IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 9, 2018, accepted July 7, 2018, date of publication July 13, 2018, date of current version August 7, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2855726

Spatiotemporal Chaos in Coupled Logistic Map Lattice With Dynamic Coupling Coefficient and Its Application in Image Encryption

WANG XINGYUAN[1,2], FENG LE[2], WANG SHIBING[2], CHUAN ZHANG[2], AND ZHANG YINGQIAN[3]

[1] School of Information Science and Technology, Dalian Maritime University, Dalian 116026, China
[2] Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, Dalian 116024, China
[3] School of Information Science and Technology, Tan Kah Kee College, Xiamen University, Zhangzhou 361005, China

Corresponding authors: Wang Xingyuan (wangxy@dlut.edu.cn) and Feng Le (18362827042@163.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61672124, Grant 61370145, and Grant 61173183, in part by the the Password Theory Project of the 13th Five-Year Plan National Cryptography Development Fund under Grant MMJJ20170203, and in part by the China Postdoctoral Science Foundation under Grant 2016M601307.

ABSTRACT This paper proposes a new spatiotemporal chaos model, which is a logistic-dynamic coupled logistic map lattice (LDCML). Through a large number of simulation experiments and theoretical analysis, it can be proved that a chaotic region has the larger parameter space, and the system is more chaotic compared with traditional CML by the introduction of a dynamic coupled method, which is more suitable for chaotic encryption and secure communications. So, this paper presents a bit-level adaptive image encryption algorithm based on this system, and further demonstrates the good chaos of the system from the aspect of encryption performance.

INDEX TERMS Logistic-dynamic, CML, parameter space, dynamic coupling, image encryption.

I. INTRODUCTION

Since Lorenz proposed chaos theory in 1963, chaos theory has gradually formed a set of concrete and practical theoretical system after several decades of development and improvement, and has achieved good results in the fields of cryptography and secure communication. The research on chaos system has also mainly gone through the stages from low dimensional to high dimensional to spatiotemporal chaos. In the recent years, with the further research on chaotic systems, the low dimensional and high dimensional chaotic systems are gradually well known. Spatiotemporal chaos is favored by its complex dynamic behavior [1]–[5]. Since Kaneko [1] proposed the coupled logistic map lattice model (CML) spatiotemporal chaos system, the follow-up people have done a lot of expansion and deepening in the spatiotemporal chaos field. Khellat *et al.* [2] proposed Globally Nonlocal Coupled Map Lattice (GNCML), and Meherzi *et al.* [3] proposed One-Way Coupled Map Lattice (OCML). Then Liu and Yu [4] proposed Two-Way coupled logistic map lattice (TCML). Sinha [6] proposed a stochastic coupled logistic map lattice model for the first time, Rajesh *et al.* [7], Mondal *et al.* [8], Poria *et al.* [9], and Chen *et al.* [10] have all improved it or proposed the new stochastic coupled logistic map lattice model. Because these are non-adjacent coupled map lattice models and the way of coupling is randomly generated, that is to say it can not be restored, so its use is greatly limited. Later, Arnold coupled logistic map lattice (ACCML) and Mixed Linear-Nonlinear Coupled Logistic Map Lattice were proposed by Zhang and Wang [11], [12]. The dimension of each lattice of coupled logistic map lattice model was also obtained from one-dimensional and two-dimensional [13] to three-dimensional [14] to the four-dimensional [15].

All mentioned above are statically coupled logistic map lattice models, and the research on the dynamic coupled logistic map lattice model is seldom. Therefore, this paper proposes a new Logistic-Dynamics coupled logistic Map lattices (LDCML). Its key idea is to use logistic chaotic map as coupling coefficient, which can ensure that the degree of coupling between each lattice and other lattices is dynamically changing. Introduction of dynamic coupling not only can increase the complexity of spatiotemporal chaos, but also make the energy uniformly diffuse among different lattices, which bring LDCML system the overall stability. Through the analysis of the entropy density, entropy breadth,

bifurcation diagram, information entropy and mutual information, the system is proved to be more robust than the traditional CML and has larger parameters space and stronger chaos. On the one hand, it makes up for the defect of dynamic coupling in the field of chaos theory, on the other hand, it also laid the good foundation for the better application of chaos theory in practice. For this reason, this paper proposes an image encryption algorithm based on LDCML system.

In recent years, people have also proposed a large number of image encryption algorithms based on chaotic systems [16]–[27]. Zhang *et al.* [16] proposed a DNA-level image encryption algorithm based on the MLNCML system. Hua and Zhou [17] proposed a bit-level image encryption algorithm based on 2D Logistic-adjusted-Sine map. Khan *et al.* [18] proposed image encryption algorithm based Non-linear Chaotic Map (NCA) and Substitution Boxes. Hussain *et al.* [19] proposed an image encryption algorithm based on Tangent Delay Ellipse Reflecting Cavity Map System (TD-ERCS) and Piecewise Linear Chaotic Map (PWLCM). This paper proposes an bit- level adaptive image encryption algorithm based on LDCML system and harsh-512. On the one hand, LDCML is more complex than the low dimensional chaotic system and CML because of introduce of dynamic coupling method, so the phase space reconstruction is more difficult, and the security performance is also better when used for image encryption. On the other hand, LDCML system can provide the wider secret key space, which can effectively resist violent attacks. In addition, Through the analysis of encryption performance, the good chaos of LDCML system is proved from the perspective of practical application.

The paper is divided into four sections. The first section introduces the LDCML model. In the second section, the chaos performance of the model is analyzed from various angles. In the third section, the image encryption algorithm based on LDCML system is proposed and its performance is analyzed. The last section summarizes the full paper and proposes the further work.

II. INTRODUCTION OF LDCML MODEL

The traditional coupled logistic map lattice model (CML) proposed by Kaneko [1]:

$$x_{n+1}(i) = (1-e)(f(x_n(i))) + (e/2)(f(x_n(i-1)) + f(x_n(i+1))). \quad (1)$$

In this model, the parameter e is coupling coefficient and $0 \le e \le 1$, the parameter $n(n = 1, 2, 3, \ldots)$ is time sequence. The parameter i is lattice number and $1 \le i \le L$. $i+1$ or $i-1$ is lattice which is adjacent with i. The function $f(x) = \mu x(1-x)$ is logistic map which is proposed by May [28]. The boundary conditions are that $i+1 = 1$ when $i = L$ and $i-1 = L$ when $i = 1$, which can ensure that lattice is in the range of $(1, L)$.

The above mentioned CML spatiotemporal chaos system has a simple structure, whose chaos is only determined by the parameter μ and e. The most important is that chaos of a large number of lattices in the CML will diminish and even disapper when $e < 0.3$ or $\mu < 3.8$, which greatly limits the parameter space. In addition, when $e > 0.7$ or $\mu > 3.8$, there are some lattices in a non-chaotic state or exist obvious periodic windows. Therefore, in practical application, only can take a few fixed lattices, which greatly limits the use of CML and reduces its safety. Cause of this phenomenon may be explained by Reaction-diffusion [1], reaction can strengthen chaos and diffusion can weaken chaos by spread of energy among lattices. In the CML, due to the way of adjacent and static coupling, spread of energy among lattices is inhomogeneous which leads to inhomogeneous distribution of different lattices' chaos strength. Therefore, this paper proposes LDCML system based on logistic map, whose coupling coefficient is dynamic, thus causing even distribution of energy and better chaos. LDCML model is:

$$x_{n+1}(i) = (1-L(e))f(x_n(i)) + (L(e)/2)(f(x_n(i-1)) + f(x_n(i+1))). \quad (2)$$

In the LDCML, the meaning of $i, n, f(x)$ is the same as CML and the boundary conditions are also consistent with CML. The difference is that coupling coefficient is e in the CML while coupling coefficient is $L(e) = \mu_2 e(1-e)$ in the LDCML. In order to obtain best dynamic, μ_2 is taken for 3.99 in logistic map $L(e)$.

Next, through the analysis of the Kolmogorov-Sinai entropy, bifurcation diagram, information entropy, space-time behavior and mutual information of LDCML system, it can be proved that LDCML is more advanced than the traditional CML model. In addition, in the paper, the parameter e represents initial value of $L(e)$ in the LDCML while parameter e represents just coupling coefficient in the CML. For specific analysis, number of lattices L is taken for 100 in the paper.

III. ANALYSIS OF LDCML SYSTEM

A. KOLMOGOROV-SINAI ENTROPY OF LDCML

The lyapunov exponent [29] is used to describe the degree of separation of adjacent orbits, which is the very powerful statistical feature for chaotic motion. The larger λ is, the better the chaos of the system is. In general, when λ is greater than 0, the system is in chaos. It is defined as:

$$\lambda = \lim \frac{1}{n} \sum_{i=0}^{n-1} \ln \left| \frac{dF(x)}{dx} \right|_{x=x_i}. \quad (3)$$

where $F(x)$ denotes the function and i denotes time sequence. The spatiotemporal chaos system can be regarded as L-dimensional chaos system, and Kolmogorov-Sinai entropy is the sum of positive lyapunov exponents of all L dimensions. Kolmogorov-Sinai entropy density h is obtained by normalizing them to eliminate the effect of the number of lattices. h is defined in Eq. (4).

$$h = \frac{\sum_{i=1}^{L} \lambda^+(i)}{L}. \quad (4)$$

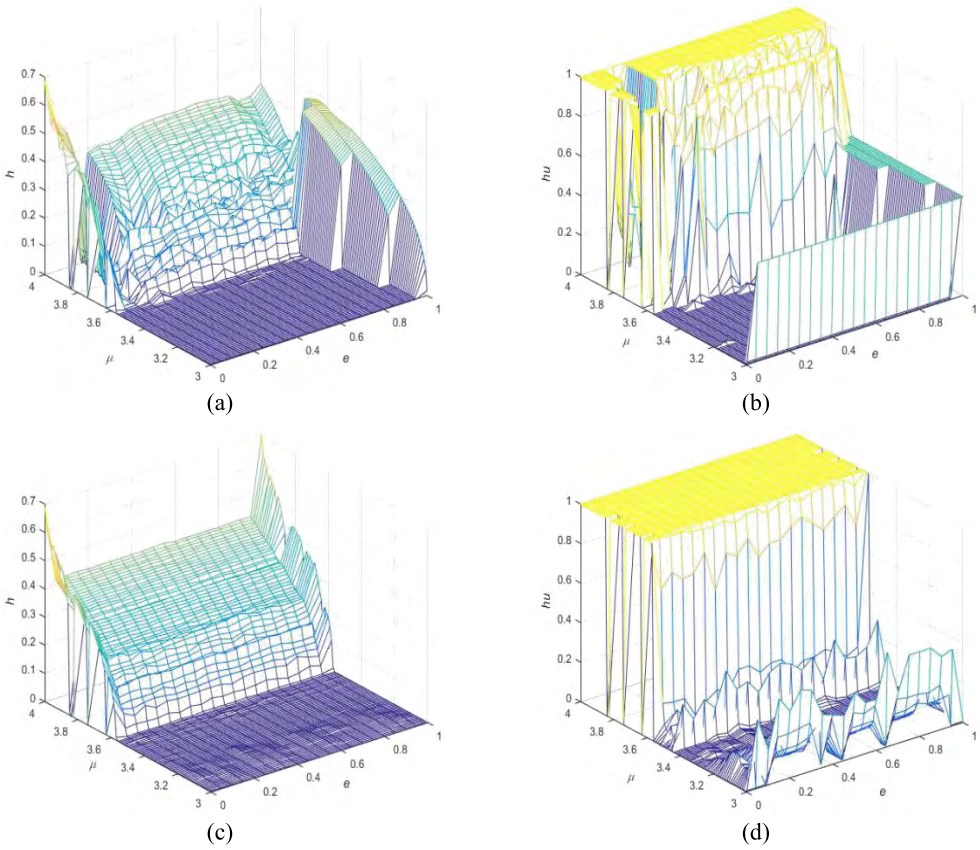


FIGURE 1. Fig. 1 Kolmogorov-Sinai entropy analysis of system. (a) Kolmogorov-Sinai entropy density of CML. (b) Kolmogorov-Sinai entropy breadth of CML. (c) Kolmogorov-Sinai entropy density of LDCML. (d) Kolmogorov-Sinai entropy breadth of LDCML.

In addition, in order to better describe the chaos of each lattice in spatiotemporal chaos system, Zhang proposed Kolmogorov-Sinai entropy breadth. It is

$$hu = \frac{L^+}{L}, \tag{5}$$

where L^+ is the number of L lattices with positive lyapunov exponents.

From Fig. 1(a) and Fig. 1(b), it can be found that many lattice lose chaos or have poor chaos at $\mu \leq 3.8$ or $e \in (0.13, 0.19)$ in the CML. While in the LDCML (as is shown in Fig. 1(c) and Fig. 1(d)), there is no such defect. Specifically, when $\mu > 3.57$, there are almost about 100% (μ, e) parameter pair make all lattices of system in chaos in the LDCML and the average Kolmogorov-Sinai entropy density is about 0.28559, while there are only about 47% (μ, e) parameter pair make all lattices of system in chaos in the CML and the average Kolmogorov-Sinai entropy density is just about 0.23333. Obviously, chaos of Kolmogorov-Sinai entropy of LDCML is better than CML in the whole.

Moreover, remove the defect parameters section of the CML system, when $\mu > 3.8$ and $e \in [0, 0.13] \cup [0.19, 1]$, there are about 88.571% (μ, e) parameter pair make all lattices in chaos and the average Kolmogorov-Sinai entropy density is about 0.328997. While at the time, there are 99.047% (μ, e) parameter pair make all lattices in chaos in the LDCML and the average Kolmogorov-Sinai entropy density is about 0.3701364, which are also all better than that of the CML. Therefore, from analysis of Kolmogorov-Sinai entropy, we can conclude that in the whole chaos of LDCML is better than CML. Because of introduce of dynamic coupled method, LDCML not only makes up defect of CML, but also enhances chaos of CML.

In addition, from Fig. 1(c), it also can be found that change of initial value e of $L(e)$ have vary little influence on chaos of system in LDCML, which is different from that of CML.

B. BIFURCATION DIAGRAM OF LDCML

From analysis of Kolmogorov-Sinai entropy in Section III.A, we know that change of initial value e have little influence on chaos of LDCML. So, when analyzing bifurcation diagram of each lattice of LDCML, e is taken for a fixed value 0.43423413435. Without loss of generality, we take the first, the 50th and 100th lattice to analyze bifurcation diagrams of different lattices of system (as is shown in Figs. 2(a)-(f) and Figs. 3(a)-(c)). In the CML, when $e \in (0.13, 0.19)$, CML will lose chaos, which is shown in Figs. 2(d)-(f). At $e = 0.15$, it can be found easily that these three lattices of CML have lost chaos. When $e \notin (0.13, 0.19)$ and $\mu \leq 3.8$ (as is shown in Figs. 2(a)-(c)), there are many obvious period

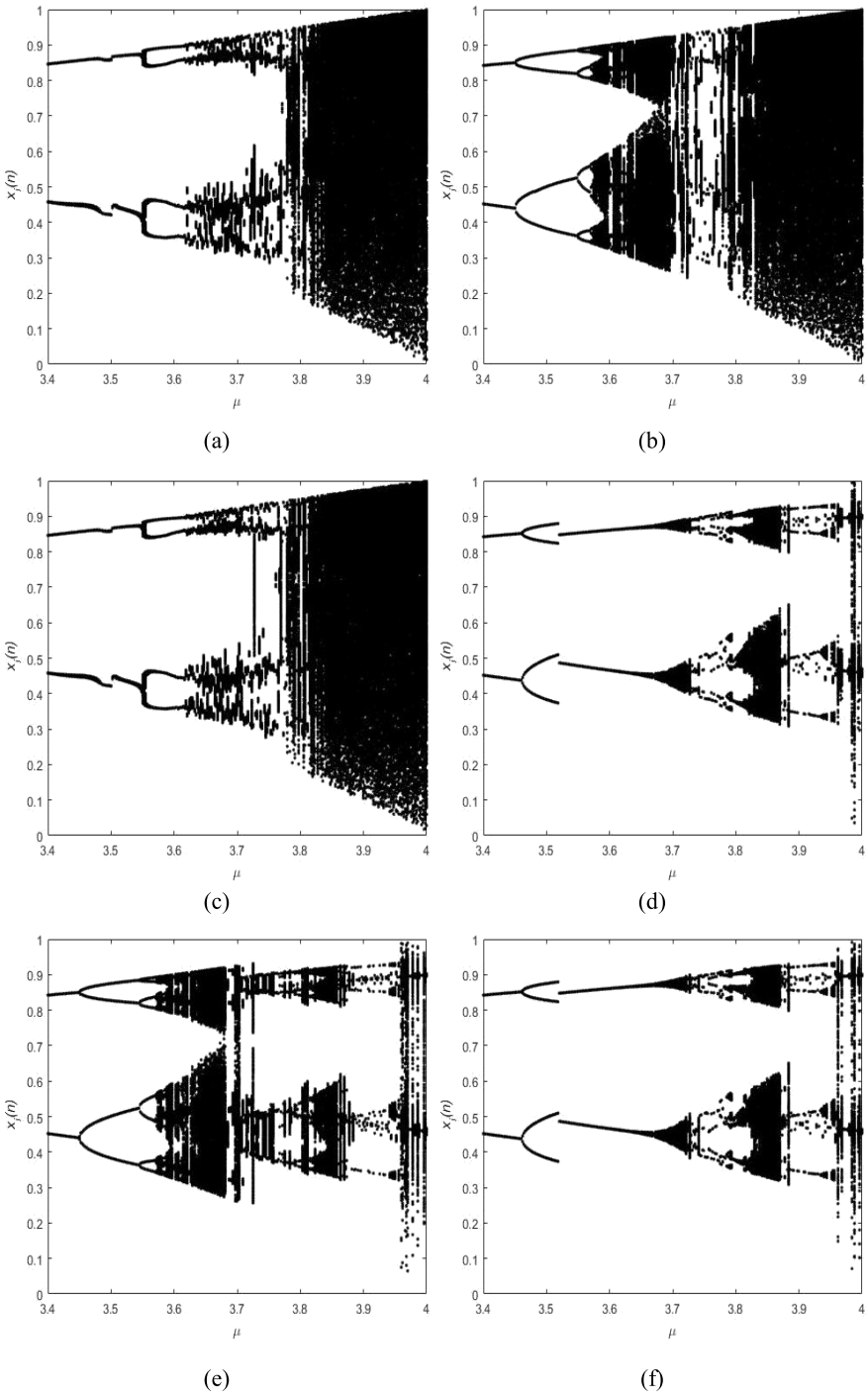


FIGURE 2. Bifurcation diagrams of lattices of CML. (a) Bifurcation diagram of the first lattice of CML at. (b) Bifurcation diagram of the 50th lattice of CML at $e = 0.8$ (c) Bifurcation diagram of the 100th lattice of CML at $e = 0.8$ (d) Bifurcation diagram of the first lattice of CML at $e = 0.15$ (e) Bifurcation diagram of the 50th lattice of CML at $e = 0.15$ (f) Bifurcation diagram of the 100th lattice of CML at $e = 0.15$.

windows in the bifurcation diagram and chaos of system is poor. While in the LDCML, due to introduce of dynamic coupling, chaos of the system (as is shown in Figs. 3(a)-(c)) has been improved significantly compared with CML. Obviously, there is no any period window in Figs. 3(a)-(c) and chaos of system is better than CML.

C. MUTUAL INFORMATION BETWEEN DIFFERENT LATTICES

Mutual information is used to describe the degree of correlation between two different sequences. When mutual information is equal to 0, it indicates that these two different sequences are independent. It can be

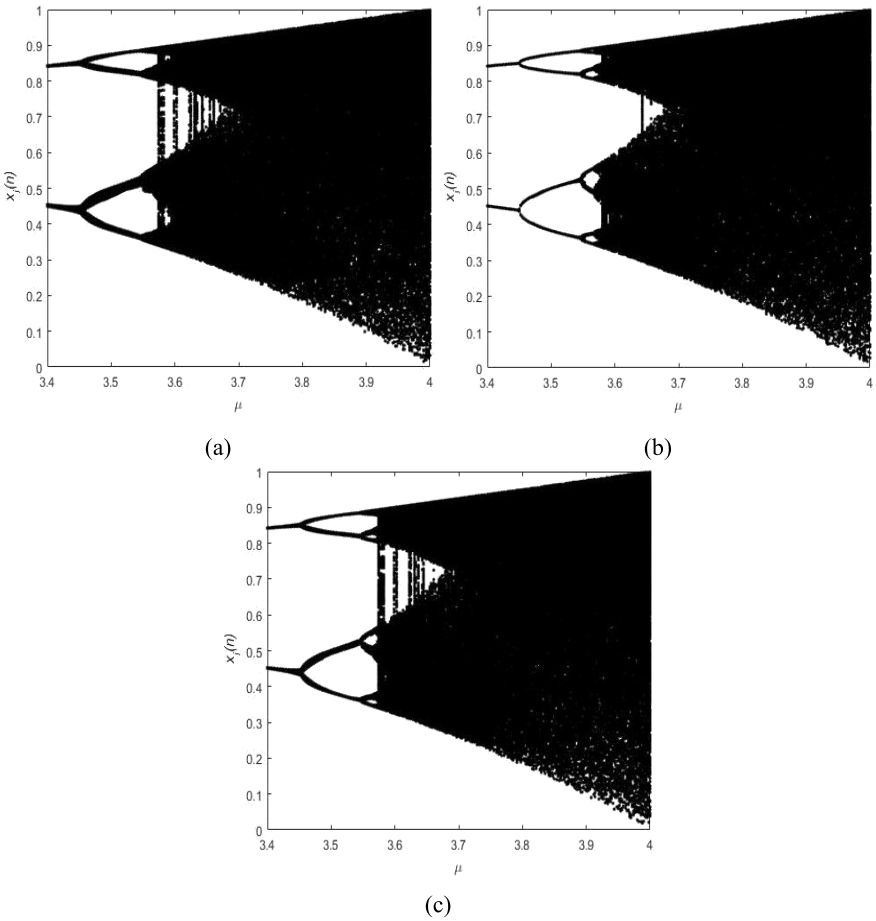


FIGURE 3. Bifurcation diagram of lattices of LDCML. (a) Bifurcation diagram of the first lattice of LDCML. (b) Bifurcation diagram of the 50th lattice of LDCML. (c) Bifurcation diagram of the 100th lattice of LDCML.

defined as:

$$I(X(i), X(j)) = H(X(i)) - H(X(i)|X(j)). \tag{6}$$

In the Eq. (6), $X(i) = (x_i(1), x_i(2), x_i(3), \ldots, x_i(n)), X(j) = (x_j(1), x_j(2), x_j(3), \ldots, x_j(n))$, which denote the two different sequences composed of the values of lattice i and j at different moments. $H(X(i))$ denotes information entropy, which is defined in Eq. (8). In the LDCML and CML, the smaller mutual information between different lattices is, the lower correlation of different lattices is, the less likely that one lattice is restored by another lattice, which indirectly illustrates the security and complexity of the system. In order to analyze mutual information between different lattices when using different parameter pair (μ, e), we normalize mutual information of L lattices. Specifically, as is Eq. (7):

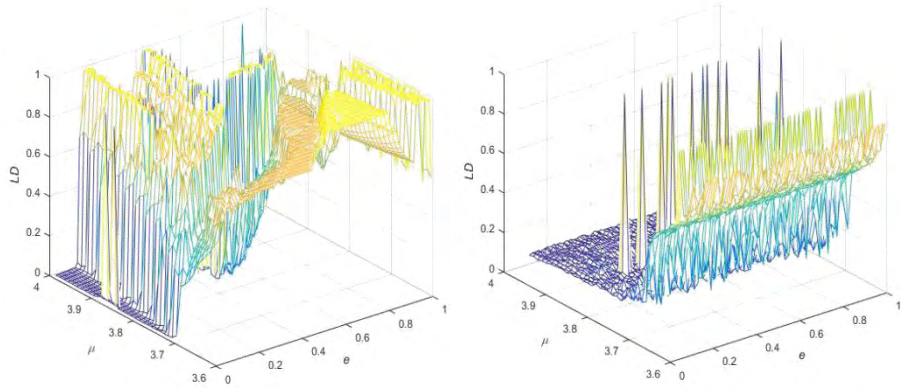
$$Ld = \frac{\sum_{i=1}^{L} \sum_{j=1}^{L, j\neq i} I(X(i), X(j))}{L(L-1)}, \tag{7}$$

where Ld denotes the average mutual information of all lattices. Fig. 4(a) shows Ld of CML and Fig. 4(b) shows Ld of LDCML. When $\mu > 3.57$ and $e \in [0, 1]$, the average Ld in the CML is about 0.59436093, while the average Ld in the LDCML is just 0.247193. It is obvious that Ld of CML is higher than that of LDCML. Specifically, in the CML, when μ approaches 4, chaos of single lattice is strongest. When e approaches 0, coupling between different lattices is the weakest, which means that each lattice is influenced most slightly by lattices coupled with it and the most dispensable. So, as is in Fig. 4(a), when μ approaches 4 and e approaches 0, there are a few of parameter pair (μ, e) make mutual information between different lattices in the CML close to 0. Most of parameter pair (μ, e) will make Ld higher than 0.5. By contrary, in the LDCML, when $\mu > 3.74$, Ld is lower than 0.1, that is to say that mutual information between different lattices is very low and approaches 0.

Obviously, because of introduce of dynamic coupling, correlations between different lattices are impaired greatly.

D. INFORMATION ENTROPY OF EACH LATTICE IN LDCML

According to the confusion principle and ergodicity of chaos system, the value of each iteration of chaos system should be uniformly distributed in [0, 1] interval. Here,



(a) (b)

FIGURE 4. Mutual information of system. (a) Average Mutual information of CML. (b) Average Mutual information of LDCML.

the characteristic of chaotic system can be quantitatively measured by information entropy.

Information entropy was proposed by Shannon in 1948, which characterizes the degree of confusion of the system. The more ordered the system, the lower information entropy it has. The more disordered the system, the higher information entropy it has. It is defined as:

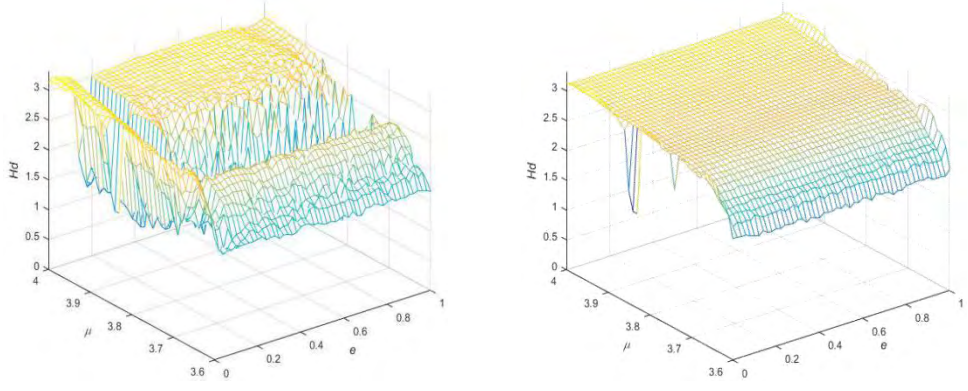
$$H(s) = -\sum_{i=1}^{n} P(s_i)\log_2(p(s_i)), \tag{8}$$

where s is information source and is the lattices in the LDCML. n represents how many states each lattice has, which is taken for 10 in this paper. Specifically, the 10 states are $s_1 = [0, 0.1)$, $s_2 = [0.1, 0.2)$, $s_3 = [0.2, 0.3)$, $s_4 = [0.3, 0.4)$, $s_5 = [0.4, 0.5)$, $s_6 = [0.5, 0.6)$, $s_7 = [0.6, 0.7)$, $s_8 = [0.7, 0.8)$, $s_9 = [0.8, 0.9)$ and $s_{10} = [0.9, 1.0]$. In addition, $p(s_i)$ indicates the probability of occurrence of s_i. So in theory, the maximum information entropy of each lattice is $\log_2 10 \approx 3.32$. Similarly, information entropy of L lattices are normalized, as follows:

$$Hd = \frac{\sum_{i=1}^{L} H(i)}{L}, \tag{9}$$

where Hd denotes average information entropy of L lattices.

When $\mu \in [3.6, 4]$ and $e \in [0, 1]$, Hd of CML and LDCML are shown in Fig. 5(a)-(b). As previous analysis of Kolmogorov-Sinai entropy (see Section III.A), at $\mu < 3.8$ or $e \in (0.13, 0.19)$, many lattices in the CML will lose chaos, so average information entropy of system is low and approach 1.5 in general. Moreover, when $\mu \in [3.6, 4]$ and $e \in [0, 1]$, the average Hd is about 2.39809. If the defected parameter area is removed, the average Hd is around 2.802932 in the CML. While in the LDCML, average Hd is up to 3.006486 and more approaches the idea value 3.32, which is obviously higher than that in the CML. In addition, in the whole, Hd of both CML and LDCML increase with μ increasing. Moreover, increase of μ in the system means enhancement of chaos of the system. So, to some extend, the larger Hd is, the more powerful chaos of system is.



(a) (b)

FIGURE 5. Analysis of the average information entropy. (a) The average information entropy of CML. (b) The average information entropy of LDCML.

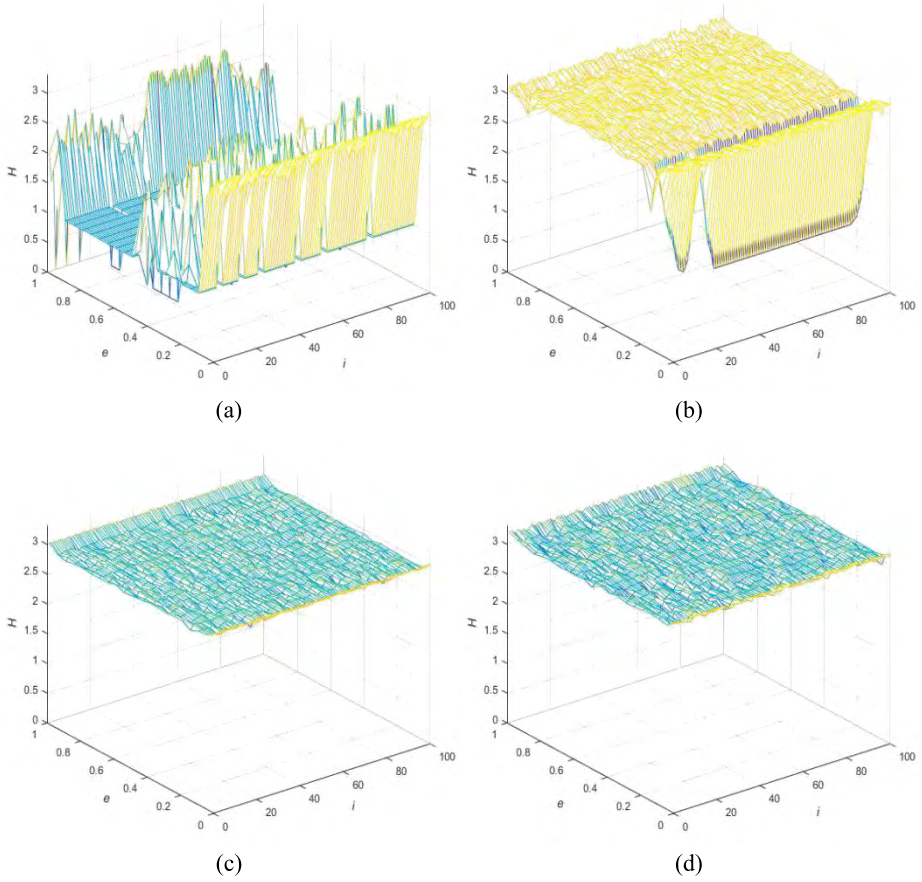


FIGURE 6. Analysis of information entropy of each lattice of system. (a) Information entropy of each lattice of CML at $\mu = 3.78$. (b) Information entropy of each lattice of CML at $\mu = 3.99$. (c) Information entropy of each lattice of LDCML at $\mu = 3.78$. (d) Information entropy of each lattice of LDCML at $\mu = 3.99$.

More meticulously, Fig. 6(a) or Fig. 6(b) shows information entropy of each lattice of the CML when $\mu = 3.78$ or $\mu = 3.99$ and $e \in [0, 1]$. Fig. 6(c) or Fig. 6(d) shows information entropy of each lattice of the LDCML when $\mu = 3.78$ or $\mu = 3.99$ and $e \in [0, 1]$. By comparison, it is easy to find that many lattices of the CML exists defect at at $\mu < 3.8$ or $e \in (0.13, 0.19)$ and LDCML makes up the defect.

Finally, we can conclude that ergodic and random of the LDCML are better that that of the CML.

E. SPACE-TIME BEHAVIOR OF LDCML SYSTEM

According to the research of Kaneko [1], CML system has six kinds of space-time behavior pattern, namely frozen random pattern, pattern selection pattern, defect turbulence pattern, defect diffusion pattern, pattern competition intermittent chaos pattern and complete turbulence pattern. Moreover, in the CML, space-time behavior pattern is determined by μ and e.

While in the LDCML, the initial value e of coupling coefficient $L(e)$ as same as the initial values of lattices only affects the location of chaotic pattern in the space-time behavior pattern, but does not change the space-time behavior pattern. Moreover, the change of the space-time behavior pattern is only decided by μ. So, for simplicity, e is taken for 0.323436536 when analyze space-time behaviour of LDCML

In addition, compared with CML, because of the introduction of dynamic coupling method, LDCML can enter complete turbulence pattern faster and does not exist defect turbulence pattern and defect diffusion pattern. Specific is following.

1) WHEN $\mu < 3.57$

At $\mu \leq 3$, chaos does not exist in the LDCML and as is shown in Fig. 7(a), there is only one-period. When $\mu > 3$, in the space-time behavior map, the thin-long X-shaped chaotic zones and two-period gradually emerge (as is shown in Fig. 7(b)) and their positions are determined by different initial value e and $x_i(0)$. As μ increasing, X-shaped chaotic zones gradually widen (as is shown in Fig. 7(c)). When μ is up to about 3.455, two-period becomes four-period and X-shaped chaotic zones further widen, which is shown in Fig. 7(d). When μ is about 3.5, four-period becomes eight-period, which is shown in Fig. 7(e). Finally, at $\mu = 3.57$, the

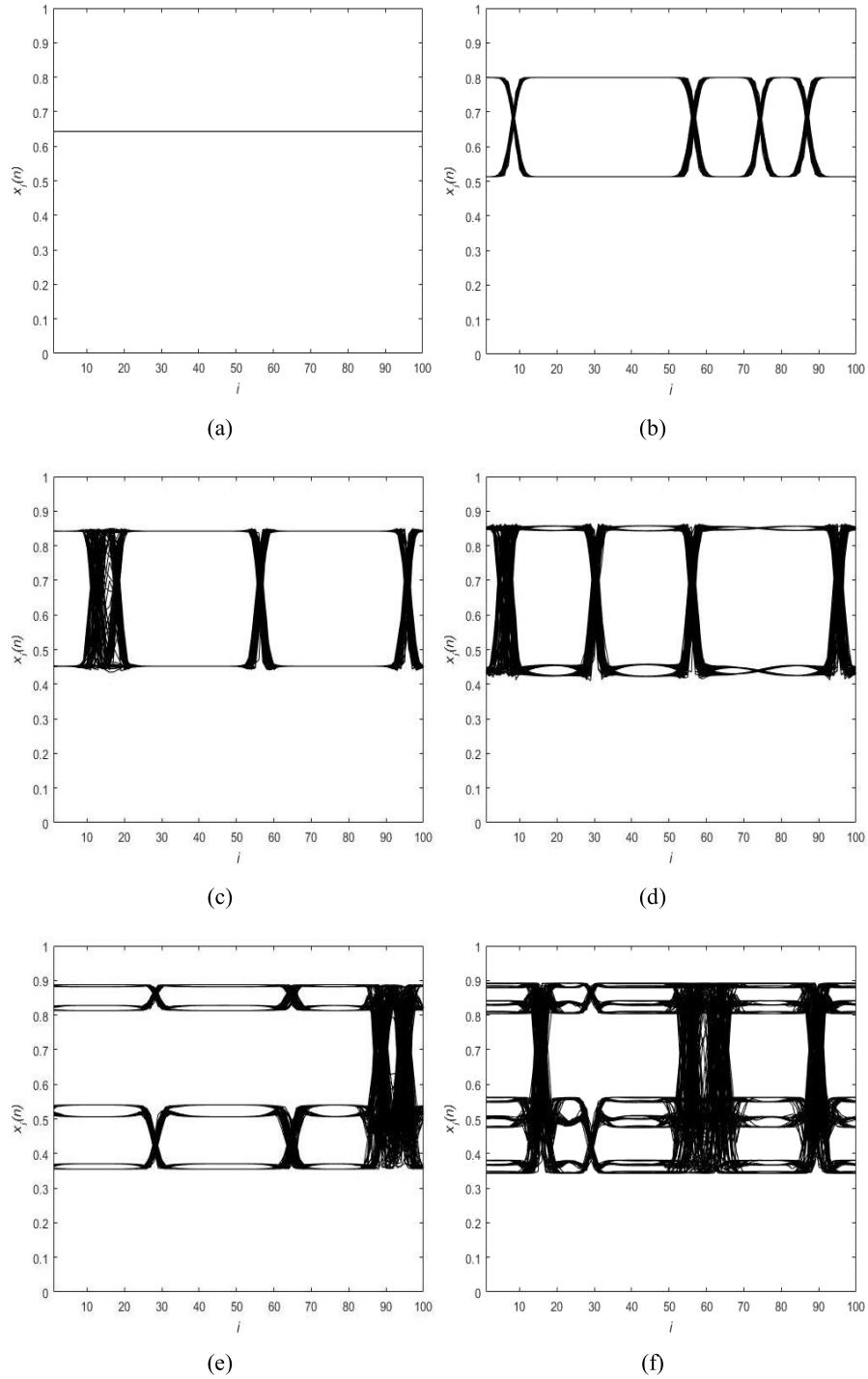


FIGURE 7. Space-time behaviour at $\mu < 3.57$. (a) Space-time behaviour at $\mu = 2.8$. (b) Space-time behaviour at $\mu = 3.01$. (c) Space-time behaviour at $\mu = 3.4$ (d) Space-time behaviour at $\mu = 3.455$. (e) Space-time behaviour at $\mu = 3.5$. (f) Space-time behaviour at $\mu = 3.57$.

obvious period phenomenon is no longer recognizable and the circular chaotic zone begins to appear in the space-time behaviour map, which is shown in Fig. 7(f).

2) WHEN $\mu \in (3.57, 3.75]$

As is shown in Fig. 8(a), when $\mu = 3.58$, there are obviously circular and X-shaped chaotic zones in the space-time behavior map. Different e and $x_i(n)$ will make different number of X-shaped chaotic zones appear in different locations. As μ increasing, the circular chaotic zone begins to be compressed and extends to both sides, which means that the two chaotic orbits begin to approach each other (see Figs. 8(b)-(c)). When μ is taken for 3.7, the two chaotic orbits have begun to merge and the circular chaotic zone is

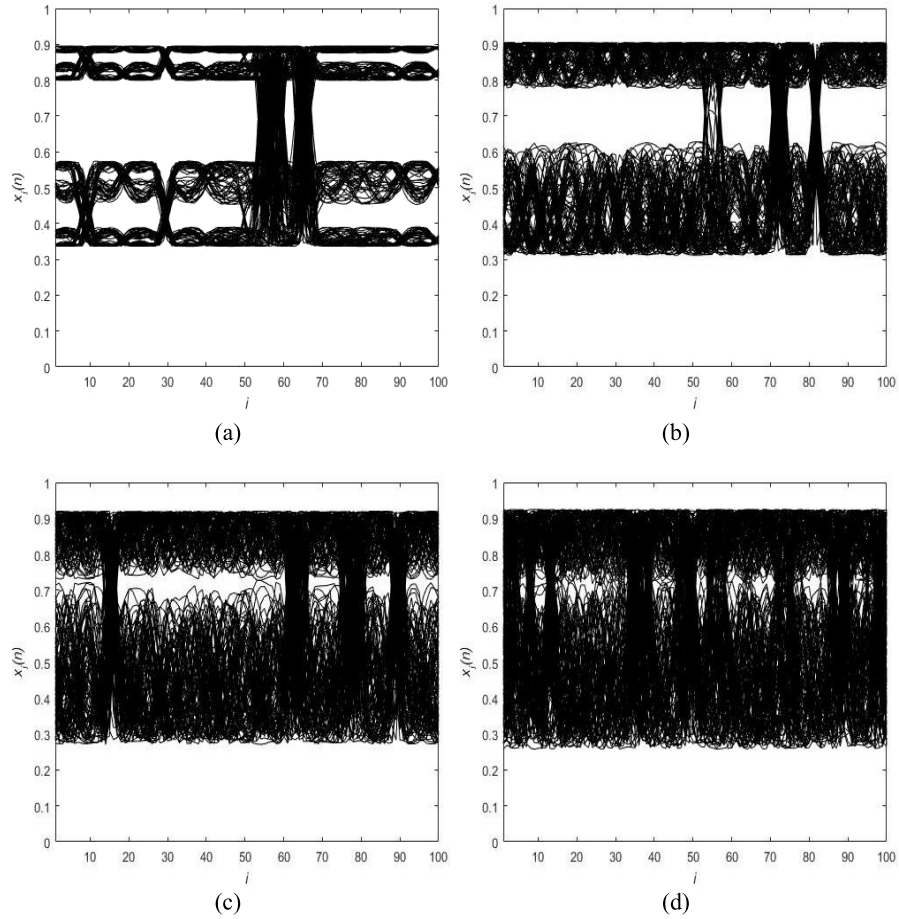


FIGURE 8. Space-time behaviour of LDCML at $\mu \in (3.57, 3.75]$. (a) Space-time behaviour at $\mu = 3.58$. (b) Space-time behaviour at $\mu = 3.62$. (c) Space-time behaviour at $\mu = 3.68$. (d) Space-time behaviour at $\mu = 3.7$.

invisible, which cause more X-shaped chaotic zones begin to appearing, which is shown in Fig. 8(d).

3) WHEN $\mu \in (3.7, 4]$

As μ increasing further, there are more and more X-shape chaotic zone appearing in space-time behaviour map. Finally, when $\mu = 3.75$, LDCML enters into complete chaos turbulence pattern, which is shown in Fig. 9(a). Then, with the further increase of μ, the chaotic zone will extend to both sides. At $\mu = 3.8$, $\max(x_i(n)) \approx 0.95$ and $\min(x_i(n)) \approx 0.1808$, which is shown in Fig. 9(b). At $\mu = 3.9$, $\max(x_i(n)) \approx 0.975$ and $\min(x_i(n)) \approx 0.095$. Finally, when μ is up to 4, $x_i(n)$ is filled with [0, 1], which is shown in Fig. 9(d).

From analysis of space-time behaviour above, it can be known that because chaos of system is mainly affected by coefficient μ in the LDCML, space-time behavior is more simple compared with that of CML (see [1], [11]). Moreover, in the CML, only at $\mu > 3.85$, can system enter complete chaos turbulence pattern, while in the LDCML system can enter complete chaos turbulence pattern just at $\mu \approx 3.75$. That is to say that system can faster enter best chaos by introduction of dynamic coupling method. It may be explained that because coupling coefficient $L(e)$ is also in chaos, which can enhance uncertainty of spatiotemporal chaos system, so chaos of all lattices are significantly strengthen.

IV. APPLICATION IN IMAGE ENCRYPTION

In order to further demonstrate the practical significance of LDCML system and excellent chaos, this paper proposed a new image encryption algorithm based on LDCML system.

A. INTRODUCTION OF ALGORITHM

1) ENCRYPTION PROCESS

Step 1: Use harsh-512 for the plaintext P sized $r \times c$ and secret key K with the length of 480 bits is generated.

Step 2: The key K is divided into 12 groups of 40-bits subkeys (k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8, k_9, k_{10}, k_{11}, k_{12}) and converted into decimal (b_1, b_2, b_3, b_4, b_5, b_6, b_7, b_8, b_9, b_{10}, b_{11}, b_{12}) in the interval [0,1], where (b_1, b_2, b_3, b_4, b_5, b_6, b_7, b_8, b_9) is the initial values of the 9 lattices of the LDCML system. The coefficient is $\mu = 3.99 + 0.01 \times b_{10}$, $\mu_2 = 3.99 + 0.01 \times b_{11}$, $e = 0.01 + 0.99 \times b_{12}$.

Step 3: Iterate the LDCML system $2 \times \max(r, c)$ times. Set $d\_one = 0$, $d\_zero = 0$. For the value x_{ij} of jth iteration of

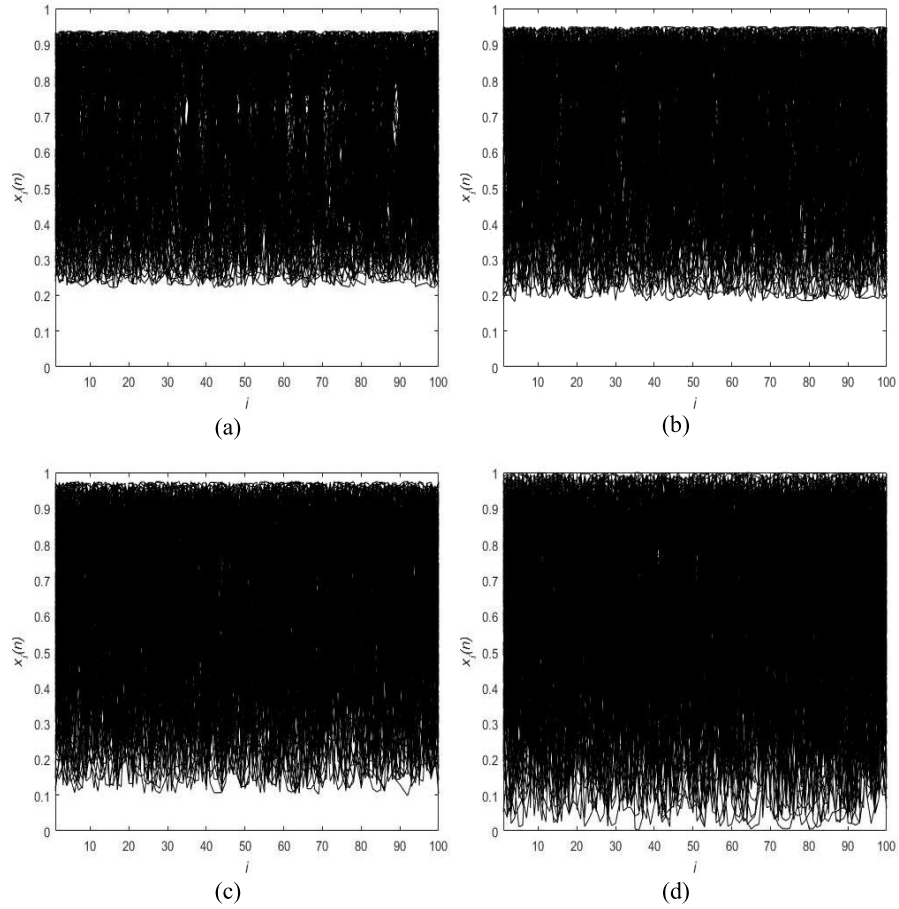


FIGURE 9. Space-time behaviour when $\mu \in$ (3.7, 4]. (a) Space-time behaviour at $\mu = 3.75$. (b) Space-time behaviour at $\mu = 3.8$. (c) Space-time behaviour at $\mu = 3.9$. (d) Space-time behaviour at $\mu = 4$.

each lattice ith, if $x_{ij} \geq 0.5$, let $d\_one = d\_one + 1$, $Z_i(j) = 1$, $V_i(d\_one) = \text{floor}\,(\text{mod}\,(x_{ij} \times 10^{14}, c)) + 1$, if $x_{ij} < 0.5$, let $d\_zero = d\_zero{+}1$, $Z_i(j) = 0$, $V\_zero_i(d\_zero) = \text{floor}\,(\text{mod}\,(x_{ij} \times 10^{14}, r)){+}1$. Finally, 9 groups of permutation bit streams Z_i and corresponding permutation values V_i and V_zero_i are obtained. In addition, the value y_0 of the last iteration of the first lattice is taken for the initial value of the diffusion.

Step 4: Pixel level permutation is performed on plaintext P with Z_1 and corresponding permutation values V_1 and V_zero_1. The specific permutation process is as follows.

I. Set initial values $d\_one = 1$, $d\_zero = 1$, $j = 1$.

II. Scans Z_1 from left to right. If $Z_1(j) == 1$, the d_oneth row of P is left shifted circularly by $V_1(d\_one)$ times and let $d\_one = d\_one{+}1$, $j = j + 1$. if $Z_1(j) == 0$, the d_zeroth column of P is upward shifted cyclically by $V\_zero_1(d\_zero)$ times and let $d\_zero = d\_zero{+}1$, $j = j + 1$.

III. If $d\_one > r$, let $d\_one = 1$. If $d\_zero > c$, let $d\_zero = 1$. It means that if the index d_one or d_zero exceeds the length or width of the image, the first row or first column is re-scanned and the shift value becomes $V_1(d\_one{+}r)$ or $V\_zero_1(d\_zero{+}c)$. Then return to II.

IV. If $j = 2 \times \max(r, c) + 1$, the permutation ends and P_1 is output.

Step 5: P_1 is divided into 8 binary matrices, which include $A_1, A_2, A_3, A_4, A_5, A_6, A_7, A_8$ according to Eq. (10). Then, $A_1, A_2, A_3, A_4, A_5, A_6, A_7, A_8$ are permuted into $B_1, B_2, B_3, B_4, B_5, B_6, B_7, B_8$ using the permutation sequence $Z_2, Z_3, Z_4, Z_5, Z_6, Z_7, Z_8, Z_9$ and corresponding permutation values as the method in *Step 4*.

$$A_k = \text{dec2bin}(P_1)_{i,8(k-1)+j}, \tag{10}$$

where $i(i \in [1, r])$ indicates row, $j(j \in [1, c])$ indicates column, dec2bin denotes converting decimal number into binary number of 8-bit.

Step 6: Use y_0 as the iterative initial value of logistic map $y_n = 4y_n\,(1 - y_n)\,(n = 1, 2, 3 \ldots, r \times c)$. If $y_n \geq 0.5$, $y_n = 1$. if $y_n < 0.5$, $y_n = 0$. The binary matrix Y is obtained after $r \times c$ iterations. Let Y = reshape $(Y, [r, c])$, which means converting Y to a binary matrix sized $r \times c$. Before performing the specific diffusion operation, we first introduce an adaptive binary matrix shift method. The specific method is as follows:

I. Input matrix Y.

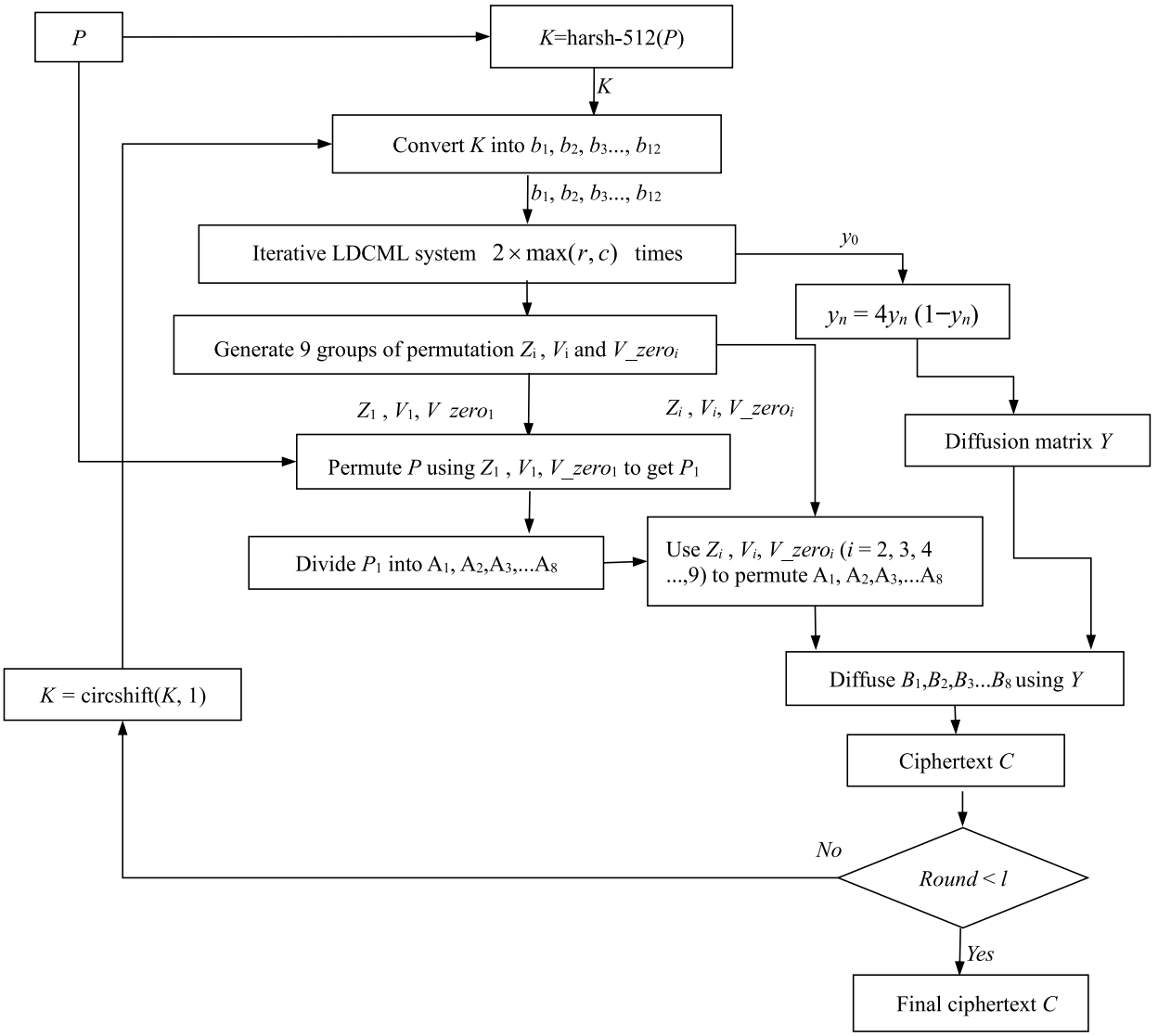


FIGURE 10. Encryption flow chart.

II. i is the row index, j is the column index, so $Y(i, j)$ is the value of ith *row* and jth column of the matrix. Make

$$total = \sum_{i=1}^{r} \sum_{j=1}^{c} Y(i, j) \times ((c-1) \times i + j).$$

III. The matrix Y is left shifted circularly by ($total$ mod c)+ 1 times, and then upward shifted circularly by ($total$ mod$r$)+ 1 times. Finally Y' is output and define $Y' = \mathrm{Ex}(Y)$.

Use Y to do the operations on B_1, B_2, B_3, B_4, B_5, B_6, B_7, B_8 as Eq. (11), and then combine the results D_1, D_2, D_3, D_4, D_5, D_6, D_7,D_8 into ciphertext C.

Step 7: If encryption rounds is less than l given encryption rounds. The key K is left shifted cyclically by one bit to obtain K, and return to *Step 2*. If encryption rounds is equal to l, the encryption ends and obtain the final ciphertext C.

Encryption is shown in Fig. 10.

$$\begin{cases} D_1 = \mathrm{bitxor}(B_1, Y) & D_5 = \mathrm{bitxor}(B_5, Y) \\ Y = \mathrm{Ex}(Y) & Y = \mathrm{Ex}(Y) \\ D_2 = \mathrm{bitxor}(B_2, Y) & D_6 = \mathrm{bitxor}(B_6, Y) \\ Y = \mathrm{Ex}(Y) & Y = \mathrm{Ex}(Y) \\ D_3 = \mathrm{bitxor}(B_3, Y) & D_7 = \mathrm{bitxor}(B_7, Y) \\ Y = \mathrm{Ex}(Y) & Y = \mathrm{Ex}(Y) \\ D_4 = \mathrm{bitxor}(B_4, Y) & D_8 = \mathrm{bitxor}(B_8, Y) \\ Y = \mathrm{Ex}(Y) \end{cases} \tag{11}$$

2) DECRYPTION PROCESS

Step 1: Input secret key K, let $K = \mathrm{circshift}(K, l-1)$ (rotate K to the left $l-1$ bits).

Step 2, ***Step 3:*** As same with the encryption, the key K is combined with the LDCML system to obtain permutation sequences Z_i, V_i, V_zero_i and initial values y_0 for diffusion.

Step 4: With reference to the *Step 6* of encryption, the initial value y_0 is brought into the logistic map $y_n = 4y_n(1 - y_n)$ $(n = 1, 2, 3 \ldots, r \times c)$ to obtain the diffusion binary matrix Y. The ciphertext C is divided into eight groups of bit matrix D_1, D_2, D_3, D_4, D_5, D_6, D_7, D_8. Decrypt them with Y, the specific operation is in Eq. (12)

Step 5: Permute $B_1, B_2, B_3, B_4, B_5, B_6, B_7, B_8$ with $Z_2, Z_3, Z_4, Z_5, Z_6, Z_7, Z_8, Z_9$ and corresponding permutation values, the exact permutation method is the opposite of encryption. The permutation bitstream Z_i is scanned forward from the last bit. If $Z_i(j) == 1$, B_i is right shifted cyclically. If $Z_i(j) == 0$, B_i is shifted downwards cyclically . Finally, $A_1, A_2, A_3, A_4, A_5, A_6, A_7, A_8$ are obtained and combined into a decimal pixel matrix P_2.

Step 6: Permute P_2 with Z_1 and corresponding permutation values, and permutation process is also opposite of encryption.

Step 7: If decryption rounds is less than l, let $K = \text{circshift}(K, -1)$ (rotate K to the right by one bit) and return to *Step 2*. If the decryption round is equal to l, decryption ends

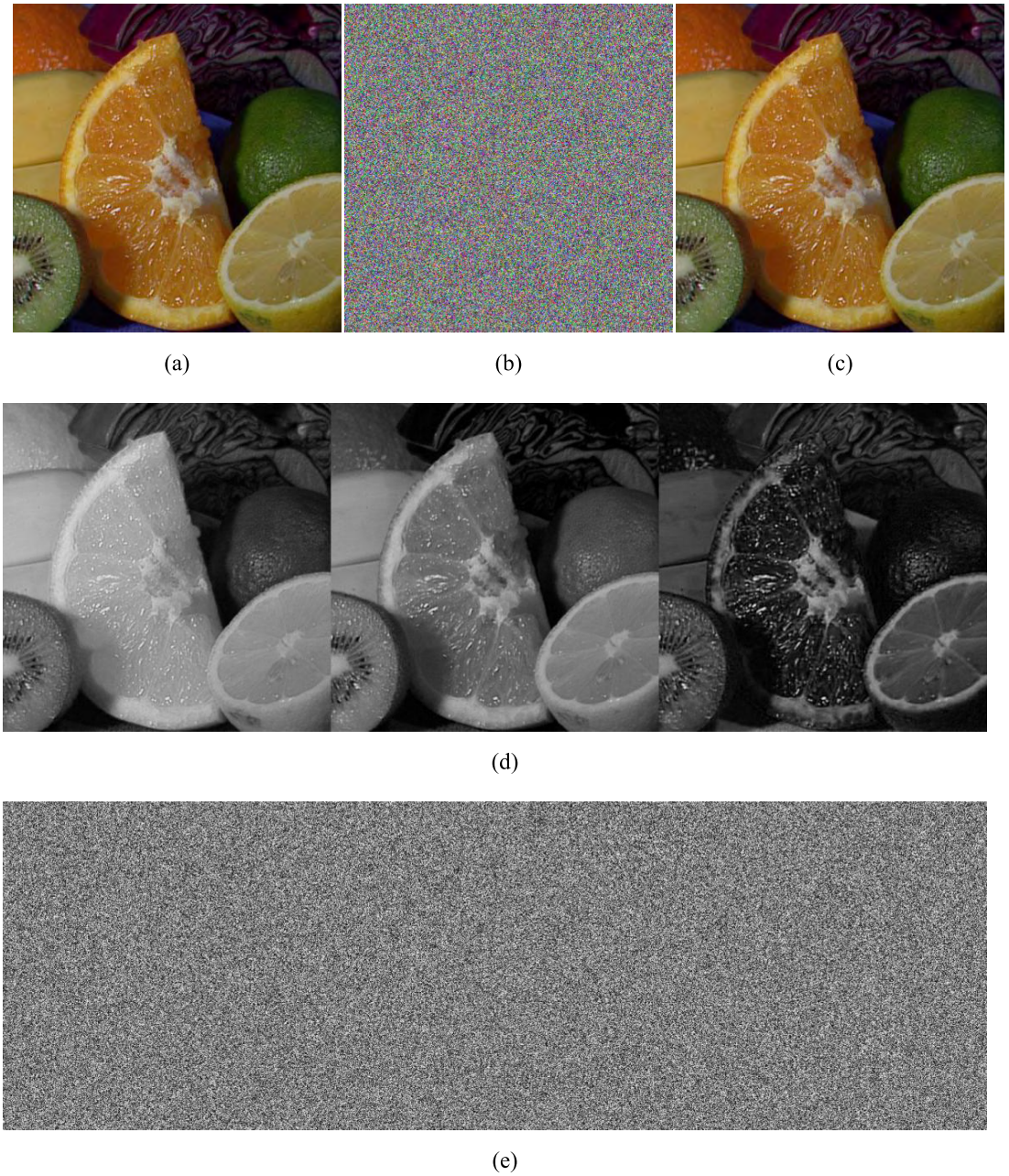


FIGURE 11. Color image encryption. (a) Fruits_color image. (b) Encrypted Fruits_color. (c) Decrypted Fruits_color. (d) The image formed by concatenating the R, G, and B components of Fruits_color. (e) The image formed by concatenating the R, G, and B components of encrypted Fruits_color.

and the final plaintext P is obtained.

$$\begin{cases} B_1 = \text{bitxor}(D_1, Y) & B_5 = \text{bitxor}(D_5, Y) \\ Y = \text{Ex}(Y) & Y = \text{Ex}(Y) \\ B_2 = \text{bitxor}(D_2, Y) & B_6 = \text{bitxor}(D_6, Y) \\ Y = \text{Ex}(Y) & Y = \text{Ex}(Y) \\ B_3 = \text{bitxor}(D_3, Y) & B_7 = \text{bitxor}(D_7, Y) \\ Y = \text{Ex}(Y) & Y = \text{Ex}(Y) \\ B_4 = \text{bitxor}(D_4, Y) & B_8 = \text{bitxor}(D_8, Y) \\ Y = \text{Ex}(Y). \end{cases} \tag{12}$$

For the color image, we concatenate together its R, G, and B components and then encrypt it. Specifically, Fig. 11(a) is Fruits_color sized 512 × 512, and Fig. 11(d) is the image formed by concatenating R, G, and B components of Fruits_color. Fig. 11(e) is the encrypted Fig. 11(d), and Fig. 11(b) is a synthesized encrypted Fruits_color. Fig. 11(c) is the decrypted Fruits_color. So essentially the encryption of the color image is the encryption of the gray image with three times size of the color image.

B. ALGORITHM PERFORMANCE ANALYSIS

1) INFORMATION ENTROPY ANALYSIS

The essence of the image is a kind of information source. The more uniform the distribution of the pixel values, the less effective information the image contains. The distribution of pixel values can be quantitatively described by the Shannon information entropy. Similar to Eq. (8), the definition of information entropy of the image is as follows:

$$H(s) = \sum_{i=0}^{255} p(s_i) \log_2(p(s_i)), \tag{13}$$

where s denotes the image, and $p(s_i)$ represents the frequency of pixel s_i. Therefore, the upper limit of $H(s)$ is 8, and the larger $H(s)$ is, the more uniform the pixel distribution is. Figs. 12(a)-(f) shows plaintexts and ciphertexts of Lena, Barb and P-0 image whose pixels are all zero. Intuitively, we can not get any valid information from the ciphertext image. Figs. 13(a)-(e) shows pixel distribution histograms about the three images. Obviously, pixel distribution of plaintext image is not uniform, while ciphertext image is uniform and the probability of occurrence of different pixels are almost equal. Table 1 shows information entropy of the images before and after being encrypted. It can be found that information entropy of ciphertext image is generally about 7.9992, which is more close to ideal value 8 than other algorithms.

2) THE LOCAL INFORMATION ENTROPY ANALYSIS

Sometimes we not only care about the encryption performance of the image in the whole, but also more care about encryption performance of certain key parts of the image, because these parts may contain more important and critical information. At this time, we can use local information entropy to measure the encryption performance of local

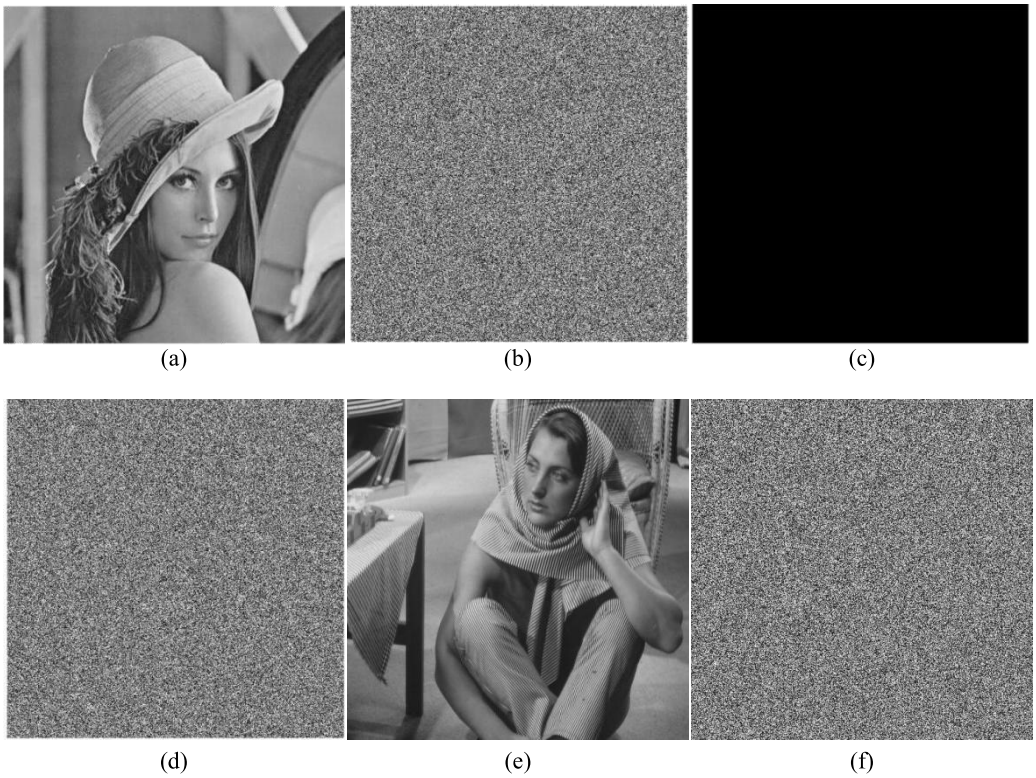


FIGURE 12. Encryption results. (a) Lena. (b) The encrypted Lena. (c) The image *P*-0. (d) The image *C*-0. (e) The image Barb. (f) The encrypted Barb.

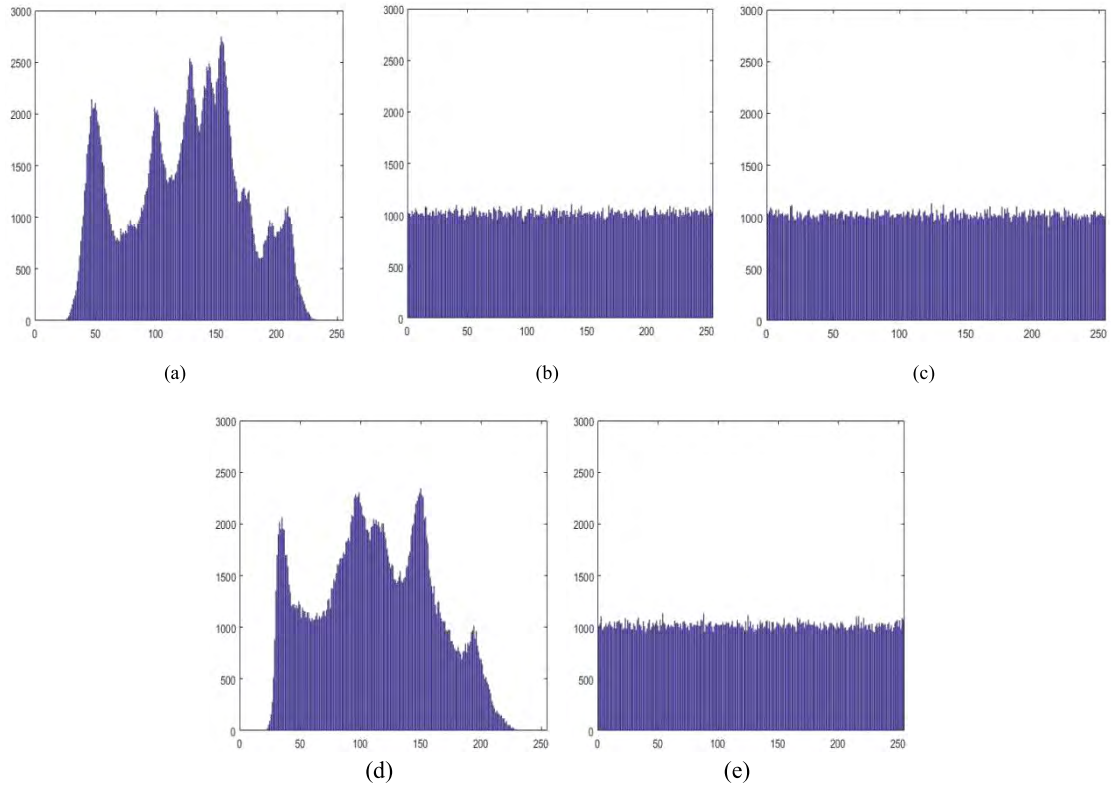


FIGURE 13. Information entropy analysis. (a) Pixel distribution histogram of Lena. (b) Pixel distribution histogram of encrypted Lena. (c) Pixel distribution histogram of *C*-0. (d) Pixel distribution histogram of Barb. (e) Pixel distribution histogram of encrypted Barb.

TABLE 1. Information entropy analysis.

State	Barb	Lena	P-0	Elaine
Plaintext	7.4649	7.4461	0	7.5048
Proposed	7.9992	7.9993	7.9992	7.9993
Ref. [21]	7.9981	7.9981	7.9981	7.9981
Ref. [22]	7.9963	7.9832	7.9958	7.9966
Ref. [25]	7.9972	7.9971	7.9972	7.9971

TABLE 2. Local Information entropy analysis.

Test image	Local information entropy	Result
Lena	7.902393578	Pass
Barb	7.902508032	Pass
P-0	7.902487841	Pass
Elaine	7.902431560	Pass

image. The local information entropy can be defined as:

$$\overline{H_{(k,T_B)}(S_i)} = \sum_{i=1}^{k} \frac{H(S_i)}{k}, \tag{14}$$

where S_i represents an optional set of pixels from the ciphertext image, T_B represents the number of pixels in S_i, k represents that k groups of S_i are selected, and $H(S_i)$ represents the information entropy of S_i. According to [30], T_B is set for 1936, k is taken for 30, confidence level α is taken for 0.05, so the local information entropy should be between [7.901901305, 7.903037329]. Table 2 shows the local information entropy of the encrypted Lena, Barb, P-0, Elaine. It is obvious that the local information entropy of the encrypted ciphertext all passed the test.

3) χ^2 TEST

In addition to information entropy, according to [31], the χ^2 test also can be used to quantitatively describe the distribution of the pixel histogram. It is defined in Eq. (15).

$$\chi^2 = \sum_{i=0}^{255} \frac{(v_i - v)^2}{v}, \tag{15}$$

where v_i denotes frequency of pixel value i appearing in the image, v denotes the average frequency and is taken for $(r \times c)/256$. The larger χ^2 is, the more the pixel values

TABLE 3. χ^2 test about the pixel histogram.

Test images	Plaintext	Ciphertext
Lena	158875.10	251.25
Barb	144839.50	283.65
Elaine	140650.90	238.16
God-hill	162089.88	248.60
Baboon	259931.55	230.70

deviates from the average level, and the more uneven the pixel distribution is., Table 3 shows χ^2 values of the five images. It can be found that χ^2 value of ciphertext image is far lower than plaintext image and around 250.

4) CORRELATION ANALYSIS

In general, neighboring pixels are similar in the image which contains valid information. The good encryption algorithm should weaken the correlation between adjacent pixels of the image by encryption. For quantitative description, correlation analysis is introduced here.

In Eq. (16), X denotes 2000 pixels randomly selected from the image, and Y denotes 2000 pixels adjacent to X. Y and X have three adjacent ways including horizontal, vertical and diagonal. $R(X, Y)$ represents the correlation coefficient between X and Y. Take Lena, BARB and P-0 as examples. As is shown in Table 4, correlation between adjacent pixels of plaintext image is very high, which is close to 1. After being encrypted, correlation between adjacent pixels of the image is about reduced to thousandth, which is near the ideal value 0.

$$\begin{cases} E(X) = \dfrac{\sum_{i=1}^{n} x_i}{n} \\ D(X) = \dfrac{\sum_{i=1}^{n} (x_i - E(X))^2}{n} \\ \mathrm{cov}(X, Y) = \dfrac{\sum_{i=1}^{n} (x_i - E(X)) \times (y_i - E(Y))}{n} \\ R(X, Y) = \dfrac{\mathrm{cov}(X, Y)}{\sqrt{D(X) \times D(Y)}} \times 100\% \end{cases} \tag{16}$$

5) ANALYSIS OF ANTI-CLIPPING ATTACK

Clipping attack is to intercept a piece of the ciphertext image, and then use the original secret key to decrypt it, and observe the difference between the decrypted image and the original

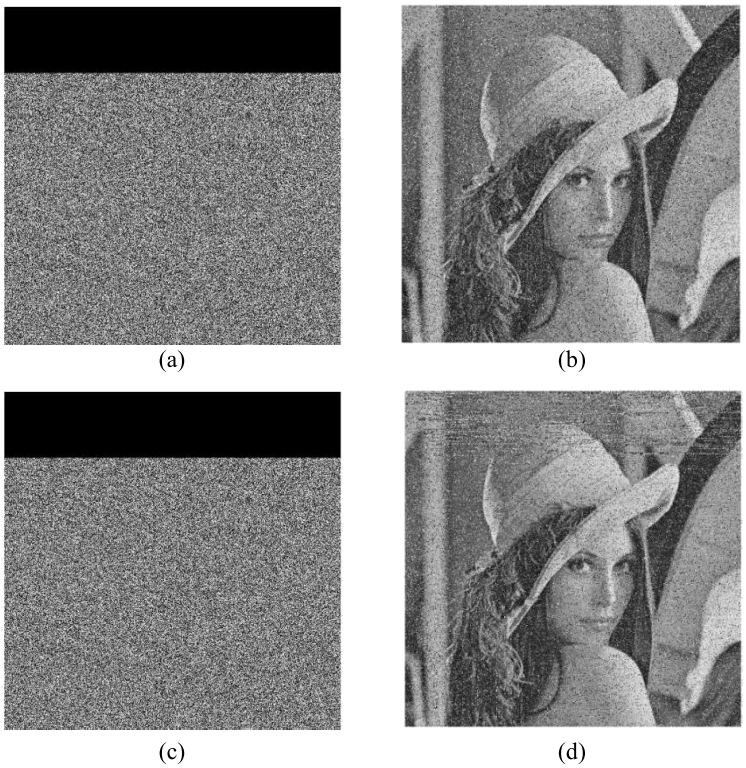


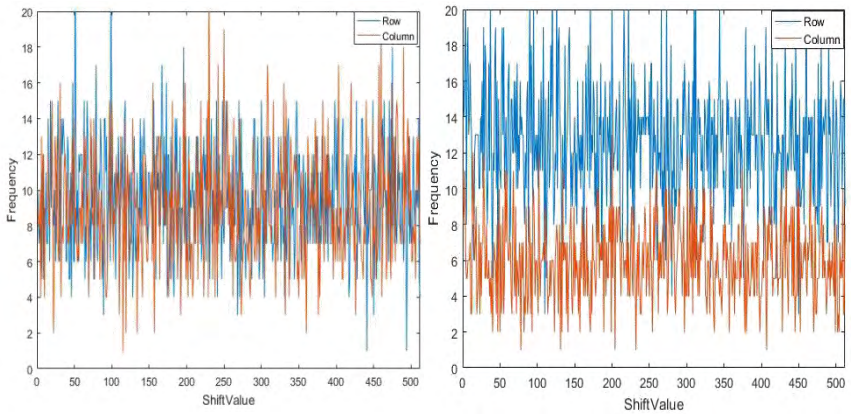
FIGURE 14. Clipping attack analysis. (a) Let $\sum_{j=1}^{512}\sum_{i=1}^{100} C(i,j) = 0$. (b) Decrypted Fig. 14(a). (c) Let $\sum_{j=1}^{512}\sum_{i=1}^{100} C(i,j) = 0$. (d) Decrypted Fig. 14(c).

plaintext image. From the side, it also can reflect that the stronger the ability of anti-clipping attack of the algorithm is, the better the performance of permutation is.

Fig. 12(a) is Lena and Fig. 12(b) is encrypted Lena called C here. Following, we clip the part of C (as is shown in Fig. 14(a)), and then decrypt clipped C to obtain image Pc (as is shown in Fig. 14(b)).

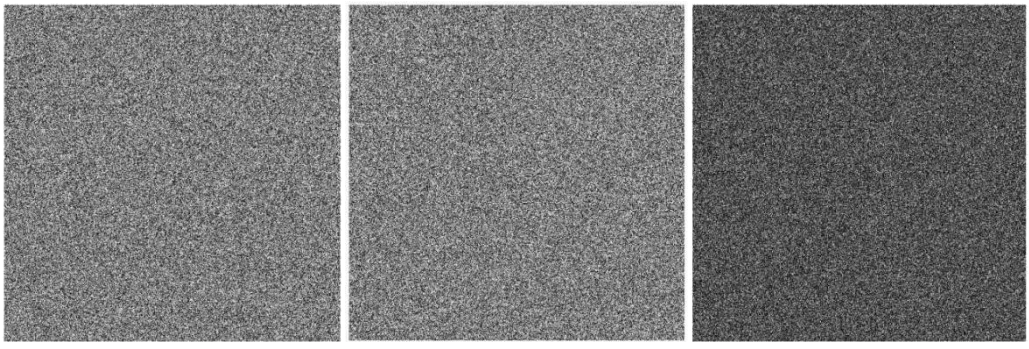
From image Pc, it can be seen that the most information of Lena can be recognized and clipped part are distributed uniformly in the decrypted image, which also illustrates the superiority of the permutation. The key of permutation is homogeneity of distribution of the 0,1 bit in the bit stream sequence Z_i and the uniformity of distribution of permutation value V_i and V_zero_i, which all depend on the LDCML system. In the paper, at $\mu = 3.99 + 0.01 \times b_{10}$, $\mu_2 = 3.99+0.01\times b_{11}$ and $e = 0.01+0.99\times b_{12}$, it can be seen that the chaos of the LDCML system is best and the frequencies of 0-bit or 1-bit appearing in Z_i is very close to 0.5 from Fig. 1(c). In addition, from Fig. 15(a), the frequency of the row shift value V_i and the frequency of the column shift value V_zero_i are also similar to each other, whose curves basically coincide.

For comparison, this paper also select the CML system at $\mu = 3.99 + 0.01 \times b_{10}$, $e = 0.01 + 0.99 \times b_{11}$ as the permutation sequence generator. At the time, the frequency of 1 bit appearing is about twice as large as that of 0 bit in Z_i, and the frequency of row shift value V_i and the frequency of column shift value V_zero_i appearing (as is shown in Fig. 15(b)) are also greatly different that the frequency of row shift values is much higher than that of column shift values. Therefore, ability of anti-clipping attack is poor using the CML. Fig. 14(c) is encrypted Lena after being clipped using CML system and Fig. 14(d) is the decrypted Fig. 14(c). It can be found that a large number of zig-zag stripes appear on the missing blocks in the Fig. 14(d), which proves that the permutation is insufficient. Of course, the chaos of the CML system is greatly enhanced when $e \leq 0.01$ is fetched. However, the overall key space of the CML system has a certain reduction compared with the LDCML system, so the security will be reduced correspondingly.



(a) (b)

FIGURE 15. Permutation sequence distribution analysis. (a) The permutation sequence shift value frequency chart generated by LDCML. (b) The permutation sequence shift value frequency chart generated by CML.



(a) (b) (c)

FIGURE 16. Analysis of image sensitivity. (a) Image *C*. (b) Image *C_one*. (c) Difference image between *C* and *C_one*.

TABLE 4. Correlation of adjacent pixel of image.

State	image	Horizontal	Vertical	Diagonal
Plaintext image	Lena	0.97228467	0.9856127	0.95933095
	BARB	0.85913004	0.9590298	0.84137439
	P-0	1	1	1
	Mean	0.94380490	0.9815475	0.93356844
Proposed encryption	Lena	0.00035115	0.0023313	0.00042744
	BARB	0.00121623	0.0003862	0.00047263
	C-0	0.00049861	0.0061802	0.00361262
	Mean	0.00068865	0.0029555	0.00150422
Ref. [17]	Mean	0.0013174	0.000642	0.001912
Ref. [22]	Mean	0.0026	0.0038	0.0062
Ref. [25]	Mean	0.0058	0.0061	0.0059

6) SENSITIVITY TO SECRET KEY

In the proposed algorithm, initial values of lattices and the coefficients of LDCML system are all generated by the secret key K. Therefore, analyzing the key sensitivity is also an indirect analysis of the sensitivity of the LDCML system to the initial state. Of course, the sensitivity of the key is also related to the design of the algorithm. In the section, the sensitivity to secret key can be described quantitatively by *NPCR* and *UACI* between two images, which is defined in Eqs. (17)-(18).

For the secret key K, the first 360 bits constitute the initial values of 9 lattices of the LDCML system, the [361, 400]th bits are the part of coefficient μ, the [401, 440]th bits are the part of coefficient μ_0, and the last 40 bits are the part of e. Therefore, the analysis of the sensitivity to secret key is divided into four situations. The 80th bit or 400th bit or 440th bit or 480th bit is negated.

Table 5 lists *NPCR* and *UACI* about sensitivity to secret key. From the table, it can be seen that the weak change in the secret key can cause the large change in the ciphertext image. Moreover, *NPCR* or *UACI* between the two ciphertext images is generally greater than 99.6 or 33.4 and meets security standard. Therefore, the algorithm is very sensitive to changes of secret key, and the LDCML system is also very sensitive to change of the initial state.

TABLE 5. Sensitivity to secret key.

Image	Change	*NPCR*	*UACI*
Lena	$K(80) = 1 - K(80)$	99.612	33.412
	$K(400) = 1 - K(400)$	99.601	33.512
	$K(440) = 1 - K(440)$	99.613	33.611
	$K(480) = 1 - K(480)$	99.609	33.421
Barb	$K(80) = 1 - K(80)$	99.621	33.435
	$K(400) = 1 - K(400)$	99.634	33.455
	$K(440) = 1 - K(440)$	99.686	33.543
	$K(480) = 1 - K(480)$	99.613	33.398
Mean	—	99.624	33.473

7) IMAGE SENSITIVITY

Image sensitivity refers to the difference between two ciphertext images obtained by encrypting two images of the same size using the same secret key. The larger the difference, the higher the image sensitivity, the less likely the attacker can use the chosen-plaintext attack or the known-plaintext attack to crack an algorithm, the more secure the algorithm is.

Specifically, take the Lena image as an example, we add 1 to the first pixel of Lena to obtain the image o_Lena, and then encrypt the Lena and o_Lena using the same key to obtain the ciphertext images C and C_one, which is shown in Figs. 16(a)-(b). Then use the *NPCR* and *UACI* to quantitatively describe the difference between C and C_one, where difference image is shown in Fig. 16(c). *NPCR* and *UACI* are defined in Eq. (17) and Eq. (18).

$$UACI = \frac{\sum_{i=1,j=1}^{r,c} \frac{|C_1(i,j) - C_2(i,j))|}{255}}{r \times c} \times 100\%, \tag{17}$$

TABLE 6. *NPCR* and *UACI* about image sensitivity.

State	Lena	BARB	Elaine
Proposed algorithm	99.639, 33.479	99.628, 33.482	99.601, 33.561
Ref. [17]	99.609, 33.447	99.602, 33.461	99.619, 33.422
Ref. [21]	99.764, 33.344	99.764, 33.344	99.764, 33.344
Ref. [27]	99.580, 17.088	99.580, 17.088	99.580, 17.088

TABLE 7. Encryption time analysis (Unit: second).

Image	Size	Proposed	Ref. [22]	Ref. [21]	Ref. [16]	Ref. [17]	Ref. [31]
Gray image	256×256	0.0602	—	—	—	0.8342	1.120
	512×512	0.203	2.25	10.84	0.325	—	4.307
Color image	512×512	0.709	—	16.03	—	—	—

TABLE 8. Comparison of different encryption algorithms.

Algorithm	Information entropy	Adjacent correlation			Image sensitivity		Key sensitivity		Encryption (unit: Sec)
		Horizontal	Vertical	Diagonal	*NPCR*	*UACI*	*NPCR*	*UACI*	
Khan [18]	7.9977	0.0127	0.0065	0.0142	99.556	33.753	99.648	—	7.45
Parvaz [24]	7.9972	0.0036	0.0020	0.0026	99.608	33.509	—	—	1.130
Proposed	7.99927	0.00068	0.0029	0.001504	99.622	33.4806	99.624	33.473	0.203

$$\begin{cases} D(i,j) = \begin{cases} 0, & (C_1(i,j) == C_2(i,j)) \\ 1, & otherwise \end{cases} \\ NPCR = \dfrac{\sum_{i=1,j=1}^{r,c} D(i,j)}{r \times c} \times 100\%, \end{cases} \tag{18}$$

where C_1 and C_2 denote two ciphertext images, m and n denote the length and width of image. When *NPCR* reaches about 99.6 and *UACI* reaches about 33.4, the algorithm meets the security criteria. Table 6 shows the *NPCR* and *UACI* of Lena, BARB, and Elaine. It can be seen that the algorithm completely meets the security standards.

8) SECRET KEY SPACE

The secret key K in the proposed algorithm consists of 480 bits. In the permutation phase, the permutation index and permutation values are generated by the LDCML system, while the initial values and coefficients of the LDCML system are completely dependent on the key K, so key space is 2^{480}. During the diffusion, the bit matrix is generated by the logistic map, and the logistic map completely depends on the initial value y_0. Therefore, under the condition that the decimal precision is 14, the secret key space for diffusion is $10^{14} \approx 2^{45}$. Of course, y_0 is also generated by the LDCML system. Therefore, the algorithm's key space is 2^{480}, which is far greater than the theoretical security key space 2^{100}.

9) COMPUTATIONAL COMPLEXITY

For any image encryption algorithm, in addition to considering the security performance of encryption, computational complexity also needs to be analyzed. Assume that the size of the grayscale image is $r \times c$. In the proposed algorithm, 9 groups of permutation indexes and permutation values sized $2 \times \max(r, c)$ need to be generated from the LDCML system and the time complexity is $O(18 \times \max(r, c))$. Then use these 9 sets of permutation indexes and permutation values to complete one time pixel-level permutation and eight time bit-level permutations, so $O(9 \times r \times c)$ sub-element permutation operations are required. Of course, the bit-level permutation can be run in parallel, so in actual operation, the time-consuming is about $O(2 \times r \times c)$ sub-element replacement. The most time-consuming parts in this phase is 8 time bit-level permutations.

In the diffusion phase, the logistic map needs to be iterated $r \times c$ times to get a bit matrix sized $r \times c$, and then another seven groups of bit matrix are obtained through the adaptive shift algorithm. Finally, the 8 groups of bit matrix and the permuted image are exclusive or to get ciphertext image. The main time-consuming in the phrase lies in the adaptive shift operation, that is because the shift value is calculated 8 times according to the element position and element value of the bit matrix, so its time complexity is $O(8 \times r \times c)$.

Specifically, when the algorithm is running in the Windows 7 operating system, 1.8 GHz CPU frequency, 8G of memory, and Matlab2016a running software, the time-consuming taken for encryption is shown in Table 7. Obviously, the proposed algorithm is far faster than other algorithms.

10) COMPARED WITH OTHER ALGORITHMS

In order to further prove the novelty of this algorithm. We compare the proposed algorithm with Parvaz algorithm [24] and Khan algorithm [18] from the angles of security and encryption time. The Table lists comparison results of the three algorithms given by taking the gray image sized 512×512 as an example. From Table 8, it can be seen that the security effect and encryption time of proposed algorithm are better than those of the other two algorithms. Especially, the running time of the proposed algorithm is much faster than that of the other two algorithms.

V. CONCLUSIONS

Through the above Kolmogorov-Sinai entropy, bifurcation diagram, mutual information, information entropy, space-time behavior of the LDCML system and the corresponding theoretical description, it can be found that LDCML has a larger parameter space than CML has because of introduction of parameter μ_2. LDCML enter into complete chaos earlier because of chaos of $L(e)$. LDCML has better security than CML has because of the lower mutual information and the higher information entropy. In addition, the model structure of LDCML is simpler than that of Space-time chaos system with parameter q proposed by Zhang *et al.* [27]. Then, the paper proposed an image encryption algorithm based on LDCML system. Through analyzing information entropy, local information entropy, anti-clipping attack, image sensitivity, secret key space, sensitivity to secret key, adjacent pixels correlation and computational complexity, the proposed algorithm is proved to be more superior than others.

In the future work, on the one hand, the dynamic coupling theory can be applied to higher dimensional spatiotemporal chaos systems. On the other hand, according to the importance of different parts of the image, image encryption can be performed differently, which makes the key information more secure and save the computational complexity.

REFERENCES

[1] K. Kaneko, "Pattern dynamics in spatiotemporal chaos: Pattern selection, diffusion of defect and pattern competition intermittency," *Phys. D, Nonlinear Phenom.*, vol. 34, pp. 1–41, Jan. 1989.

[2] F. Khellat, A. Ghaderi, and N. Vasegh, "Li–Yorke chaos and synchronous chaos in a globally nonlocal coupled map lattice," *Chaos, Solitons Fractals*, vol. 44, no. 11, pp. 934–939, 2011.

[3] S. Meherzi, S. Marcos, and S. Belghith, "A new spatiotemporal chaotic system with advantageous synchronization and unpredictablitily features," *Proc. Nonlinear Theory Appl.*, pp. 147–150, Sep. 2006.

[4] J. D. Liu and Y.-M. Yu, "A TCML-based spatiotemporal chaotic one-way Hash function with changeable-parameter," *Acta Phys. Sinica*, vol. 56, no. 3, pp. 1297–1304, 2007.

[5] R. Li, F. Huang, and Y. Zhao, "A note on Li–Yorke chaos in a coupled lattice system related with Belusov–Zhabotinskii reaction," *J. Math. Chem.*, vol. 51, no. 8, pp. 2173–2178, 2013.

[6] S. Sinha, "Random coupling of chaotic maps leads to spatiotemporal synchronization," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 66, no. 1, p. 016209, 2002.

[7] S. Rajesh, S. Sinha, and S. Sinha, "Synchronization in coupled cells with activator-inhibitor pathways," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 75, no. 1, p. 011906, 2007.

[8] A. Mondal, S. Sinha, and J. Kurth, "Rapidly switched random links enhance spatiotemporal regularity," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 78, no. 2, p. 066209, 2008.

[9] S. Poria, M. D. Shrimali, and S. Sinha, "Enhancement of spatiotemporal regularity in an optimal window of random coupling," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 78, no. 2, p. 035201, 2008.

[10] Y. Chen, J. Xiao, Y. Wu, L. Li, and Y. Yang, "Optimal windows of rewiring period in randomly coupled chaotic maps," *Phys. Lett. A*, vol. 374, nos. 31–32, pp. 3185–3189, 2010.

[11] Y.-Q. Zhang and X.-Y. Wang, "Spatiotemporal chaos in Arnold coupled logistic map lattice," *Nonlinear Anal. Model. Control*, vol. 18, no. 4, pp. 526–541, 2013.

[12] Y.-Q. Zhang and X.-Y. Wang, "Spatiotemporal chaos in mixed linear–nonlinear coupled logistic map lattice," *Phys. A, Stat. Mech. Appl.*, vol. 402, pp. 104–118, May 2014.

[13] K. Kaneko, "Spatiotemporal chaos in one- and two-dimensional coupled map lattices," *Phys. D, Nonlinear Phenom.*, vol. 37, nos. 1–3, pp. 60–82, 1989.

[14] P. Muruganandam, G. Francisco, M. De Menezes, and F. F. Ferreira, "Low dimensional behavior in three-dimensional coupled map lattices," *Chaos, Solitons Fractals*, vol. 41, no. 2, pp. 997–1004, 2009.

[15] L. Zhang, S. Liu, and C. Yu, "Chaotic behaviour of nonlinear coupled reaction–diffusion system in four-dimensional space," *Pramana*, vol. 82, no. 6, pp. 995–1009, 2014.

[16] Y.-Q. Zhang, X.-Y. Wang, J. Liu, and Z.-L. Chi, "An image encryption scheme based on the MLNCML system using DNA sequences," *Opt. Lasers Eng.*, vol. 82, pp. 95–103, Jul. 2017.

[17] Z. Hua and Y. Zhou, "Image encryption using 2D logistic-adjusted-sine map," *Inf. Sci.*, vol. 339, pp. 237–253, Apr. 2016.

[18] J. S. Khan, M. A. Khan, J. Ahmad, S. O. Hwang, and W. Ahmed, "An improved image encryption scheme based on a non-linear chaotic algorithm and substitution boxes," *Informatica*, vol. 28, no. 4, pp. 629–649, 2017.

[19] I. Hussain, T. Shah, and M. A. Gondal, "Image encryption algorithm based on *PGL(2, GF(2^8))* S-boxes and TD-ERCS chaotic sequence," *Nonlinear Dyn.*, vol. 70, no. 1, pp. 181–187, 2017.

[20] M. Saval-Calvo, J. Azorin-Lopez, A. Fuster-Guillo, J. Garcia-Rodriguez, and S. Orts-Escolano, "Evaluation of sampling method effects in 3D non-rigid registration," *Neural Comput. Appl.*, vol. 28, nos. 1–5, pp. 953–967, 2017.

[21] F. A. Khan, J. Ahmed, J. S. Khan, J. Ahmad, and M. A. Khan, "A novel image encryption based on Lorenz equation, Gingerbreadman chaotic map and S_8 permutation," *J. Intell. Fuzzy Syst.*, vol. 33, no. 6, pp. 3753–3765, 2017.

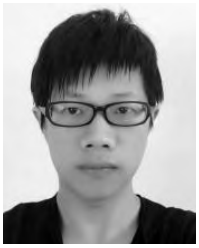
[22] J. Ahmad and S. O. Hwang, "A secure image encryption scheme based on chaotic maps and affine transformation," *Multimedia Tools Appl.*, vol. 75, no. 21, pp. 13951–13976, 2016.

[23] F. A. Khan, J. Ahmed, J. S. Khan, J. Ahmad, M. A. Khan, and S. O. Hwang, "A new technique for designing 8×8 substitution box for image encryption applications," in *Proc. Comput. Sci. Electron. Eng. (CEEC)*, Sep. 2017, pp. 7–12.

[24] R. Parvaz and M. Zarebia, "A combination chaotic system and application in color image encryption," *Opt. Laser Technol.*, vol. 101, pp. 30–41, May 2018.

[25] X. Wang, S. Wang, Y. Zhang, and K. Guo, "A novel image encryption algorithm based on chaotic shuffling method," *Inf. Secur. J., Global Perspective*, vol. 26, no. 1, pp. 7–16, 2017.
[26] Y.-Q. Zhang and X.-Y. Wang, "A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice," *Inf. Sci.*, vol. 273, pp. 329–351, Jul. 2014.
[27] H. Zhang, X.-Y. Wang, S.-W. Wang, K. Guo, and X. H. Lin, "Application of coupled map lattice with parameter q in image encryption," *Opt. Lasers Eng.*, vol. 88, pp. 65–74, Jul. 2017.
[28] R. M. May, "Simple mathematical models with very complicated dynamics," *Nature*, vol. 261, no. 5560, p. 459, 1976.
[29] A. Wolf, J. B. Swift, H. L. Swinney, and J. A. Vastano, "Determining Lyapunov exponents from a time series," *Phys. D, Nonlinear Phenom.*, vol. 16, no. 3, pp. 285–317, 1985.
[30] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J. P. Noonan, and P. Natarajan, "Local Shannon entropy measure with statistical tests for image randomness," *Inf. Sci.*, vol. 222, pp. 323–342, Feb. 2013.
[31] X. Wang, C. Liu, D. Xu, and C. Liu, "Image encryption scheme using chaos and simulated annealing algorithm," *Nonlinear Dyn.*, vol. 84, pp. 1417–1429, May 2016.

WANG XINGYUAN received the Ph.D. degree in computer software and theory from Northeast University, China, in 1999. From 1999 to 2001, he was a Post-Doctoral Researcher at Northeast University. He is currently a Professor with the Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, China. He has published three books and over 400 scientific papers in refereed journals and proceedings. His research interests include nonlinear dynamics and control, image processing, chaos cryptography, systems biology, and complex networks.



FENG LE received the bachelor's degree from the College of Information Engineering, Yangzhou University, China. He is currently pursuing the master's degree in electronic information and electrical engineering with the Dalian University of Technology, China. His main research direction is chaotic encryption and image processing.

WANG SHIBING received the Ph.D. degree in circuits and systems from Anhui University, China, in 2010. He is currently a Post-Doctoral Researcher with the Dalian University of Technology and is also a Professor with the School of Computer and Information Engineering, Fuyang Normal University, China. His research interests include nonlinear circuits and systems, chaos control and synchronization, chaotic signal, and information processing.

CHUAN ZHANG received the B.S. degree in statistics from Qufu Normal University, China, in 2013, and the master's degree in applied mathematics from the Nanjing University of Finance and Economics in 2015. He is currently pursuing the Ph.D. degree with the Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, China. His research interests include nonlinear dynamics, synchronization control, and complex networks.

ZHANG YINGQIAN received the Ph.D. degree in computer application from the Dalian University of Technology, China, in 2014. From 2014 to 2016, he was a Professor with the City Institute, Dalian University of Technology. He is currently a Professor with the Tan Kah Kee College, Xiamen University, China. He has published over 30 scientific papers in journals and proceedings. His research interests include nonlinear dynamics, cryptography, and image processing.