

Two-dimensional-lag complex logistic map with complex parameters and its encryption application

Fangfang Zhang(张芳芳), Jinbo Wu(武金波), Lei Kou(寇磊), Fengying Ma(马凤英), Liming Wu(吴黎明), and Xue Zhang(张雪)

Citation: Chin. Phys. B, 2024, 33 (**5**): 050505. DOI: 10.1088/1674-1056/ad2a69
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

A novel algorithm to analyze the dynamics of digital chaotic maps in finite-precision domain

Chunlei Fan(范春雷) and Qun Ding(丁群)
Chin. Phys. B, 2023, 32 (**1**): 010501. DOI: 10.1088/1674-1056/ac785c

A novel pseudo-random coupled LP spatiotemporal chaos and its application in image encryption

Xingyuan Wang(王兴元), Yu Wang(王宇), Siwei Wang(王思伟), Yingqian Zhang(张盈谦), Xiangjun Wu(武相军)
Chin. Phys. B, 2018, 27 (**11**): 110502. DOI: 10.1088/1674-1056/27/11/110502

A self-cited pixel summation based image encryption algorithm

Guo-Dong Ye(叶国栋), Xiao-Ling Huang(黄小玲), Leo Yu Zhang(张愉), Zheng-Xia Wang(王政霞)
Chin. Phys. B, 2017, 26 (**1**): 010501. DOI: 10.1088/1674-1056/26/1/010501

A fast image encryption algorithm based on only blocks in cipher text

Wang Xing-Yuan (王兴元), Wang Qian (王倩)
Chin. Phys. B, 2014, 23 (**3**): 030503. DOI: 10.1088/1674-1056/23/3/030503

A fast image encryption algorithm based on only blocks in cipher text

Wang Xing-Yuan (王兴元), Wang Qian (王倩)
Chin. Phys. B, 2014, 23 (**3**): 030503. DOI: 10.1088/1674-1056/23/3/030503

Two-dimensional-lag complex logistic map with complex parameters and its encryption application

Fangfang Zhang(张芳芳)[1], Jinbo Wu(武金波)[1], Lei Kou(寇磊)[2], Fengying Ma(马凤英)[1,†], Liming Wu(吴黎明)[1], and Xue Zhang(张雪)[1]

[1] *School of Information and Automation Engineering, Qilu University of Technology (Shandong Academy of Sciences), Jinan* 250353, *China*
[2] *Institute of Oceanographic Instrumentation, Qilu University of Technology (Shandong Academy of Sciences), Qingdao* 266000, *China*

(Received 26 October 2023; revised manuscript received 8 February 2024; accepted manuscript online 19 February 2024)

With the rapid development of internet technology, security protection of information has become more and more prominent, especially information encryption. Considering the great advantages of chaotic encryption, we propose a 2D-lag complex logistic map with complex parameters (2D-LCLMCP) and corresponding encryption schemes. Firstly, we present the model of the 2D-LCLMCP and analyze its chaotic properties and system stability through fixed points, Lyapunov exponent, bifurcation diagram, phase diagram, etc. Secondly, a block cipher algorithm based on the 2D-LCLMCP is proposed, the plaintext data is preprocessed using a pseudorandom sequence generated by the 2D-LCLMCP. Based on the generalized Feistel cipher structure, a round function F is constructed using dynamic S-box and DNA encoding rules as the core of the block cipher algorithm. The generalized Feistel cipher structure consists of two F functions, four XOR operations, and one permutation operation per round. The symmetric dynamic round keys that change with the plaintext are generated by the 2D-LCLMCP. Finally, experimental simulation and performance analysis tests are conducted. The results show that the block cipher algorithm has low complexit, good diffusion and a large key space. When the block length is 64 bits, only six rounds of encryption are required to provide sufficient security and robustness against cryptographic attacks.

Keywords: logistic map, block ciphers, chaotic system, encryption

PACS: 05.45.Pq, 89.20.Hh, 06.30.Ft **DOI:** 10.1088/1674-1056/ad2a69

1. Introduction

Information technology has entered an era of rapid development, people's daily interaction as well as the normal operation of enterprises can not be separated from exchange of information. If these information data are transmitted in public channels, it will bring a lot of security risks. Encryption technology can protect their confidentiality and integrity.[1–4]

It is widely known that chaos have many characteristics well suited to cryptography,[5–7] for instance: (1) For sensitivity to initial values, chaotic systems are highly sensitive when the initial points have a small changes, which can be applied to generation and protection of encryption keys. (2) For pseudo-randomness and non-periodicity, the output of chaotic systems can be seen as a pseudo-random sequence to generate encryption keys, position sequence, integer sequence and initialization vectors, etc.

However, traditional encryption algorithms are limited to encrypt large amounts of data due to constraints in key space and security. Therefore, many researchers have proposed combining chaotic systems with traditional encryption algorithms, Zheng *et al.*[8] proposed an efficient redundant blocks method and also proposed a parallel image encryption algorithm with great security performance and high efficiency. Liu *et al.*[9] designed a uniform non-degenerate chaotic system to solve defects of chaos degradation, weak chaotic behaviors, and proposed a fractal image compression algorithm. Rezaei *et al.*[10] designed a two-dimensional Henon chaotic system and also designed an algorithm based on it.

As for chaotic systems, a complex chaotic system has multiple chaotic attractors and complex dynamic characteristics, which can generate more complicated secret keys, thereby improving the encryption strength and making it more difficult to crack. Many scholars have paid much attention to complex chaotic encryption. Liu *et al.*[11] proposed a complex hyper chaotic Lü system, which injects impulse into control parameters to mitigate the dynamical degradation. Great encryption performance can be obtained by using this system to encrypt color images. Zhang *et al.*[12] proposed a 9-dimensional (9D) complex chaotic system and used its pseudo-random sequence to encrypt power data. Liu *et al.*[13] constructed a novel cryptosystem based on a complex chaotic network system. The above algorithms only encrypt images and do not encrypt text, but the information interaction contains both text data and images, so we need to design an algorithm that can encrypt both text and images.

As for traditional encryption algorithms, the block cryptographic algorithms have strong adaptability,[14] great diffusivity, and arbitrary key length. The block symmetric cipher algorithm mainly disrupts the relationship between plaintexts and keys through substitution-permutation network (SPN) and Feistel cryptographic structures with chaos and diffusion functions.[15] Dhall *et al.*[16] proposed a symmetric image en-

†Corresponding author. E-mail: mafengy@163.com

© 2024 Chinese Physical Society and IOP Publishing Ltd

cryption scheme based on chaos with customizable block size.

The generalized Feistel cryptographic structure is an extension of the Feistel cryptographic structure in the horizontal direction, which improves operational efficiency and increases the number of operational units.[17] Su *et al.*[18] designed a block cipher algorithm using high-performance S-box, chaotic mapping and an improved generalized Feistel structure, etc. Tong *et al.*[19] proposed a combination chaotic mapping to structure S-box with better encryption performance and then designed a lightweight encryption algorithm based on SPN structure.

In 2021, based on a real logistic map, Zhang *et al.*[20] proposed a 2D-lag complex logistic map (2D-LCLM) and designed a color image encryption algorithm. The 2D-LCLM attracts some scholars' great attention.[21–23] However, the algorithm has the following two defects: (1) The position sequence produced by the proposed chaotic system has defects, which makes the algorithm vulnerable to selective plaintext attacks. (2) The mean value of pixels is taken as the initial value, which increases the security risk because the distribution of the mean value satisfies the normal distribution.

Considering the simple structure of 2D-LCLM, based on the advantages of a block cipher and generalized Feistel cipher structure, we propose a 2D-lag complex logistic map with complex parameters (2D-LCLMCP) and a block cipher algorithm text and images. The 2D-LCLMCP can generate the pseudo-random sequences with better randomness. We reconstruct the initial value and create a small perturbation to the initial value by using a hash function to process the information that will be encrypted. The innovation points and main work of this paper are as follows:

(1) We propose the 2D-LCLMCP and analyze its chaotic properties and system stability. The 2D-lag complex logistic map with real parameters has been applied to some extent, but the 2D-lag complex logistic map with complex parameters has rarely been discussed in the literature.

(2) Based on the 2D-LCLMCP and baker map, the S-box which dynamically changes with plaintext is constructed, then the round function F is combined with DNA encoding rules as the nonlinear part of the algorithm. When the number of encryption round is 6, the algorithm can achieve great diffusion and low complexity.

(3) The experimental simulation and performance analysis tests show that our block cipher algorithm has a large key space, good sensitivity and great encryption effect for both text data and images.

The rest of the article is as structured follows: We analyze the chaotic properties and stability of the 2D-LCLMCP in detail in Section 2. In Section 3, we introduce the construction process of the encryption algorithm and describe its process. In Section 4, the experimental simulations are conducted to verify the security performance of the algorithm. Finally, a summary of the article is presented in Section 5.

2. The 2D-LCLMCP

2.1. Mathematical model

The 2D-LCLM model[20] is as follows:

$$\begin{aligned} u_{n+1} &= bu_n(1-g_n),\\ g_{n+1} &= ax_n^2+y_n^2, \end{aligned} \tag{1}$$

where a is a real parameter, and b is a positive real parameter, x_n, y_n and g_n are real state variables, $u_n = x_n + \mathrm{i}y_n$. We can obtain the following expansion form for Eq. (1):

$$\begin{aligned} x_{n+1} &= bx_n(1-g_n),\\ y_{n+1} &= by_n(1-g_n),\\ g_{n+1} &= ax_n^2+y_n^2. \end{aligned} \tag{2}$$

Let $b = c + \mathrm{i}d$, the real and imaginary parts of 2D-LCLM are separated to get the 2D-lag complex logistic map with complex parameters (2D-LCLMCP). It can be expressed by

$$\begin{aligned} x_{n+1} &= (cx_n - dy_n)(1-g_n),\\ y_{n+1} &= (cy_n + dx_n)(1-g_n),\\ g_{n+1} &= ax_n^2+y_n^2, \end{aligned} \tag{3}$$

where a, d, and c are real parameters.

2.2. Fixed point

To solve the fixed points of Eq. (3), we set

$$\begin{aligned} x_{n+1} &= x_n = x,\\ y_{n+1} &= y_n = y,\\ g_{n+1} &= g_n = g. \end{aligned} \tag{4}$$

Substituting Eq. (4) into Eq. (3) yields

$$\begin{aligned} x &= (cx-dy)(1-g),\\ y &= (cy+dx)(1-g),\\ g &= ax^2+y^2. \end{aligned} \tag{5}$$

We get the following fixed point by solving Eq. (5):

(i) When a, c and d take any value, the fixed point is $S_1 = (0,0,0)$.

(ii) When $x \neq 0$, $y \neq 0$, and $d = 0$, the fixed points are $S_{2,3,4,5}$,

$$S_{2,3,4,5} = \left(\pm\sqrt{\frac{c-1}{c(a+1)}}, \pm\sqrt{\frac{c-1}{c(a+1)}}, \frac{c-1}{c} \right). \tag{6}$$

(iii) When $x = 0$, $y \neq 0$, and $d = 0$, the fixed points are $S_{6,7}$,

$$S_{6,7} = \left(0, \pm\sqrt{\frac{c-1}{c}}, \frac{c-1}{c} \right). \tag{7}$$

(iv) When $x \neq 0$, $y = 0$, and $d = 0$, the fixed points are $S_{8,9}$,

$$S_{8,9} = \left(\pm \sqrt{\frac{c-1}{ac}}, 0, \frac{c-1}{c} \right). \tag{8}$$

The Jacobian matrix of system (5) is

$$J = \begin{pmatrix} c(1-g) & -d(1-g) & -cx+dy \\ d(1-g) & c(1-g) & -cy-dx \\ 2ax & 2y & 0 \end{pmatrix}. \tag{9}$$

At the fixed point $S_1 = (0,0,0)$, the characteristic equation can be written in the form of

$$\lambda[(\lambda - c)^2 + d^2] = 0. \tag{10}$$

The general expressions of characteristic roots are $\lambda_1 = 0$ and $\lambda_{2,3} = c + \mathrm{i}d$. $S_1 = (0,0,0)$ is an unstable fixed point when $|\lambda_{2,3}| = c^2 + d^2 > 1$.

Under the conditions of other remaining fixed points S_i $(i = 2,3,\ldots,8,9)$, the characteristic equation can be given by

$$(\lambda - 1)(\lambda^2 - \lambda + 2c - 2) = 0. \tag{11}$$

The characteristic roots are

$$\lambda_1 = 1, \quad \lambda_{2,3} = \frac{1 \pm \sqrt{9 - 8c}}{2}. \tag{12}$$

Detailed results are listed in Table 1. When the modulus of the eigenvalues of the Jacobian matrix at fixed points is less than 1, the chaotic systems at fixed points are stable; otherwise, they are unstable.

Table 1. The stability of the fixed point.

Fixed points	Range	Characteristic roots	Stability
$S_1 = (0,0,0)$	$c^2 + d^2 > 1$	$\lambda_1 = 0, \lambda_{2,3} = c + \mathrm{i}d$	unstable
	$c^2 + d^2 < 1$	$\lambda_1 = 0, \lambda_{2,3} = c + \mathrm{i}d$	stable
$S_{2,3,4,5} = \left(\pm\sqrt{\frac{c-1}{a+1}}, \pm\sqrt{\frac{c-1}{a+1}}, \frac{c-1}{c} \right)$	$c = \frac{9}{8}, a > -1$	$\lambda_1 = 1, \lambda_{2,3} = \frac{1}{2}$	stable
	$c > \frac{9}{8}, a > -1$	$\lambda_1 = 1, \lambda_{2,3} = \frac{1 \pm \mathrm{i}\sqrt{9-8c}}{2}$	Hopf bifurcation
	$c < 0, a < -1$	$\lambda_1 = 1, \lambda_{2,3} = \frac{1 \pm \sqrt{9-8c}}{2}$	unstable saddle points
$S_{6,7} = \left(0, \pm\sqrt{\frac{c-1}{c}}, \frac{c-1}{c} \right)$	$c = \frac{9}{8}$	$\lambda_1 = 1, \lambda_{2,3} = \frac{1}{2}$	stable
	$c < 0$	$\lambda_1 = 1, \lambda_{2,3} = \frac{1 \pm \sqrt{9-8c}}{2}$	unstable saddle points
	$c = \frac{7}{4}$	$\lvert\lambda_{2,3}\rvert = 1$	Hopf bifurcation
$S_{8,9} = \left(\pm\sqrt{\frac{c-1}{ac}}, 0, \frac{c-1}{c} \right)$	$c = \frac{9}{8}, a > 0$	$\lambda_1 = 1, \lambda_{2,3} = \frac{1}{2}$	stable
	$c < 0, a < 0$	$\lambda_1 = 1, \lambda_{2,3} = \frac{1 \pm \sqrt{9-8c}}{2}$	unstable saddle points
	$c = \frac{7}{4}$	$\lvert\lambda_{2,3}\rvert = 1$	Hopf bifurcation

2.3. Lyapunov exponent

According to the general expression of the characteristic root, the chaotic properties of the 2D-LCLMCP depend mainly on the parameters c and d. Set $a = 1$, the initial value of the 2D-LCLMCP is (0.2, 0.4, 0.1). We make the Lyapunov exponent (LE) diagram changing with c when d takes different positive values, as shown in Fig. 1.

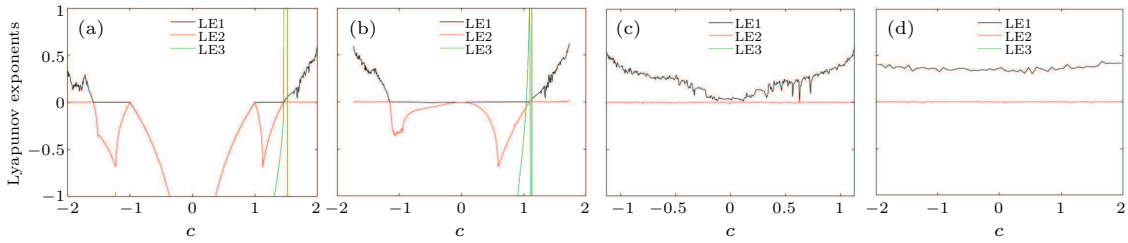


Fig. 1. Lyapunov exponent diagram of the 2D-LCLMCP: (a) $d = 0$, (b) $d = 1.0$, (c) $d = 1.65$, (d) $d = 1.99$.

When $0 < |d| < 1.65$, the value range of the parameter c corresponding to the Lyapunov index greater than 0 gradually becomes larger as $|d|$ increases, and at this time, the interval range of the parameter c is discontinuously distributed on the positive and negative axes of the x-axis [Figs. 1(a) and 1(b)]. When $|d| = 1.65$, the value range of the parameter c begins to form a continuous area, and the 2D-LCLMCP is intermittently chaotic. When $1.65 \leq |d| < 2$, the value range of c corresponding to the positive Lyapunov index is always continuous but shrinks with $|d|$ increases. Until $|d| = 2$, the chaotic border crisis happens, and the Lyapunov index disappears.

2.4. Bifurcation diagram

For system (2), we choose $a = 1$, $0 \leq |d| < 2$, (0.2, 0.4, 0.1) as the initial values, and get the bifurcation diagrams on c–x–g plane as d changes, as shown in Fig. 2.

From Figs. 2 and 3, when the value of parameter d fluctuates around 0, the shapes of this diagram like two symmetrical

"sand piles" with no intersection. The two sand piles begin to intersect and merge into a "dumbbell" as d increases, the curvature of the upper and lower curves in the dumbbell-shaped figure gradually flattens until it becomes a straight line. When $d = 1.99$, which is the critical maximum of the 2D-LCLMCP, the 3D bifurcation diagram ends up as a cylinder. Figures 4 and 5 are both 2D figures, and their evolution laws are consistent with Figs. 2 and 3. There also exists some obvious period-window phenomenon in Fig. 5, around which the system is intermittently chaotic.

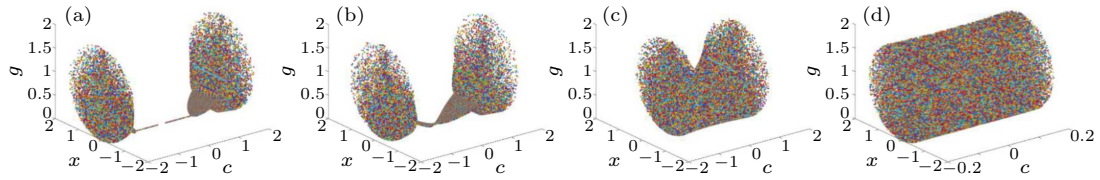


Fig. 2. Bifurcation diagrams on c–x–g plane: (a) $d = 0$, (b) $d = 1.0$, (c) $d = 1.65$, (d) $d = 1.99$.

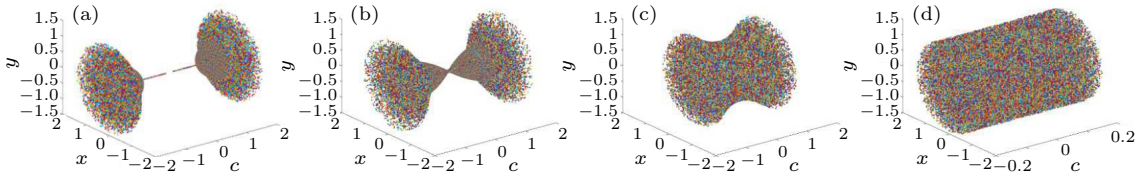


Fig. 3. Bifurcation diagrams on c–x–y plane: (a) $d = 0$, (b) $d = 1.0$, (c) $d = 1.65$, (d) $d = 1.99$.

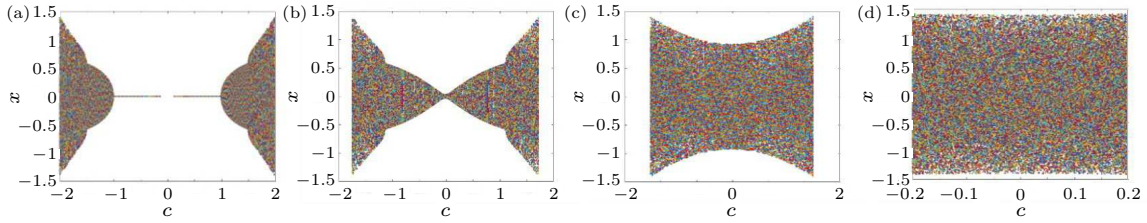


Fig. 4. Bifurcation diagrams on c–x plane: (a) $d = 0$, (b) $d = 1.0$, (c) $d = 1.65$, (d) $d = 1.99$.

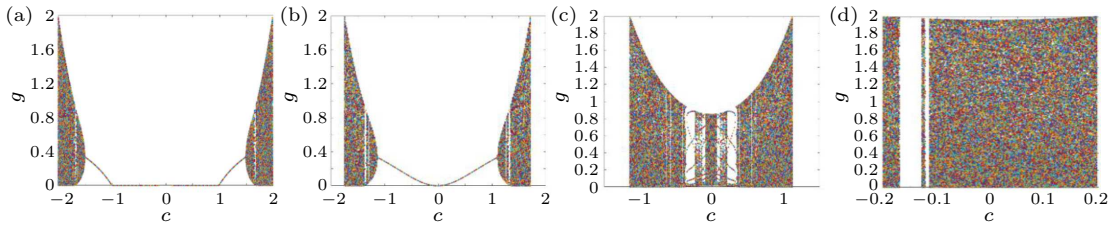


Fig. 5. Bifurcation diagrams on c–g plane: (a) $d = 0$, (b) $d = 1.0$, (c) $d = 1.65$, (d) $d = 1.99$.

2.5. Phase diagram

The parameters c and d both have wide range of values. We depict several typical chaotic attractor graphs in Fig. 6 with $d = 1.69$.

Figure 6(a) depicts the critical case that the 2D-LCLMCP goes from period-doubling bifurcation to chaos, and those figures are composed of fixed points. In Figs. 6(b)–6(d), the chaotic attractors in x–y plane are elliptical and contain many disordered particles; attractors in x–g plane shape like two symmetric ellipses whose vertices are coincident. Meanwhile, with the increase of parameter c, the symmetric ellipses tend to coincide along the symmetry axis and eventually evolve into one ellipse with numerous particles scattered inside. The 3D figure of attractors on the x–y–g plane changes from ellipsoid to spheroid with the increase of c. Generally speaking, the shapes of the attractors are roughly the same when the parameter c takes different values, with only horizontal or vertical scaling between the graphs.

We also study the case of $c = 0$ in the 2D-LCLMCP. The changing process of phase diagrams are shown in Fig. 7.

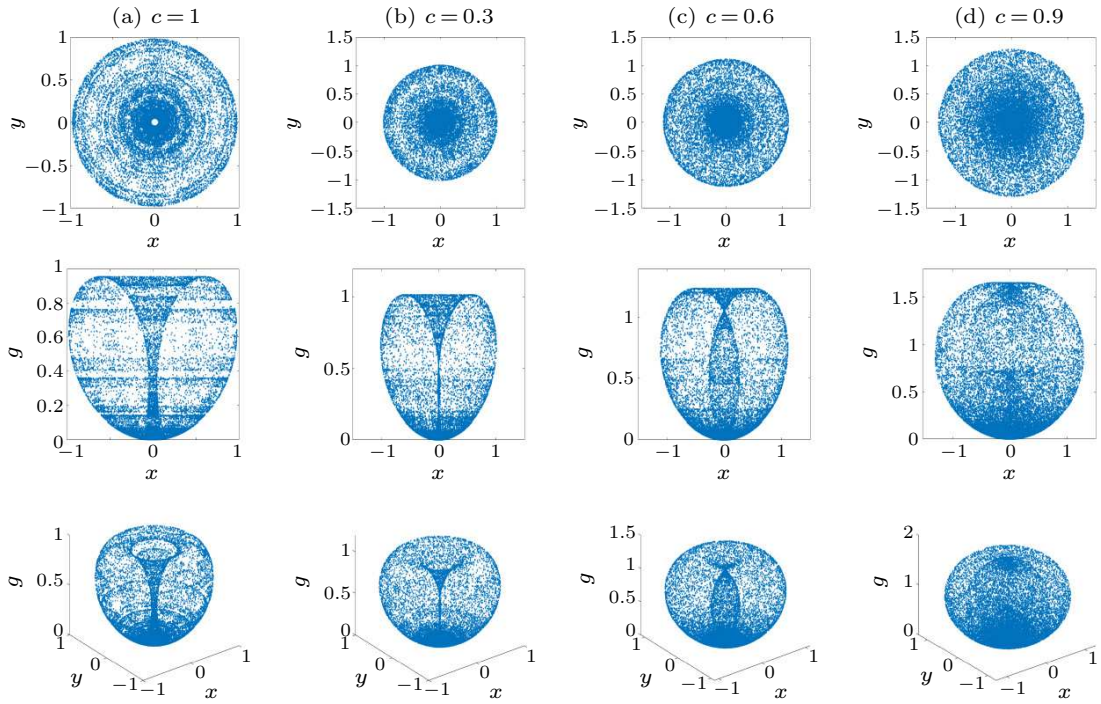


Fig. 6. Chaotic attractor graphs of the 2D-LCLMCP at $a=1$, $d=1.69$: (a) $c=0.1$, (b) $c=0.3$, (c) $c=0.6$, (d) $c=0.9$.

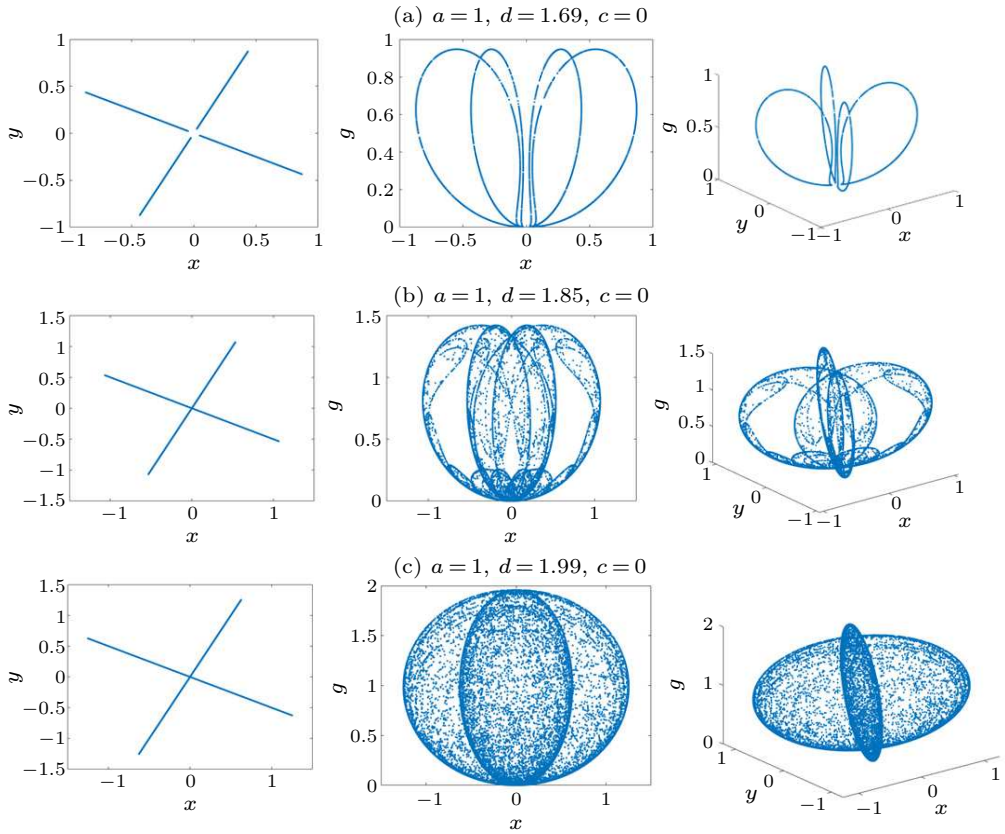


Fig. 7. Phase diagram of the 2D-LCLMCP when $c=0$.

At the beginning, the phase diagram is composed of four disjoint ellipses with an angle about 90°. With the increasing d, the mother ellipses begin to converge and intersect, with many new small ellipses and particles appearing and diffusing inside. Until $d=1.999$, the phase diagram eventually evolves into two tangent ellipses.

When system moving from a fixed point to chaos, chaos phenomenon and periodic window phenomenon appear alternately, that is, the system is intermittently chaotic. The value of the right limit of $|c|$ decreases gradually with the increase

of $|d|$. When $|d| \approx 1.5$, the positive and negative semi-axis chaotic intervals are connected, the system has better chaotic performance for encrypting parameters.

Table 2. Initial value of the 2D-LCLMCP.

Initial conditions	G1	G2	G3	G4
a	1	1.0001	1.0002	1.0003
b	1.2	1.20001	1.20002	1.20003
c	1.5	1.500001	1.50002	1.50003
x_1	0.2	0.20001	0.20002	0.20003
y_1	0.4	0.40001	0.40002	0.40003
g_1	0.1	0.10001	0.10002	0.10003

3. Performance test of the 2D-LCLMCP

The 2D-LCLMCP iterates with different initial values (Table 2), we get 10000 initial values from the 2D-LCLMCP for frequency test, balance analysis, initial value sensitivity and other performance tests, the knot details are shown in Table 3, i.e., x_1, y_1 and g_1 as initial values of the chaotic system.

3.1. Frequency test for the 2D-LCLMCP

The frequency test can verify that the number of 0 and 1 is approximately equal. The formula is as follows:

$$x_1^2 = \frac{(p-q)^2}{m^2}, \tag{13}$$

where x_1^2 is chi-square distribution, p and q are the numbers of 1 and 0 in the binary sequence, respectively; m is the length of the binary sequence. The binary sequence has a better randomness as long as the value of x_1^2 is not greater than 3.84. As the value of x_1^2 is much smaller than 3.84 in Table 3, the sequences generated by the 2D-LCLMCP can successfully pass the frequency test and has good randomness.

Table 3. Performance Indicator of the 2D-LCLMCP.

Performance parameters	G1	G2	G3	G4
Frequency test	6.4366×10^{-4}	1.1938×10^{-4}	7.9012×10^{-5}	1.3717×10^{-4}
Balance analysis	0.0254	0.0109	0.0089	0.0037
Initial value sensitivity	49.47%	48.65%	49.77%	49.34%

3.2. Balance analysis

The balance e is defined as

$$e = \frac{|p-q|}{m}. \tag{14}$$

The smaller the value of e is, the closer the numbers of 1 and 0 in the sequence is, and the better the randomness is. It can be seen that e is close to 0, so it has better randomness.

3.3. Initial value sensitivity

We make small changes to the initial values and calculate the bit change rate of the sequence by counting the changes in the values of 1 and 0 at the corresponding positions in the sequence. The bit change rate R is defined as

$$R = \frac{m_1}{m}, \tag{15}$$

where m_1 is the number of bits that changes the corresponding position value after a small change under the initial condition, the closer the R is to 50%, the more sensitive the system is to the initial conditions. When the initial conditions are slightly changed. From Table 3, R is close to 50%, which satisfies the requirements of encryption.

4. Block cipher algorithm

The block cipher algorithm adopts the generalized Feistel cipher structure, which divides each plaintext block into four operation units for round operations. Each round includes two F functions.

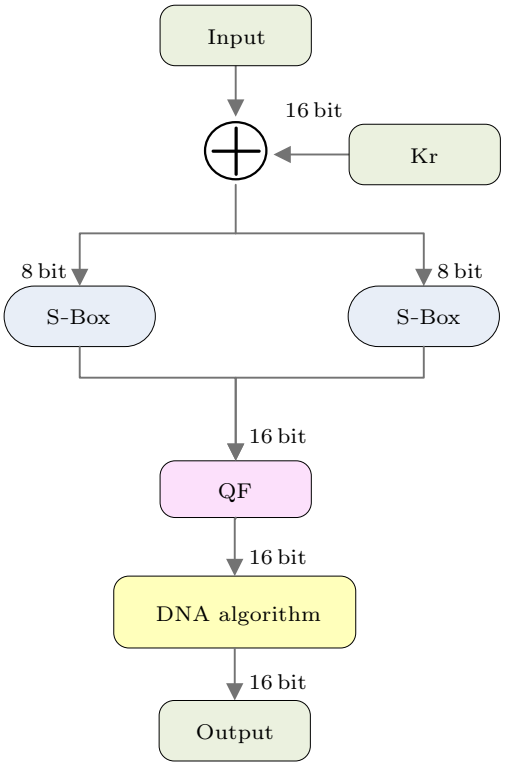


Fig. 8. Structural diagram of F.

4.1. Construction of the round function F

The round function F is nonlinear and plays a major role in confusion and diffusion. We propose that F is composed of a dynamic S-box and DNA encoding rules,[24] as shown in

Fig. 8. Its pseudocode can be represented as

$$\begin{aligned} F(k,l) &= \text{DNA_algorithm}(\text{QF}(f_1,f_2)),\\ f_1 &= \text{S_box}(\{k\oplus l\}(1:8)),\\ f_2 &= \text{S_box}(\{k\oplus l\}(9:16)), \end{aligned} \tag{16}$$

where l denotes the 16-bit sequence, k represents the 16-bit round key, DNA_algorithm$(\cdot)$ represents the DNA encoding rule, S_box$(\cdot)$ represents the dynamic S-box, $\oplus$ represents the per-bit dissimilarity operation, QF is a nonlinear equation.

4.2. Dynamic S-box

The dynamic S-box is composed of the 2D-LCLMCP and Baker map. Firstly, a pseudo-random sequence is generated by iterating the 2D-LCLMCP. Then, the sequence is subject to modulo and rounding operations, ensuring that the real number sequence falls into 256 different intervals between 0 and 255 without repetition, forming the S_1-Box. Finally, the S_1-Box is scrambled using a position sequence generated by a chaotic sequence and the Baker map to obtain the final dynamic S-box, as shown in Fig. 9.

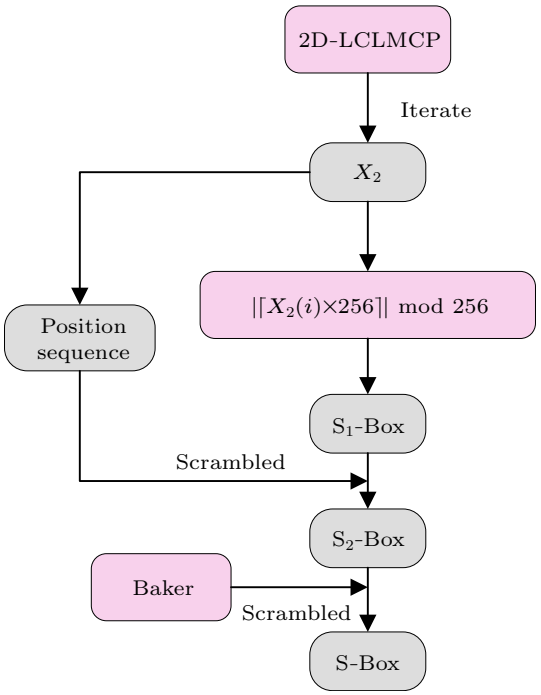


Fig. 9. Structural diagram of S-box.

4.3. Generation of round keys

The dynamic round keys are generated using the 2D-LCLMCP and DNA encoding rules. The 2D-LCLMCP is highly sensitive to small perturbations in the plaintext, which means that the keystream changes with the variation of the plaintext. The pseudocode for the round keys k is as follows:

$$k = \text{DNA_algorithm}(T(\text{hex2bin}(\text{Key},4))), \tag{17}$$

where Key is the seed key in hexadecimal, and $T(\cdot)$ indicates the position scrambling operation.

4.4. Encryption algorithms

In this block cipher algorithm, plaintext is divided into groups of 64 bits each. The flowchart is shown in Fig. 10 and the encryption algorithm proceeds as follows:

Step 1 Read the plaintext, use the original image as the input of Sha-256, get the 256-bit hash value $m_1, m_2, m_3, \ldots, m_{32}$.

Step 2 Let the original initial value of the 2D-LCLMCP be (x_1, y_1, g_1), use the Sha-256 to generate a small perturbation to (x_1, y_1, g_1), and obtain the initial value:

$$\begin{aligned} x_1' &= x_1 + \text{mod}\left(\frac{m_1\oplus\cdots\oplus m_8+\text{mean}}{256},1\right),\\ y_1' &= y_1 + \text{mod}\left(\frac{m_9\oplus\cdots\oplus m_{16}+\text{mean}}{256},1\right),\\ g_1' &= g_1 + \text{mod}\left(\frac{m_{17}\oplus\cdots\oplus m_{24}+\text{mean}}{256},1\right),\\ \text{mean} &= \sum_{i=1}^{32}\frac{m_i}{32}. \end{aligned} \tag{18}$$

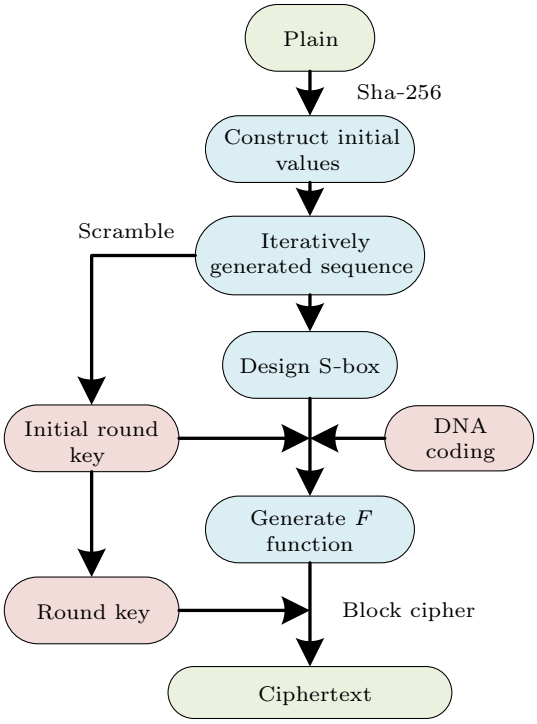


Fig. 10. Encryption algorithm flowchart.

Iterate the chaotic system to obtain the pseudo-random sequence X_1, X_2, X_3, perform modulo and integer operations on the sequence X_1, X_3 to obtain the sequence of integers w and z:

$$\begin{aligned} w &= \text{floor}(((X_1\times 10^3 - \text{floor}(X_1\times 10^3))\times 10^3)) \bmod 256,\\ z &= \text{floor}(((X_3\times 10^3 - \text{floor}(X_3\times 10^3))\times 10^3)) \bmod 256. \end{aligned} \tag{19}$$

Step 3 Extract three segments of data from sequence X_2 and sort them in ascending order to obtain position sequence T_1, T_2, T_3. The position sequence T_4 is obtained by intercepting three segments of the sequence X_1 and arranging them in

the order, where the T_1 is used to disrupt the S_1-box. The DNA encoding rules, T_2 and the initial round key are used to generate the round key.

Step 4 Compress the data information value *plain* into the range of [0,255] by taking modulo and XOR operations to obtain P_1:

$$P_1 = ((plain + w) \bmod 256) \oplus z. \tag{20}$$

Step 5 First, use T_3 to scramble the position of data in P_1, $P_2 = P_3T(P_1)$; then use T_4 to scramble the position of data in P_1, $P_3 = P_4T(P_2)$; finally, convert all integers in P_3 to 8-bit binary numbers P_4, and divide them into groups of 64 bits, denoted as Plain_block(i).

Step 6 Perform round operations on data according to the generalized Feistel cipher structure. Its pseudo-code is shown in Algorithm 1.

Step 7 Finally, all binary sequences are converted into integers every 8 bits, and the final ciphertext is translated according to the ASCII code table.

Algorithm 1 Generalized Feistel cipher algorithm

Initialize:
Round key k; encrypted data per group $Plain_block(i)$;
Initialize vectors IV (64bit); number of rounds $round$;
Round function F;
for $i = 1:1:length(Plain_block(i))$

$$Block_i \leftarrow IV_i \oplus Plain_block(i)$$
$$L_{0,1}, L_{0,2}, R_{0,1}, R_{0,2} \leftarrow permutation(Block_i)$$

for $j = 1:1:round$

$$L_{j,1} = R_{j-1,2}$$
$$L_{j,2} = L_{j-1,1} \oplus F(k_{j,1}, L_{j-1,2})$$
$$R_{j,1} = L_{j-1,2}$$
$$R_{j,2} = R_{j-1,1} \oplus F(k_{j,2}, R_{j-1,2})$$

end for

$$L_{j,1} = R_{j-1,2}$$
$$L_{j,2} = L_{j-1,1} \oplus F(k_{j,1}, L_{j-1,2})$$
$$R_{j,1} = L_{j-1,2}$$
$$R_{j,2} = R_{j-1,1} \oplus F(k_{j,2}, R_{j-1,2})$$
$$Ciphered_block(i) \leftarrow permutation(L_{j+1,1}L_{j+1,2}R_{j+1,1}R_{j+1,2})$$
$$IV_{i+1} \leftarrow Ciphered_block(i)$$

end for
Output: Ciphertext $Ciphered_block(i)$

4.5. Decryption algorithm

The decryption algorithm is the inverse operation of the encryption algorithm, but it must satisfy the following three conditions:

(1) The number of rounds can only be an even number.

(2) The left and right round keys in odd rounds are exactly the same: $k_{j,1} = k_{j,2}$.

(3) The permutation rule for the last round is as follows: $L_{j+1,1} = R_{j,2}$, $L_{j+1,2} = L_{j,1}$, $R_{j+1,1} = L_{j,2}$, $R_{j+1,2} = R_{j,1}$.

Here, $R_{j,2}$, $L_{j,1}$, $L_{j,2}$, $R_{j,1}$ are the result of each round of block encryption operations, and $L_{j+1,1}$, $L_{j+1,2}$, $R_{j+1,1}$, $R_{j+1,2}$ are the final output of each round.

5. Experimental simulation and performance analysis

5.1. Experimental simulation

The power data from the receiver and transmitter, standardized test image, and images of power failure equipment are used as inputs for the algorithm to conduct simulation experiments on the MATLAB platform of the Windows 10 system, the host system utilizes an Intel(R) Core(TM) i5-7200U CPU @ 2.50 GHz 2.70 GHz. The number of rounds is 6, the initial value of the 2D-LCLMCP is (1, 1.2, 1.5, 0.2, 0.4, 0.1) and the initial key in hexadecimal is set to key = a4360d25e71dcbf807483c1bb957f0e4533ca6. The encrypted results and original data of power text data are shown in Fig. 11, and the encryption and decryption results of power images are shown in Fig. 12.

Figure 11(a) is the original text, and Fig. 11(b) is the ciphertext. When the secret key is incorrect, the decrypted text is different from the original text, which is shown in Fig. 11(c). When the secret key is correct, we can recover the original text exhibited in Fig. 11(d). There are the original images of example 1, example 2 and example 3 in Fig. 12(a), and the encrypted images of the three examples in Fig. 12(b), and the decryption diagrams of the three examples in Fig. 12(c).

5.2. Key sensitivity analysis

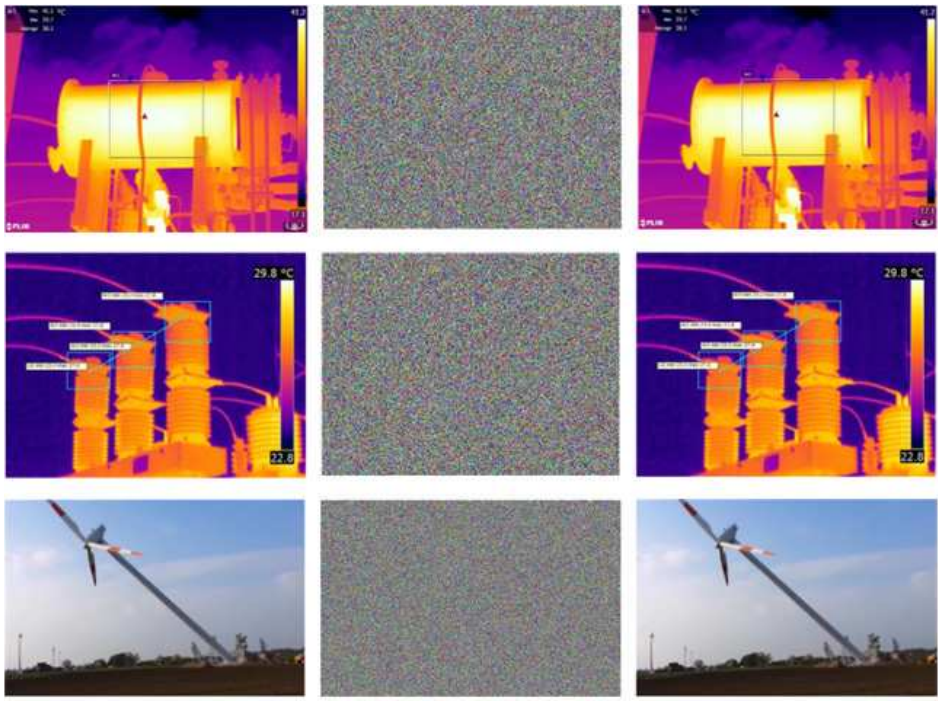
The key consists of two main parts: one is the initial value of the 2D-LCLMCP (x_1', y_1', g_1') and parameters a and b; the other is the round key k. Assume that the computer memory accuracy is 10^{15}, the key space is at least $10^{15\times5} = 10^{70} > 2^{100}$, in addition to parameter $b \in [1.69, 2)$ has a lot of room for change, and the chaotic system and the key sequence transform adaptively with the plaintext.



(a) Power text data (b) Ciphertext

(c) Error decryption text (d) Decrypt the text correctly

Fig. 11. Results of encryption and decryption of power text data.



(a) Original image (b) Encrypted images (c) Decrypted images

Fig. 12. Power image encryption and decryption results (examples 1, 2 and 3 are presented).

5.3. Frequency test for algorithm

Frequency test is mainly used to detect the frequency of each ASCII code value, Fig. 13 is its result. Before encryption, the ASCII values of plaintext are clustered around some characters, with obvious regularity; after encryption, the distribution frequency of the ASCII code value of the ciphertext fluctuates around the ideal value 3.90625×10^{-3}, therefore, the algorithm has a strong robustness against statistical attacks.

5.4. Information entropy test

Information entropy reflects the uncertainty of image information, its ideal value is 8. For the image, the frequency of 256 gray values from 0–255 is tested, and the results are listed in Table 4. The frequency of 256 ASCII codes in ciphertext is tested, and the results are listed in Table 5, with the growth of test data, the maximum image information entropy can reach 7.9993, and the maximum text information entropy can reach 7.98, which are mostly better than the simulation test results in

the comparison algorithms.[24,25] Therefore, the block cipher algorithm proposed has better randomness and scrambling effect.

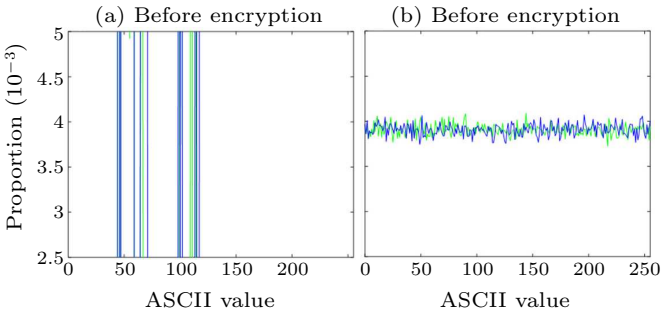


Fig. 13. Frequency test diagram. The horizontal coordinate is the ASCII value of each character, the vertical coordinate is the proportion of the ASCII value in the ciphertext.

Table 4. Test results of image information entropy.

Image	Before encryption	After encryption
Lena_R	7.2531	7.9993
Lena_G	7.5940	7.9993
Lena_B	6.9784	7.9993
Case2_R	7.1671	7.9983
Case2_G	6.5545	7.9986
Case2_B	7.6085	7.9984
Case3_R	6.4398	7.9982
Case3_G	5.8086	7.9986
Case3_B	6.7483	7.9984
Case4_R	7.4042	7.9992
Case4_G	7.0371	7.9993
Case4_B	6.9031	7.9993
Singh *et al.*[24]		7.9971
Wu *et al.*[25]		7.9992

Table 5. Test results of text information entropy.

length/byte	Algorithm in this paper (receiving)	Algorithm in this paper (sending)	RC5	RC6	AES
5000	7.96261	7.98181	7.99792	7.99984	7.96261
10000	7.96379	7.98194	7.99760	7.99982	7.96379
100000	7.95834	7.98035	7.99794	7.99981	7.95834
1000000	7.96545	7.98238	7.99812	7.99983	7.96545

Table 6. Correlation between adjacent pixel points.

Image	Before encryption			After encryption		
	H	V	D	H	V	D
LenaR	0.9790	0.9880	0.9660	0.0130	−0.0046	0.0146
LenaG	0.9299	0.9561	0.9138	−0.0067	0.0058	−0.0043
LenaB	0.9671	0.9816	0.9524	0.0187	0.0151	0.0070
Case4-R	0.9947	0.9947	0.9870	0.0024	−0.0018	0.0059
Case4-G	0.9967	0.9903	0.9865	0.0019	−0.0032	0.0007
Case4-B	0.9867	0.9971	0.9876	−0.0005	0.0014	0.0007
Singh *et al.*[24]	0.9715	0.9654	0.9723	0.0023	−0.0051	0.0071
Wu *et al.*[25]	0.8922	0.7470	0.7598	0.0021	0.0029	0.0016

5.5. Correlation test

Correlation test can quantitatively analyze the degree of correlation between adjacent pixels. Select 8000 pairs of pixel points at random of 'Lena', make a pixel distribution map.

The closer the value of the correlation test is to 1, the stronger the correlation between adjacent pixels of the image is. The closer the correlation test to 0, the more irrelevant the gray value of adjacent pixel points.

The correlation test results between pixel points are recorded in Table 6. According to the analysis of the data in the table, the distribution of gray values of adjacent pixel points before encryption is obviously linear, while the distribution of gray values of encrypted pixel points is uniform and scattered across the whole plane. The calculation results are mostly better than the test results in Refs. [24,25].

5.6. Histogram analysis

Figure 14 shows the histograms of the 'Lena'. The distribution of pixels before encryption has obvious regularity, while the distribution of pixels after encryption is uniform. The information features of the image are hidden, indicating that this block cipher algorithm has good confidentiality.

5.7. Differential attack test

Differential attack testing, also known as plaintext sensitivity testing, can quantitatively analyze the differences between the output ciphertexts before and after the pixel values undergo small changes. The number of pixels change rate (NPCR) and the unified average changing intensity (UACI) are used to measure this indicator.

The closer the test result to the expected value, the more sensitive the algorithm to the disturbance. From Table 7, the test images have good test values and are mostly better than the test results in Refs. [24,25].

5.8. Cut attack and noise attack test

Cut out 64×64, 80×80 and 128×128 pixel points in Example 1 to perform the cut attack test, and then add Poisson noise with density of 0.01, Gaussian noise with mean value of 0 and variance of 0.01, salt and pepper noise with density of 0.01 to Example 3 to perform the noise attack test. From Fig. 15, although the sharpness of the image is reduced by clipping and noise attacks, the characteristics and basic colors of the image are still recognizable.

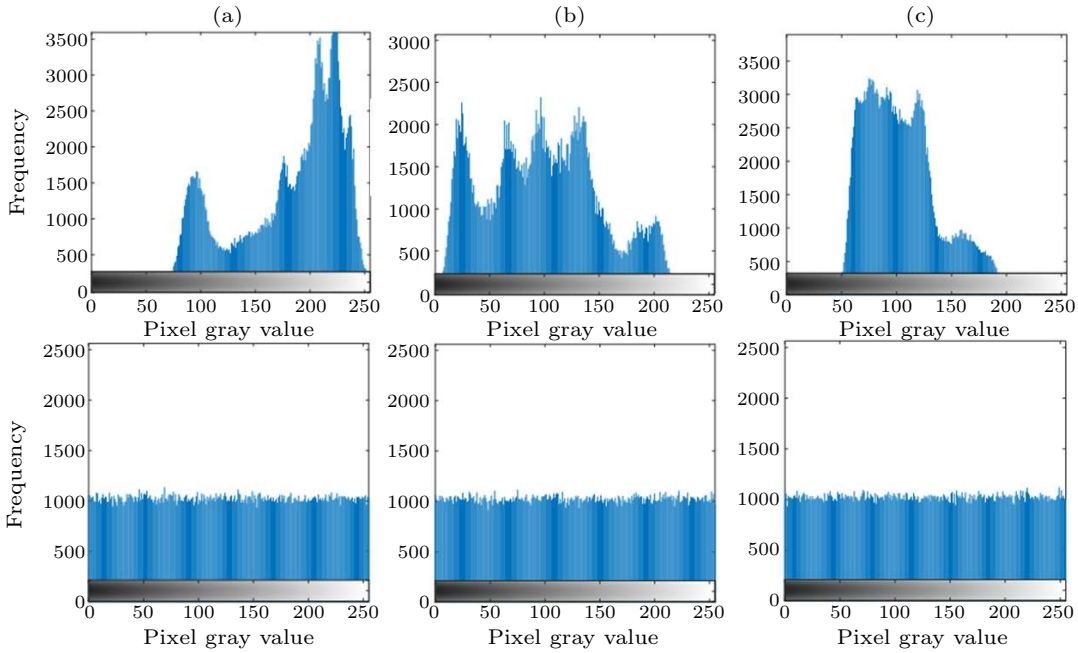
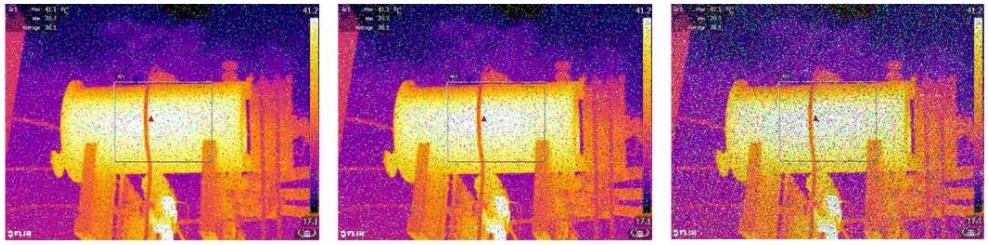


Fig. 14. Histograms of Lena before and after encryption (the horizontal coordinate is the pixel gray value, and the vertical coordinate is the frequency of each gray value): (a) before and after R channel encryption, (b) before and after G channel encryption, (c) before and after B channel encryption.

Table 7. NPCR and UACI values of images.

Image	NPCR (%)			UACI (%)		
	R	G	B	R	G	B
Lena	99.10	99.38	99.39	33.36	33.47	33.54
Case2	99.66	99.61	99.61	33.43	33.52	33.46
Case3	99.59	99.60	99.59	33.55	33.46	33.47
Case4	99.60	99.61	99.60	33.45	33.47	33.46
Singh *et al.*[24]	33.44	–	–	33.46	–	–
Wu *et al.*[25]	99.68	–	–	33.44	–	–



(a) 64×64 Decryption diagram (b) 80×80 Decryption diagram (c) 128×128 Decryption diagram



(d) SN 0.01 (e) SPN 0.01 (f) GN(0, 0.01)

Fig. 15. Cutting attack and noise attack test.

6. Conclusion

Aiming at protect information security issues in the public channel, we design a block cipher algorithm base on the 2D-LCLMCP. The chaotic properties are analyzed by using the fixed point, Lyapunov exponent, bifurcation diagram, phase Diagram, etc. The algorithm mainly adopts the generalized Feistel cipher structure, in which the function F is composed of dynamic S-box and DNA coding rules. The round function F and the position sequence generated by the 2D-LCLMCP provide the scrambling effect for the algorithm. With P scrambling, the transposition operation contained in each round and the integer sequence generated by the 2D-LCLMCP play a replacement role in the algorithm. The research results show that when the block length of the encryption algorithm is 64 bit, only 6 rounds can make the power text and image achieve better encryption effect. The algorithm had great robustness and high security against data analysis tests, sensitivity tests and cryptographic attack tests.

Acknowledgments

Project supported by the Shandong Province Natural Science Foundation (Grant Nos. ZR2023MF089, R2023QF036, and ZR2021MF073), the Industry-University-Research Collaborative Innovation Fund Project of Qilu University of Technology (Shandong Academy of Sciences) (Grant Nos. 2021CXY-13 and 2021CXY-14), the Major Scientific and Technological Innovation Projects of Shandong Province (Grant No. 2020CXGC010901), the Talent Research Project of Qilu University of Technology (Shandong Academy of Sciences) (Grant No. 2023RCKY054), and the Basic Research Projects of Science, Education and Industry Integration Pilot Project of Qilu University of Technology (Shandong Academy of Sciences) (Grant No. 2023PX081).

References

[1] Zhang Z, Tang J, Ni H and Huang T 2023 *Nonlinear Dyn.* **111** 10629
[2] Liu P, Wang X, Su Y, Liu H and Unar S 2023 *IEEE Trans. Circuits Syst. I* **70** 2511
[3] Zhou S, Qiu Y, Wang X and Zhang Y 2020 *Nonlinear Dyn.* **111** 9571
[4] Nan R, Hu L, Huang Z, Wang M and Luo G 2023 *Expert Syst. Appl.* **238** 122052
[5] Nan R, Tong W and Zhou W 2023 *Signal Process.* **211** 109107
[6] Gong L and Luo H 2023 *Opt. Laser Technol.* **167** 109665
[7] Wang X and Liu P 2022 *IEEE Trans. Circuits Syst. I* **69** 1291
[8] Zheng W, Yan L, Gou C and Wang F Y 2021 *IEEE Trans. Cybern.* **52** 13181
[9] Liu X, Tong X, Zhang M, Wang Z and Fan Y 2023 *Nonlinear Dyn.* **111** 8771
[10] Rezaei B, Ghanbari H and Enayatifar R 2023 *Nonlinear Dyn.* **111** 9629
[11] Liu H, Zhang Y, Kadir A and Xu Y 2019 *Appl. Math. Comput.* **360** 83
[12] Zhang F F, Huang Z, Kou L, Li Y, Cao M Y and Ma F Y 2023 *Chin. Phys. B* **32** 010502
[13] Liu H, Wan H, Tse C K and Lu J 2016 *IEEE Trans. Circuits Syst. I* **63** 2010
[14] Bensikaddour, E H, Bentoutou Y and Taleb N 2020 *J. King Saud Univ.: Comput. Inf. Sci.* **32** 50
[15] Haddad S, Coatrieux G, Moreau-Gaudry A and Cozic M 2020 *IEEE Trans. Inf. Forensics Secur.* **15** 2556
[16] Dhall S, Pal S K and Sharma K 2022 *J. King Saud Univ.: Comput. Inf. Sci.* **34** 1533
[17] Cheng J, Guo S and He J 2022 *IEEE Internet Things J.* **9** 11408
[18] Su Y, Tong X, Zhang M and Wang Z 2023 *Nonlinear Dyn.* **111** 2841
[19] Tong X, Liu X, Liu J, Zhang M and Wang Z 2021 *Int. J. Bifur. Chaos* **31** 2150152
[20] Zhang F F, Zhang X, Cao M Y, Ma F Y and Li Z 2021 *IEEE Multimedia* **28** 96
[21] Teng L, Wang X and Xian Y 2022 *Inf. Sci.* **605** 71
[22] Mahalingam H, Veeramalai T, Menon A R and Amirtharajan R 2023 *Mathematics* **11** 457
[23] Hsieh K S and Wang C M 2022 *J. Inf. Secur. Appl.* **65** 103126
[24] Singh A K, Chatterjee K and Singh A 2023 *IEEE Trans. Industrial Informatics* **19** 1957
[25] Wu Y, Zhang L, Berretti S and Wan S 2023 *IEEE Trans. Industrial Informatics* **19** 2089