

According to characteristic analysis of the novel complex chaotic system in section III, we can see that the system has abundant dynamic performances. To further study the nonlinear dynamic characteristics of the system, the bifurcation diagrams, Lyapunov exponent spectrums and complexity under different parameters are analyzed.

A. BIFURCATION DIAGRAM AND LYAPUNOV EXPONENT SPECTRUM ANALYSIS

Fix the parameters $b = 9$, $c = 5$, make the parameter $a \in [0,6]$, the time step is 0.01 s, the maximum simulation time is 200, and the initial value of the new system are $(u_1, u_2, u_3, u_4, u_5, u_6) = (1, 1, 1, 1, 1, 1)$. In this case, the bifurcation diagram and Lyapunov exponent spectrum are shown in Fig. 2(a) and Fig. 3(a). Setting $a = 4$, $b \in [7,15]$, and keeping other parameter values, and the corresponding of bifurcation diagram and Lyapunov exponent spectrum are demonstrated in Fig. 2(b) and Fig. 3(b). Moreover, setting $b = 9$, $c \in [0,9]$, and keeping other parameter values, then the corresponding bifurcation diagrams and Lyapunov exponent spectrums are shown in Fig. 2(c) and Fig. 3(c). The dynamical performances of the system (3) with different parameter values are listed in Table. 1. Obviously, dynamical characteristics of the novel system are rich.

B. COMPLEXITY ANALYSIS

Complexity is an important index to measure the randomness of signal sequences. Generally speaking, the bigger the sequence complexity value is, the better the randomness of the sequence is. For the complexity of chaotic system refers to adopting the correlation algorithm to measure the degree of chaos sequence approaching random sequence. The higher the complexity value is, the closer the sequence is to random sequence, and the higher the corresponding security is. Complexity of chaotic sequence includes the behavioral complexity and structural complexity. In this section, complexity of the novel complex chaotic system is analyzed by Spectral Entropy (SE), Lempl-Ziv (LZ) behavioral complexity and C0 structural complexity algorithms. On the basis of the above system parameter values and initial values, the complexity of system (3) for the system parameter a, b and c are shown in Fig. 4, Fig. 5 and Fig. 6. The system is period state when complexity value relatively small. The system is chaotic when complexity value bigger. Therefore, the results of complexity analysis illustrates that the complexity value corresponds exactly to the randomness of the system.

Furthermore, chaos diagrams of complex chaotic system (3) are studied. Set the parameters $b = 9$, $a \in [0,6]$, $c \in [0,9]$, $b \in [7,15]$, $a = 4$, $c \in [0,9]$, $b \in [7,15]$, $a \in [0,6]$, $c = 4$, respectively, and then chaos diagrams based on complex are obtained in Fig. 7, Fig. 8 and Fig. 9. The color degree of chaos diagrams represent the complexity degree of chaotic system under parameter rang. Deep color

TABLE 1. Dynamical characteristics of system (3) for different system parameter values.

System parameters	Parameter values	Lyapunov exponents	System states
a	(0, 0.1)	(0, 0,-,-,-,-)	period
	(0.1, 1.9)	(+, 0,-,-,-,-)	chaos
	(1.9, 2.1)	(0, 0,-,-,-,-)	period
	(2.1, 4.1)	(+, 0,-,-,-,-)	chaos
	(4.1, 4.2)	(0, 0,-,-,-,-)	period
	(4.2, 5.6)	(+, 0,-,-,-,-)	chaos
	(5.6, 6)	(0, 0,-,-,-,-)	period
b	(7, 7.5)	(0, 0,-,-,-,-)	period I
	(7.5, 8)	(0, 0,-,-,-,-)	period II
	(8, 8.1)	(0, 0,-,-,-,-)	multiple period
	(8.1, 14.7)	(+, 0,-,-,-,-)	chaos
	(14.7, 14.8)	(0, 0,-,-,-,-)	period I
	(14.8, 15)	(0, 0,-,-,-,-)	multiple period
c	(0, 1.5)	(+, 0,-,-,-,-)	Chaos
	(1.5, 2)	(0, 0,-,-,-,-)	period
	(2. 9)	(+, 0,-,-,-,-)	Chaos

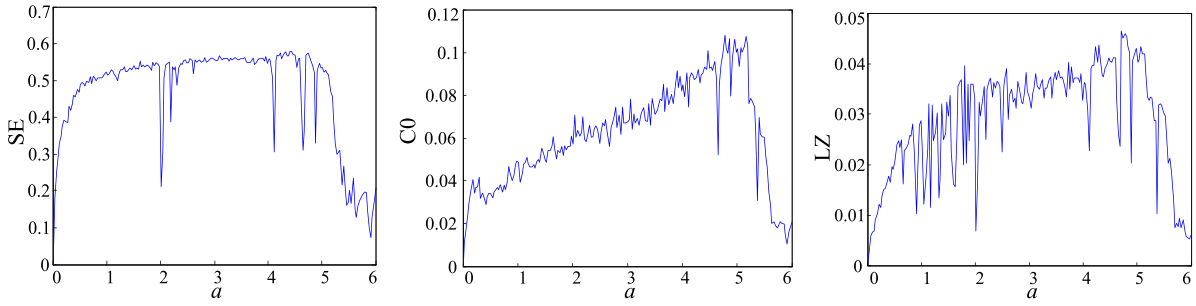


FIGURE 4. Complexity for parameter $b = 9$, $c = 5$, $a \in [0,6]$: (a) SE complexity; (b) C0 complexity; (c) LZ complexity.

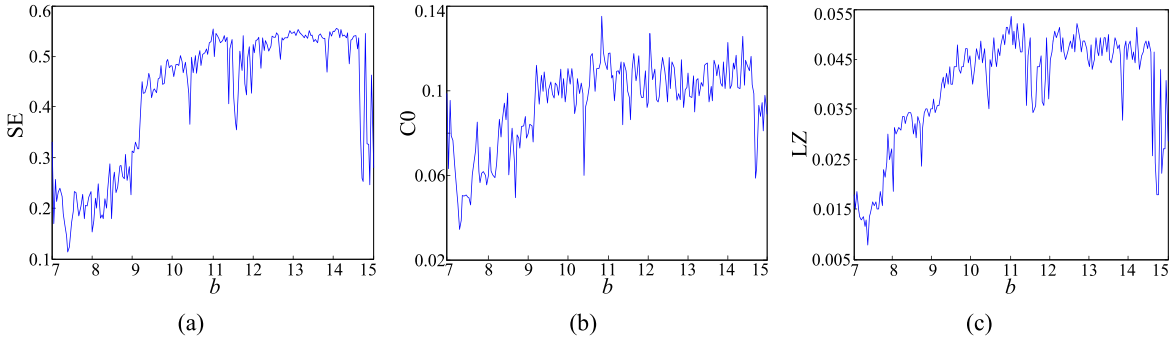


FIGURE 5. Complexity for parameter $a = 4$, $c = 5$, $b \in [7,15]$: (a) SE complexity; (b) C0 complexity; (c) LZ complexity.

means the system has high complexity value, and the random performance is good. On the contrary, light color means the random performance is poor. The chaotic diagrams illustrate that the chaotic parameters of complex chaos are in a large range, which shows that the new chaotic system is more suit for secure communication application.

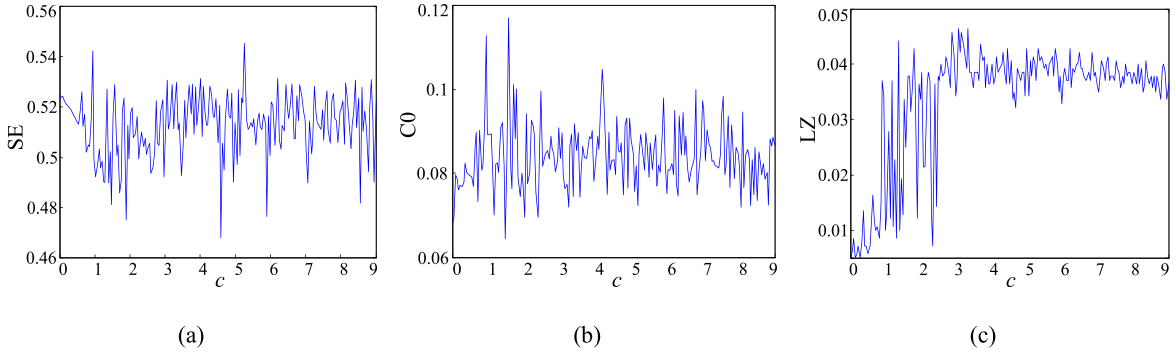


FIGURE 6. Complexity for parameter $b = 9$, $a = 4$, $c \in [0,9]$: (a) SE complexity; (b) C0 complexity; (c) LZ complexity.

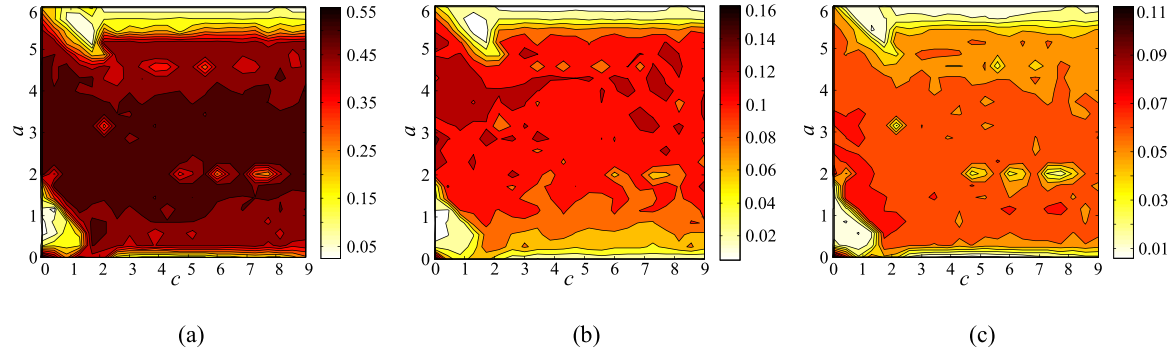


FIGURE 7. System parameter $b = 9$, $a \in [0,6]$, $c \in [0,9]$: (a) SE complexity; (b) C0 complexity; (c) LZ complexity.

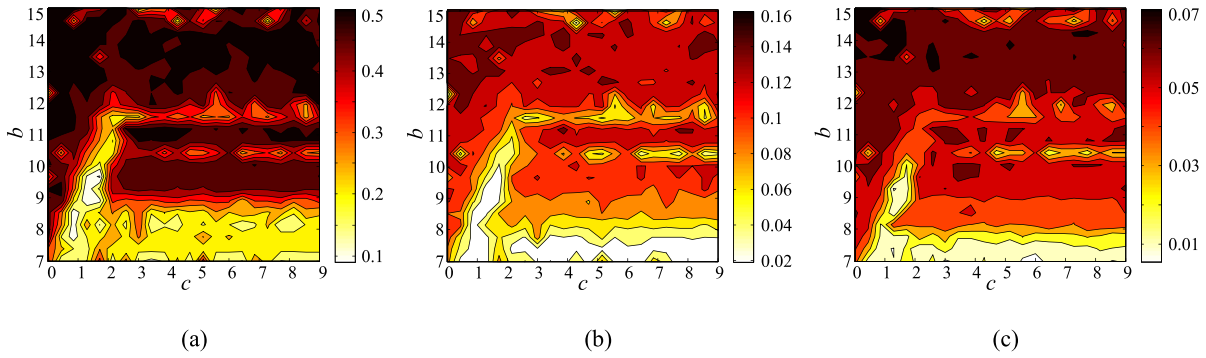


FIGURE 8. System parameter $b \in [7,15]$, $a = 4$, $c \in [0,9]$: (a) SE complexity; (b) C0 complexity; (c) LZ complexity.

C. RANDOM ANALYSIS OF SEQUENCE

To quantitatively determine the pseudo-randomness of the sequence generated by the new complex chaotic system, by using NIST test to test the random of sequence.

Chaotic digital sequences are obtained by four-order Runge-Kutta method and integer redundancy. Setting $a = 4$, $b = 9$, $c = 5$, $u_1(0) = u_2(0) = u_3(0) = u_4(0) = u_5(0) = u_6(0) = 1$, to getting the two hundred million values. In addition, each value is quantized based on integer redundancy, and convert the integer into an 8-bit binary numbers, get chaotic binary sequence. Then binary sequence is tested through NIST test. The test was conducted by STS (Statistical Test Suite) Test package, the STS is proposed through the national bureau of technology and standards of America. It has 15 indicators to test the performance of pseudo-random sequences, and 2 performance indicators (P VALUE values, passing rate of PROPOTION) are used to evaluate the sequence.

P-VALUE value reflect the characteristic of uniform distribution of sequence, it is calculated by

$$\chi^2 = \sum_{i=1}^{10} \frac{(F_i - 0.1n)^2}{0.1n}, \tag{13}$$

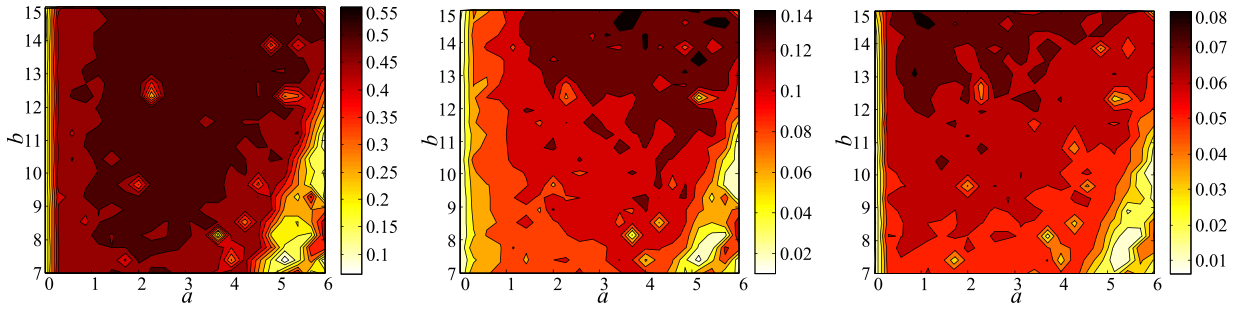


FIGURE 9. System parameter $b \in [7,15]$, $a \in [0,6]$, $c = 4$: (a) SE complexity; (b) C0 complexity; (c) LZ complexity.

TABLE 2. Test results of NIST test.

Statistical Test	Complex system		Ref [42] 2D-LICM		Ref [29] PWLCM	
	P-VALUE	PROPORTION	P-VALUE	PROPORTION	P-VALUE	PROPORTION
Frequency	0.83679	0.98	0.81679	0.97	0.73679	1
Block Frequency	0.77596	0.99	0.87596	1	0.72561	0.97
Cumulative Sums	0.68987	0.99	0.48987	0.98	0.742987	0.98
Runs	0.32879	0.98	0.12879	0.97	0.22586	0.98
Longest Run	0.52678	0.99	0.62678	1	0.49312	0.97
Rank	0.25873	0.99	0.35873	0.97	0.19456	1
FFT	0.35798	1	0.31798	0.98	0.45798	0.98
Non Overlapping Template	0.12475	0.98	0.22475	0.97	0.19475	0.97
Overlapping Template	0.68974	0.99	0.58974	1	0.49897	0.99
Universal	0.89471	1	0.81471	0.97	0.79471	1
Approximate Entropy	0.32841	0.98	0.36841	0.97	0.19841	0.97
Random Excursions	0.01589	0.99	0.01989	0.98	0.05589	1
Random Excursion Variant	0.01356	0.98	0.11356	0.98	0.01356	0.97
Serial	0.00710	1	0.10710	1	0.00910	0.97
Linear Complexity	0.57895	0.99	0.37895	0.99	0.52395	0.98

where F_i represent the number of P-VALUE value in $[0.1(i-1), 0.1i]$, n means the number of groups.

$$P - \text{VALUE} = \text{igamc}(4.5, \frac{\chi^2}{2}), \tag{14}$$

where igamc is a high-priced incomplete gamma function. When P-VALUE more than 0.0001, the sequence is uniform distribution.

Passing rate of PROPOTION is mainly the percentage of test sequences passed, the confidence interval passed by the test is

$$1 - \alpha \pm \sqrt{\alpha(1-\alpha)/n}, \tag{15}$$

where significant level α is 0.01, group test $n \geq 1000$.

Based on windows platform, the data of new complex system, Ref [42] 2D-LICM chaotic map and Ref [29] PWLCM were respectively divided into 5000 groups, and the each group is 2×10^4 bit, then the corresponding of test result is shown in Table. 2. It indicates that sequence of new complex chaotic has better randomness, which can be used for chaotic encryption.

V. APPLICATION OF THE NOVEL COMPLEX CHAOTIC SYSTEM IN IMAGE DIFFUSION

According to above dynamic performance of new complex chaotic system, in this section, we propose an image diffusion algorithm based on the complex chaotic system and the model of law of gravity.

A. THE LAW OF GRAVITY

As everyone knows, any two objects in nature have an attracted, the force of gravity with the product of the masses

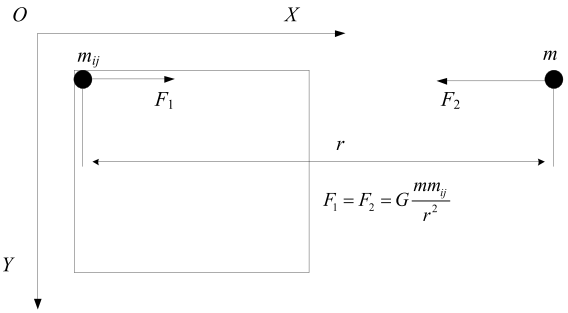


FIGURE 10. Sketch map of image in the XOY plane.

of two between objects is direct ratio, but with the distance squared of two between objects is inverse ratio. The relationship between them can be expressed as

$$F = G\frac{m_1 m_2}{r^2}, \tag{16}$$

where m_1 and m_2 represent the mass of two particles, r is distance between two particles, G means that gravity constant.

B. PRINCIPLE OF DIFFUSION ALGORITHM BASED ON THE MODEL OF LAW OF GRAVITY

Image I $(M \times N)$ can be viewed as $M \times N$ particles located in the same plane in space, assumption, there is a unit particle out of this plane, then the unit particle must exert gravity on $M \times N$ particles in the plane, on the basis of this gravity, the image pixel values are changed. For simplicity, the XOY plane of image as shown in Fig. 10.

Assumption,

$$C_{ij} = [g\frac{mm_{ij}}{(x-i)^2 + (y-j)^2 + z^2}] \bmod 256 \oplus I_{ij}, \tag{17}$$

where m is mass of unit particle (in order to facilitate the calculation, setting $m = 1$). (x, y, z) represent the coordinate of unit particle in space plane, here, $z \neq 0$, therefore, $(x\text{-}i)^2 + (y\text{-}j)^2 + z^2 > 0$, setting x and y are any value. m_{ij} is quality of image in row i, column j, g means that gravity constant and has a larger value. I_{ij} represent the pixel value of original in row i, column j, C_{ij} means changed pixel value, [] is rounding operation, mod represent modulus operation, $\oplus$ is XOR operation.

C. THE PROPOSED DIFFUSION ALGORITHM BASED ON THE MODEL OF LAW OF GRAVITY

In this paper, the proposed image diffusion algorithm based on complex chaotic system and the model of law of gravity is shown in Fig. 11, and the corresponding steps are in detail described as follows.

Step1 Inputting an image I $(M \times N)$.

Step2 To meet the diffusion requirements, the continuous chaotic system need to be discretize. Therefore, complex chaotic is discretized based on four-order Runge-Kutta method.

Step3 On the basis of four-order Runge-Kutta method, setting system parameter and initial values, the system (3) is iterated $(M \times N)$ times, and then six chaotic sequences with the length of $(M \times N)$ are obtained.

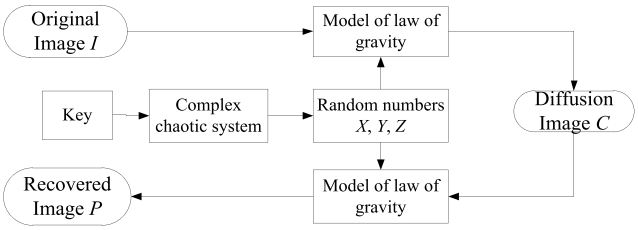


FIGURE 11. Flow chart of diffusion algorithm.

Step4 Three chaotic sequences x, y and z are randomly selected from six chaotic sequences, and then, three random numbers X, Y, Z are obtained through

$$\begin{cases} X = (\sum_{i=1}^{M\times N} |floor(x_i)|)/(M \times N) \\ Y = (\sum_{i=1}^{M\times N} |floor(y_i)|)/(M \times N) \\ Z = (\sum_{i=1}^{M\times N} |floor(z_i)|)/(M \times N). \end{cases} \tag{18}$$

Step5 Based on the Principle of diffusion algorithm and the model of law of gravity in section V.B, the image pixels are diffused through Eq. (17), here, fix the m_{ij} follows the $m_{ij} = Xi + Yj + Z$ distribution in XOY plane and X, Y, Z are obtained in step 4.

Step6 Finally, the diffused image C is obtained.

Regression algorithm is the same as the encryption algorithm, the diffused image C is been as input, the recovered image P is obtained by

$$P_{ij} = [g\frac{mm_{ij}}{(x-i)^2 + (y-j)^2 + z^2}] \bmod 256 \oplus C_{ij}. \tag{19}$$

D. SIMULATION RESULTS

To verify the proposed algorithm, the experiments are implemented by MATLAB 2014a. The size of 256 × 256 Lena, finger, brain, camera, couple, flower, girl, fruits and fingerprint images are used to algorithm test. Setting the secret key: complex chaotic parameter $a = 4$, $b = 9$, $c = 5$, $x = 1 + i$, $y = 1 + i$, $z = 1$ and $w = 1$, gravity constant $g = 3 \times 10^8$. Lena and camera images are illustrated in Fig. 12. As we can see, diffused image is noise-like image, which shows that the original image information is well hidden through the proposed image diffusion algorithm. In addition, recovered image is same as original image, which means that the proposed algorithm can effectively recover hidden image information.

VI. PERFORMANCES ANALYSIS

A. KEY SPACE

Key space refers to collection of all secret key. A good image cipher system should be has enough large key space, so that it can effectively resist brute force attacks. The key model of the proposed algorithm is complex chaotic system

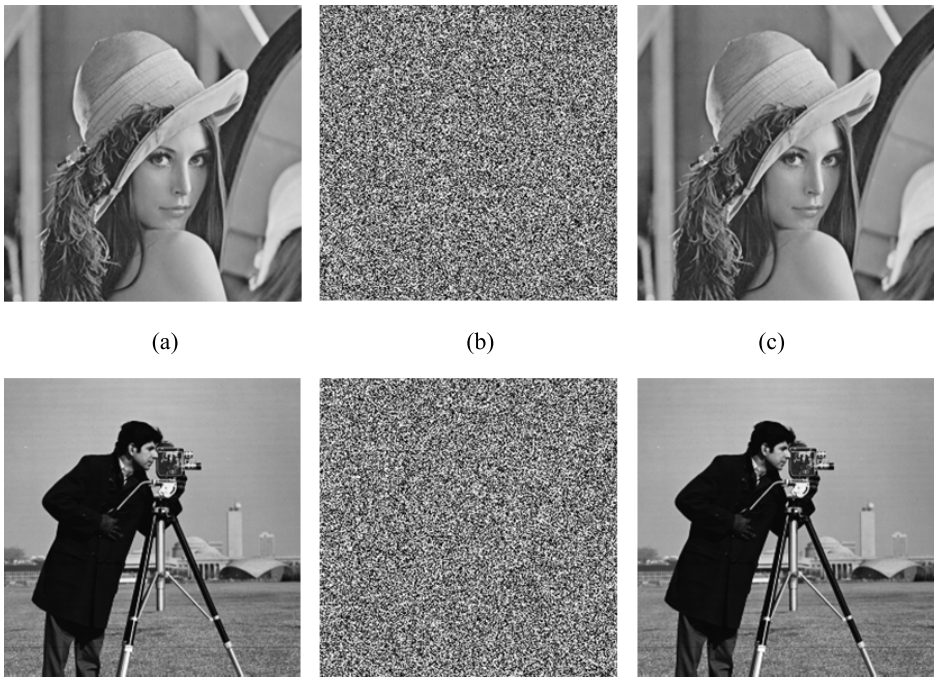


FIGURE 12. Simulation results: (a) Original Lena image; (b) Diffused Lena image; (c) Recovered Lena image; (d) Original camera image; (f) Diffused camera image; (f) Recovered camera image.

parameters a, b, c, initial values u_{10}, u_{20}, u_{30}, u_{40}, u_{50}, u_{60} in complex chaotic system real form, gravity constant g. The key space obtained by calculation is 2^{366} much larger than 2^{100} [44] when the computational accuracy is 11 decimal places. Therefore, the proposed new image algorithm has larger key space and can prevent the brute force attacks.

B. KEY SENSITIVITY

To test the key sensitivity of the proposed algorithm, Setting the secret key $a = 4$, $b = 9$, $c = 5$, $x = 1 + i1$, $y = 1 + i1$, $z = 1$, $w = 1$, $g = 3 \times 10^8$, then the proposed algorithm is used to encrypt Lena image. Then secret key a, b and g are changed 10^{-11} respectively, then according to decryption algorithm the corresponding encrypted image are recovered, the results are shown in Fig.13. It can be seen that even if the key is slightly changed, the cipher image cannot be decrypted correctly. In addition, the decrypted image is entirely different from the original image. What's more, the experiment changed other keys of the key group to test and got similar results. Therefore, the key of the proposed algorithm is sufficiently sensitive.

C. STATISTIC ANALYSIS

1) HISTOGRAM

Histogram is an important method for analyze statistic. In this test, histograms of original and encrypted images are obtained by experimental numerical simulation as shown in Fig. 14. It shows that the distribution range and number of pixel values in the plaintext image histogram are not uniform, which means that the information of original image is vulnerable to statistical attacks. On the contrary, the original image is encrypted by the proposed algorithm, then its pixel values are evenly distributed within the range of 0-250 and the occurrence probability of each pixel value is basically the same, which shows that the statistical characteristics of plaintext pixels have been fundamentally changed. In addition, it can be judged that the proposed algorithm can effectively resist attacks based on statistical analysis.

2) CORRELATION COEFFICIENTS

Correlation between adjacent pixels means that an important method for statistical analysis. The Image cipher system can be cracked by statistical analysis when correlation coefficient between adjacent pixels is high. Therefore, the proposed algorithm needs to be able to reduce the correlation between adjacent pixels. In this test, correlation coefficients between adjacent pixels are calculated by

$$r_{xy} = \frac{cov(x, y)}{\sqrt{D(x)D(y)}} \tag{20}$$

where, cov (x, y) means the covariance of x and y, $D(x)$ and $D(y)$ are variance of x and y. In addition, the mathematical expectation $E(x)$, cov (x, y), $D(x)$ and $D(y)$ are calculated by

$$cov(x, y) = E\left\{[x - E(x)]\,[y - E(y)]\right\}, \tag{21}$$

$$E(x) = \frac{1}{M}\sum_{i=1}^{M} x_i, \tag{22}$$

$$D(x) = \frac{1}{M}\sum_{i=1}^{M} [x_i - E(x)]^2, \tag{23}$$

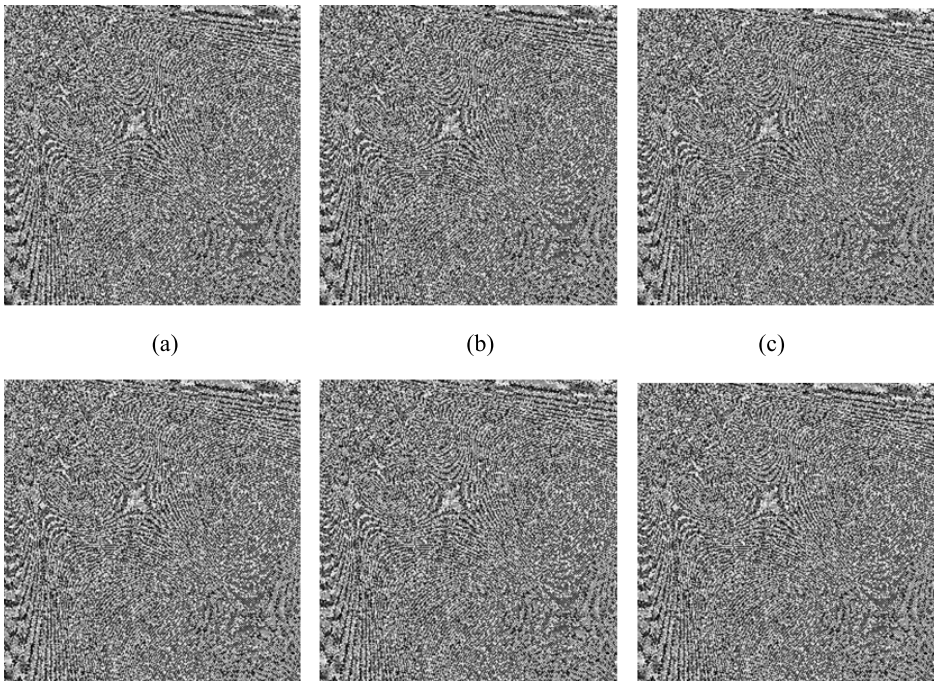


FIGURE 13. Decryption results: (a) $a + 10 - 11$; (b) $b + 10 - 11$; (c) $g + 10 - 11$; (d) $x + 10 - 11$; (e) $y + 10 - 11$; (f) $z + 10 - 11$.

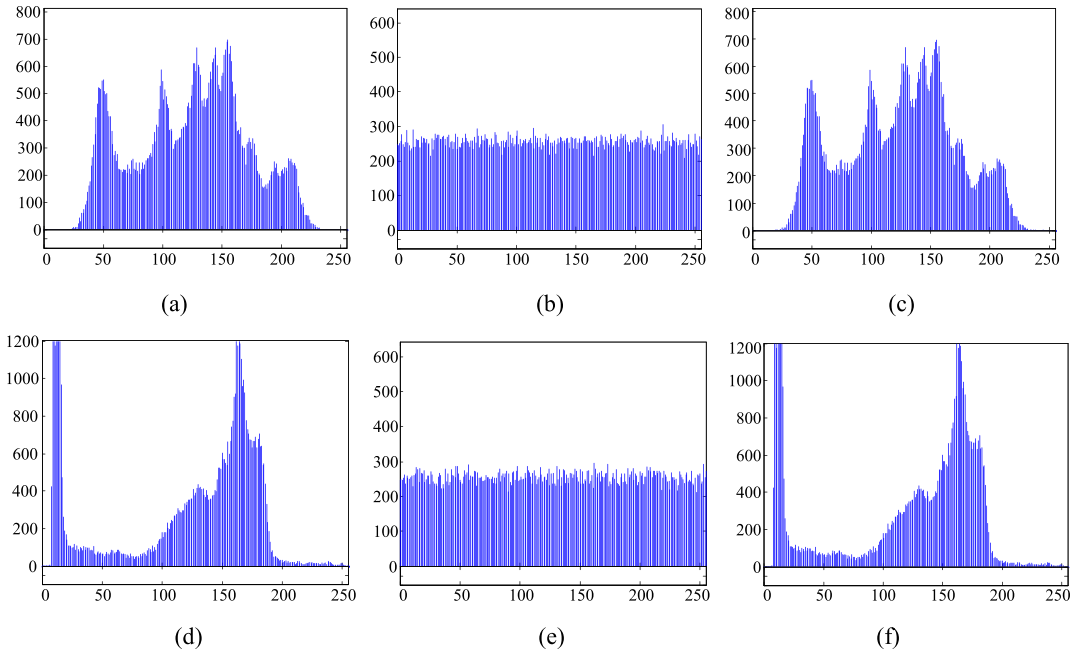


FIGURE 14. Histograms: (a) Original Lena image; (b) Diffused Lena image; (c) Recovered Lena image; (d) Original camera image; (e) Diffused camera image; (f) Recovered camera image.

where M represent the overall pixels of the image. 2000 sets of pixel points of the original Lena image and the encrypted Lena image were selected from the horizontal, vertical and diagonal directions respectively, and then the relationship between the gray values of the adjacent pixels are shown as Fig. 15. As can be seen from Fig. 15, the gray value of adjacent pixels of plaintext image is distributed around $y = x$ in horizontal, vertical and diagonal directions.

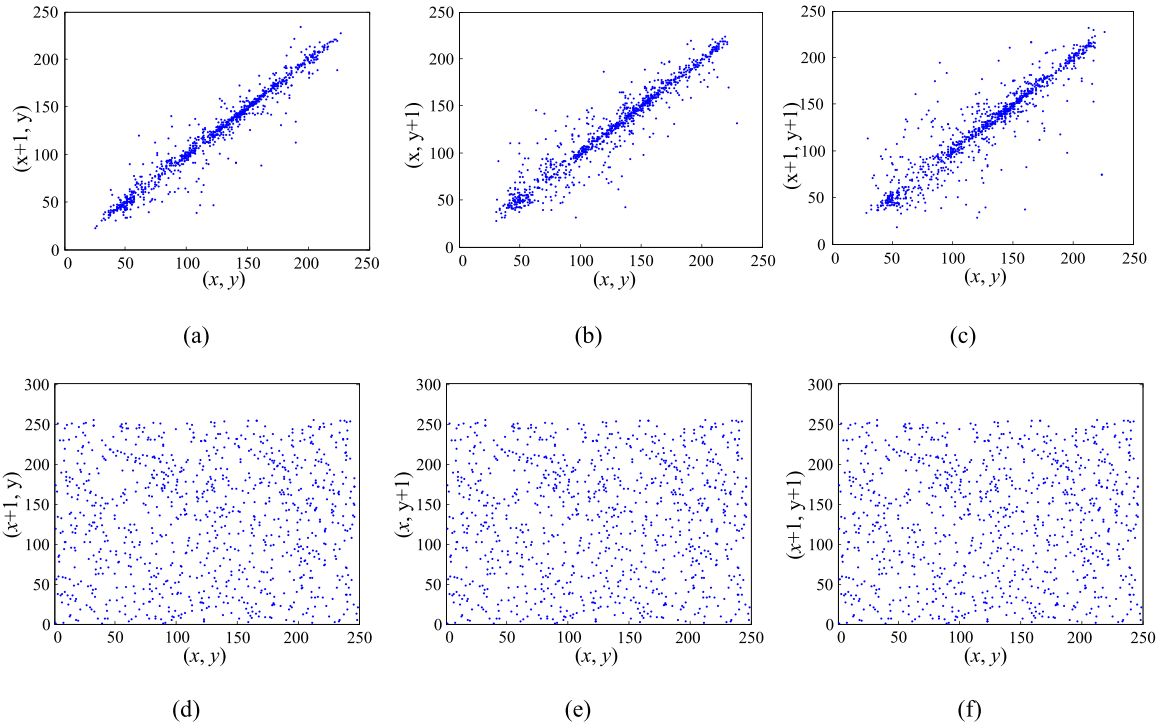


FIGURE 15. Distribution of pixel values between adjacent pixels, (a) horizontal direction of plaintext Lena image, (b) vertical direction of plaintext Lena image, (c) diagonal direction of plaintext Lena image, (d) horizontal direction of ciphertext Lena image, (e) vertical direction of ciphertext Lena image, (d) diagonal direction of ciphertext Lena image.

TABLE 3. Correlation coefficients of images.

Directions	finger	Lena	brain	camera	couple	flower	girl	fruits	fingerprint
Horizontal	-0.0054	0.0004	-0.0009	0.0078	-0.0018	-0.0020	0.0028	-0.0007	-0.0037
Vertical	0.0008	-0.0048	-0.0022	-0.0047	0.0010	-0.0008	-0.0023	-0.0504	0.0069
Diagonal	-0.0019	0.0022	-0.0039	0.0015	0.0017	0.0013	-0.0002	-0.0201	-0.0105

TABLE 4. Correlation coefficients of lena image with different algorithms.

Directions	Plaintext image	Our algorithm	Ref [27]	Ref [28]	Ref [29]	Ref [30]	Ref [39]	Ref [40]	Ref [41]	Ref [42]
Horizontal	0.9704	0.0004	0.0070	0.0012	0.0049	0.0124	0.0012	0.0019	0.0065	0.0019
Vertical	0.9412	-0.0048	0.0022	0.0074	0.0041	0.0141	0.0013	0.0038	0.0035	0.0012
Diagonal	0.9162	0.0022	0.0148	0.0028	0.0047	0.0115	0.0020	-0.0019	0.0036	0.0009

While the gray value of adjacent pixels of the encrypted image is randomly distributed between 0 and 250. It indicates that the proposed algorithm can effectively reduce correlation of adjacent pixels.

The correlation coefficient values of horizontal, vertical and diagonal directions of the original images and encrypted images are listed Table 3. The results of comparison with the correlation coefficients of Lena images in other literatures are shown in Table 4. Obviously, the horizontal, vertical and diagonal correlation of adjacent pixels in original Lena image are all greater than 0.9, the correlation degree of adjacent pixels is high. But the correlation of adjacent pixels in the encrypted image by the proposed algorithm is close to 0. This will be further illustrates that the proposed algorithm can effectively reduce correlation of adjacent pixels.

D. INFORMATION ENTROPY

Information entropy refer to reflect randomness of image information, in a general way, the greater the information entropy, the greater the uncertainty. Information entropy

TABLE 5. Information entropy, NPCR and UACI of encrypted images.

Figures	finger	Lena	brain	camera	couple	flower	girl	fruits	fingerprint
Entropy	7.9971	7.9974	7.9969	7.9970	7.9974	7.9973	7.9972	7.9971	7.9972

TABLE 6. Information entropy of encrypted images.

Algorithms	Our algorithm	Ref [27]	Ref [28]	Ref [29]	Ref [30]	Ref [39]	Ref [40]	Ref [42]
Entropy	7.9974	7.9982	7.9974	7.9971	7.9972	7.9978	7.9971	7.9973

TABLE 7. NPCR of encrypted images.

Images	*NPCR* (%)	*NPCR* Critical Value		
		*NPCR**0.05= 99.58	*NPCR**0.01=99.57	*NPCR**0.001=99.56
finger	99.61	Pass	Pass	Pass
Lena	99.62	Pass	Pass	Pass
brain	99.60	Pass	Pass	Pass
camera	99.59	Pass	Pass	Pass
couple	99.61	Pass	Pass	Pass
flower	99.58	Pass	Pass	Pass
girl	99.61	Pass	Pass	Pass
fruits	99.61	Pass	Pass	Pass
fingerprint	99.60	Pass	Pass	Pass

usually can be calculated by

$$H(m) = \sum_{i=0}^{L-1} p(m_i) \log \frac{1}{p(m_i)}, \tag{24}$$

where $p(m_i)$ means the probability that the state m_i might occur, and L represent the number of all state m_i. For the 256 gray-level images $i = 2^8$, so the ideal value of information entropy is 8.

According to the Eq. (24), information entropy of different image diffusion after is listed in Table. 5. The information entropy compared results with algorithms [27]–[30], [39], [40], [42] are shown in Table. 6. As we can see that information entropy of image diffusion after is more than 7.997, which is close to ideal value. Therefore, the diffused image can be approximated as a random image. The comparison shows that the proposed algorithm is better than most exiting algorithms, which illustrates that the algorithm more conducive to image encryption to improve security.

E. DIFFERENTIAL ATTACK ANALYSIS

Differential attack refers to sensitivity of ciphertext to plaintext. In generally, number of pixels change rate (NPCR) and unified average changing intensity (UACI) are used to test differential attack. The computational formula is defined as

$$\begin{cases} NPCR = \dfrac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{M \times N} \times 100\% \\ UACI = \dfrac{\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{|C_1(i,j) - C_2(i,j)|}{256}}{M \times N} \times 100\%, \end{cases} \tag{25}$$

where M and N respectively represent the number of rows and columns of the image. $C_1(i, j)$ and C_2 (i, j) means pixel value of point (i, j) for two encrypted images. D (i, j) is

$$D(i,j) = \begin{cases} 1, & C_1(i,j) \neq C_2(i,j) \\ 0, & C_1(i,j) \neq C_2(i,j). \end{cases} \tag{26}$$

The idea value of *NPCR* and *UACI* are

$$\begin{cases} NPCR_E = (1 - 2^{-n}) \times 100\% \\ UACI_E = \dfrac{1}{2^{2n}} \dfrac{\sum_{i=1}^{2^n-1} i(i+1)}{2^{2n}-1} \times 100\%, \end{cases} \tag{27}$$

where n is image color bit depth, for the gray image of 8 bit, the idea value of NPCR and UACI are 0.9961 and 0.3346.

In this experiment test, based on Eq. (26) and Eq. (27), the NPCR and UACI of different image is calculated as Table. 7 and 8. In addition, according to Ref [45, 46], the critical values based on 5%, 1% and 0.1% significance are

TABLE 8. UACI of encrypted images.

Images	*UACI* (%)	*UACI* Critical Value		
		*UACI**-0.05= 33.41	*UACI**-0.01=33.40	*UACI**-0.001=33.39
		*UACI**+0.05=33.52	*UACI**+0.01=33.51	*UACI**+0.001=33.50
finger	33.50	Pass	Pass	Pass
Lena	33.50	Pass	Pass	Pass
brain	33.43	Pass	Pass	Pass
camera	33.42	Pass	Pass	Pass
couple	33.48	Pass	Pass	Pass
flower	33.45	Pass	Pass	Pass
girl	33.47	Pass	Pass	Pass
fruits	33.41	Pass	Pass	Pass
fingerprint	33.42	Pass	Pass	Pass

TABLE 9. NPCR and UACI of different algorithms.

Algorithms	*NPCR* (%)	*UACI* (%)
Ref [27]	99.61	33.46
Ref [28]	99.61	33.46
Ref [29]	99.60	33.47
Ref [30]	99.62	33.49
Ref [39]	99.58	33.36
Ref [40]	99.58	33.25
Ref [42]	99.60	33.45
Our algorithm	99.62	33.50

calculated. What's more, the comparison results of algorithms [27]–[30], [39], [40], [42] are listed in Table. 9. The results indicate that the proposed algorithm can resist differential attack.

F. NOISE ATTACK ANALYSIS

Since the information is easily affected by various noises such as Gaussian noise and Salt & Pepper noise in the process of transmission, it is necessary to analyze the algorithm's ability to against the noise. In this test, the Gaussian noise and Salt & Pepper noise are used to noise test.

Gaussian noise is mathematically easy to deal with and is the most commonly used noise model in practice. Its probability density function is

$$p(z) = \frac{1}{\sqrt{2\pi}\sigma} e^{-(z-z_1)^2/z\sigma^2}, \tag{28}$$

where z represent the grey value, z_1 is the average value of z, σ means the standard deviation of z, σ^2 is the variance of z.

TABLE 10. Speed Analysis of different algorithms.

Our algorithm	Ref [39]	Ref [40]	Ref [41]	Ref [42]
0.02279	0.028	0.175	0.77796	0.32432

The probability density function of Salt & Pepper noise is expressed by

$$p(z) = \begin{cases} P_a(z=a) \\ P_b(z=b) \\ 0(\text{other}). \end{cases} \tag{29}$$

If $b > a$, the grayscale value b will appear as a bright spot in the image, whereas the value of a will appear as a dark spot. If P_a is 0, or P_b is 0, the impulse noise is called unipolar pulse. If P_a and P_b are not 0, especially if they are approximately equal, the impulse noise values will be similar to Salt & Pepper dust particles randomly distributed on the image. For this reason, bipolar impulse noise is also known as salt-pepper noise. At the same time, they are sometimes referred to as scattershot and spike noise.

Based on the principle of Gaussian noise and Salt & Pepper noise, the different variances noise are selected to attack the diffused Lena image of Fig 12(b), and then the proposed algorithm is used to decrypt image of noise attacks. The corresponding recovered images are shown in Fig. 16 and 17. As we can see, when a certain range of noise attacks the ciphertext image, the main image information can be recovered by the proposed decryption algorithm. It indicates that the proposed algorithm can resist a certain degree of noise attack

G. SPEED ANALYSIS

In real time applications, speed performance of the algorithm is an important evaluation criterion. In this experiment, the time complexity is used to analysis speed performance

(a) (b) (c)

FIGURE 16. Analysis of Gaussian noise attack, (a) noise with variance of 0.0005, (b) noise with variance of 0.0003, (c) noise with variance of 0.0001.

(a) (b) (c)

FIGURE 17. Analysis of Salt & Pepper noise attack, (a) noise with variance of 0.1, (b) noise with variance of 0.05, (c) noise with variance of 0.01.

of the encryption algorithm. On the basis of the computer of the Intel Celeron (R) CPU G540 @ 2.50 GHz, 4GB RAM with windows 7 to running MATLAB (R2014a) encryption algorithm, the 256 × 256 Lena image is encrypted for 30 times. Then obtained average encryption time is 0.02279 s, and Table listed the time complexity values of the different encryption algorithms. Obviously, the proposed algorithm is much faster than other algorithms in [39]–[42], which shows that the proposed algorithm is more suitable for real applications.

VII. CONCLUSION

In this study, we achieved four important goals. In the first place, a novel complex chaotic system is obtained. The second one is the analysis of the characteristics of new system using symmetric, dissipative and stability. Thirdly, dynamical features of the system are analyzed by bifurcation diagram, Lyapunov exponent spectrum and complexity. In the end, combining the novel complex chaotic system with model of law of gravity is used in image diffusion algorithm. Simulation results show that the constructed complex chaotic system has rich nonlinear dynamic characteristic, and the corresponding image diffusion algorithm support high security and effectiveness.

REFERENCES

[1] A. C. Fowler, J. D. Gibbon, and M. J. McGuinness, "The complex Lorenz equations," *Phys. D, Nonlinear Phenomena*, vol. 4, no. 2, pp. 139–163, 1982.

[2] A. C. Fowler, J. D. Gibbon, and M. J. McGuinness, "The real and complex Lorenz equations and their relevance to physical systems," *Phys. D, Nonlinear Phenomena*, vol. 7, nos. 1–3, pp. 126–134, 1983.

[3] J. D. Gibbon and M. J. McGuinness, "The real and complex Lorenz equations in rotating fluids and lasers," *Phys. D, Nonlinear Phenomena*, vol. 5, no. 1, pp. 108–122, 1982.

[4] G. M. Mahmoud, E. E. Mahmoud, and M. E. Ahmed, "A hyperchaotic complex Chen system and its dynamics," *Int. J. Appl. Math. Statist.*, vol. 12, pp. 90–100, Dec. 2007.

[5] G. M. Mahmoud, M. A. Al-Kashif, and S. A. Aly, "Basic properties and chaotic synchronization of complex lorenz system," *Int. J. Mod. Phys. C*, vol. 18, no. 2, pp. 253–265, 2007.

[6] G. M. Mahmoud and E. E. Mahmoud, "Synchronization and control of hyperchaotic complex Lorenz system," *Math. Comput. Simul.*, vol. 80, no. 12, pp. 2286–2296, Aug. 2010.

[7] C. Luo and X. Wang, "Chaos in the fractional-order complex Lorenz system and its synchronization," *Nonlinear Dyn.*, vol. 71, nos. 1–2, pp. 241–257, 2013.

[8] S. Liu and F. Zhang, "Complex function projective synchronization of complex chaotic system and its applications in secure communication," *Nonlinear Dyn.*, vol. 76, no. 2, pp. 1087–1097, 2014.

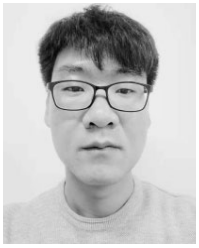
[9] C. Jiang and S. Liu, "Generalized combination complex synchronization of new hyperchaotic complex Lü-like systems," *Adv. Difference Equ.*, vol. 2015, Jul. 2015, Art. no. 214.

[10] J. Liu, S. Liu, and C. Yuan, "Adaptive complex modified projective synchronization of complex chaotic (hyperchaotic) systems with uncertain complex parameters," *Nonlinear Dyn.*, vol. 79, no. 2, pp. 1035–1047, 2015.

[11] V. K. Yadav, N. Srikanth, and S. Das, "Dual function projective synchronization of fractional order complex chaotic systems," *Optik*, vol. 127, pp. 10527–10538, Nov. 2016.

[12] J. Liu, S. Liu, and J. C. Sprott, "Adaptive complex modified hybrid function projective synchronization of different dimensional complex chaos with uncertain complex parameters," *Nonlinear Dyn.*, vol. 83, nos. 1–2, pp. 1109–1121, Jan. 2016.

[13] L.-X. Yang and J. Jiang, "Complex dynamical behavior and modified projective synchronization in fractional-order hyper-chaotic complex Lü system," *Chaos, Solitons Fractals*, vol. 78, pp. 267–276, Sep. 2015.
[14] G. M. Mahmoud, E. E. Mahmoud, and A. A. Arafa, "On modified time delay hyperchaotic complex Lü system," *Nonlinear Dyn.*, vol. 80, nos. 1–2, pp. 855–869, 2015.
[15] F. Zhang and S. Liu, "Self-time-delay synchronization of time-delay coupled complex chaotic system and its applications to communication," *Int. J. Mod. Phys. C*, vol. 25, no. 3, 2014, Art. no. 1350102.
[16] Y. Liu, X. Tong, and S. Hu, "A family of new complex number chaotic maps based image encryption algorithm," *Signal Process., Image Commun.*, vol. 28, no. 10, pp. 1548–1559, 2013.
[17] L. Wang, H. Song, and P. Liu, "A novel hybrid color image encryption algorithm using two complex chaotic systems," *Opt. Lasers Eng.*, vol. 77, pp. 118–125, Feb. 2016.
[18] H. Liu, A. Kadir, and Y. Li, "Asymmetric color pathological image encryption scheme based on complex hyper chaotic system," *Optik*, vol. 127, no. 15, pp. 5812–5819, 2016.
[19] G. Liu, A. Kadir, and H. Liu, "Color pathological image encryption scheme with S-boxes generated by complex chaotic system and environmental noise," *Neural Comput. Appl.*, vol. 27, no. 3, pp. 687–697, 2016.
[20] X. Chai, Z. Gan, K. Yuan, Y. Chen, and X. Liu, "A novel image encryption scheme based on DNA sequence operations and chaotic systems," *Neural Comput. Appl.*, vol. 31, no. 1, pp. 219–237, 2019.
[21] X. Chai, Z. Gan, Y. Lu, Y. Chen, and D. Han, "A novel image encryption algorithm based on the chaotic system and DNA computing," *Int. J. Mod. Phys. C*, vol. 28, no. 5, 2017, Art. no. 1750069.
[22] X. Wu, B. Zhu, Y. Hu, and Y. Ran, "A novel color image encryption scheme using rectangular transform-enhanced chaotic tent maps," *IEEE Access*, vol. 5, pp. 6429–6436, 2017.
[23] C. Zhu and K. Sun, "Cryptanalyzing and improving a novel color image encryption algorithm using RT-enhanced chaotic tent maps," *IEEE Access*, vol. 6, pp. 18759–18770, 2018.
[24] A. A. A. El-Latif, B. Abd-El-Atty, and M. Talha, "Robust encryption of quantum medical images," *IEEE Access*, vol. 6, pp. 1073–1081, 2017.
[25] X. Zhang and X. Wang, "Digital image encryption algorithm based on elliptic curve public cryptosystem," *IEEE Access*, vol. 6, pp. 70025–70034, 2018.
[26] R. Hamza, K. Muhammad, N. Arunkumar, and G. Ramírez-González, "Hash based encryption for keyframes of diagnostic hysteroscopy," *IEEE Access*, vol. 6, pp. 60160–60170, 2017.
[27] Y. Wang, K.-W. Wong, X. Liao, and G. Chen, "A new chaos-based fast image encryption algorithm," *Appl. Soft Comput.*, vol. 11, no. 1, pp. 514–522, 2011.
[28] B. Norouzi, S. M. Seyedzadeh, S. Mirzakuchaki, and M. R. Mosavi, "A novel image encryption based on hash function with only two-round diffusion process," *Multimedia Syst.*, vol. 20, no. 1, pp. 45–64, 2014.
[29] X. Wang, S. Wang, N. Wei, and Y. Zhang, "A novel chaotic image encryption scheme based on hash function and cyclic shift," *IETE Tech. Rev.*, vol. 36, no. 1, pp. 39–48, 2018.
[30] L. Xu, Z. Li, J. Li, and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps," *Opt. Lasers Eng.*, vol. 78, pp. 17–25, Mar. 2016.
[31] S. Hanis and R. Amutha, "A fast double-keyed authenticated image encryption scheme using an improved chaotic map and a butterfly-like structure," *Nonlinear Dyn.*, vol. 95, no. 1, pp. 421–432, Jan. 2019.
[32] P. Li, J. Xu, J. Mou, and F. Yang, "Fractional-order 4D hyperchaotic memristive system and application in color image encryption," *EURASIP J. Image Video Process.*, vol. 2019, Jan. 2019, Art. no. 22.
[33] F. Yang, J. Mou, C. Luo, and Y. Cao, "An improved color image encryption scheme and cryptanalysis based on a hyperchaotic sequence," *Physica Scripta*, vol. 94, no. 8, 2019, Art. no. 85206.
[34] J. Ahmad and S. O. Hwang, "Chaos-based diffusion for highly autocorrelated data in encryption algorithms," *Nonlinear Dyn.*, vol. 82, no. 4, pp. 1839–1850, 2015.
[35] F. Yang, J. Mou, K. Sun, Y. Cao, and J. Jin, "Color image compression-encryption algorithm based on fractional-order memristor chaotic circuit," *IEEE Access*, vol. 7, pp. 58751–58763, 2019.
[36] X. Zhang and X. Wang, "Multiple-image encryption algorithm based on DNA encoding and chaotic system," *Multimedia Tools Appl.*, vol. 78, no. 6, pp. 7841–7869, 2019.
[37] M. Zhang and T. Tong, "Joint image encryption and compression scheme based on a new hyperchaotic system and curvelet transform," *Proc. SPIE*, vol. 26, no. 4, 2017, Art. no. 043008.
[38] J. Liu, X. Tong, Y. Liu, M. Zhang, and J. Ma, "A joint encryption and error correction scheme based on chaos and LDPC," *Nonlinear Dyn.*, vol. 93, no. 3, pp. 1149–1163, 2018.
[39] L. Liu, S. Hao, J. Lin, Z. Wang, X. Hu, and S. Miao, "Image block encryption algorithm based on chaotic maps," *IET Signal Process.*, vol. 12, no. 1, pp. 22–30, Feb. 2018.
[40] X. Wang, L. Liu, and Y. Zhang, "A novel chaotic block image encryption algorithm based on dynamic random growth technique," *Opt. Lasers Eng.*, vol. 66, pp. 10–18, Mar. 2015.
[41] A.-V. Diaconu, "Circular inter–intra pixels bit-level permutation and chaos-based image encryption," *Inf. Sci.*, vols. 355–356, pp. 314–327, Aug. 2016.
[42] C. Cao, K. Sun, and W. Liu, "A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map," *Signal Process.*, vol. 143, pp. 122–133, Feb. 2018.
[43] L. Wang and M. Ding, "Dynamical analysis and passive control of a new 4D chaotic system with multiple attractors," *Mod. Phys. Lett. B*, vol. 32, no. 22, 2018, Art. no. 1850260.
[44] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurcation Chaos*, vol. 16, no. 8, pp. 2129–2151, 2006.
[45] D. Ravichandran, P. Praveenkumar, J. B. B. Rayappan, and R. Amirtharajan, "DNA chaos blend to secure medical privacy," *IEEE Trans. Nanobiosci.*, vol. 16, no. 8, pp. 850–858, Dec. 2017.
[46] D. Ravichandran, P. Praveenkumar, J. B. B. Rayappan, and R. Amirtharajan, "Chaos based crossover and mutation for securing DICOM image," *Comput. Biol. Med.*, vol. 72, pp. 170–184, May 2016.



FEIFEI YANG received the B.E. degree from Longdong University, Qingyang, China, in 2016. He is currently pursuing the Ph.D. degree in control science and engineering with Dalian Polytechnic University, Dalian, China. His main research interest includes chaos theory and application.

JUN MOU received the B.S., M.S., and Ph.D. degrees in physics and electronics from Central South University, Changsha, China. He is currently an Associate Professor with the School of Information Science and Engineering, Dalian Polytechnic University, China. His main research interests include the nonlinear system control, secure communication, power system automation, and smart grid research.

HUIZHEN YAN received the B.S. and M.S. degrees from Xian Jiaotong University (XJU), Xi'an, China, and the Ph.D. degree in applied mathematics from Northeastern University (NEU), Shenyang, China, in 2000. She is currently a Professor with the School of Information Science and Engineering, Dalian Polytechnic University. Her research interests include game theory and its application and ecological mathematics.

JINHUA HU received the B.E. degree from Dalian Polytechnic University, Dalian, China, in 2015, where she is currently pursuing the Ph.D. degree with the Liaoning Provincial Key Laboratory of Ecological Textiles, National Supercritical Fluid Waterless Dyeing Technology Research and Development Center. Her main research interests include solubility prediction and data processing.