

Synchronously scrambled diffuse image encryption method based on a new cosine chaotic map

Xiaopeng Yan(闫晓鹏), Xingyuan Wang(王兴元), and Yongjin Xian(咸永锦)
Citation: Chin. Phys. B, 2022, 31 (**8**): 080504. DOI: 10.1088/1674-1056/ac5a43
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

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

Exponential sine chaotification model for enhancing chaos and its hardware implementation

Rui Wang(王蕊), Meng-Yang Li(李孟洋), and Hai-Jun Luo(罗海军)
Chin. Phys. B, 2022, 31 (**8**): 080508. DOI: 10.1088/1674-1056/ac6335

Neural-mechanism-driven image block encryption algorithm incorporating a hyperchaotic system and cloud model

Peng-Fei Fang(方鹏飞), Han Liu(刘涵), Cheng-Mao Wu(吴成茂), and Min Liu(刘旻)
Chin. Phys. B, 2022, 31 (**4**): 040501. DOI: 10.1088/1674-1056/ac272d

FPGA implementation and image encryption application of a new PRNG based on a memristive Hopfield neural network with a special activation gradient

Fei Yu(余飞), Zinan Zhang(张梓楠), Hui Shen(沈辉), Yuanyuan Huang(黄园媛), Shuo Cai(蔡烁), and Sichun Du(杜四春)
Chin. Phys. B, 2022, 31 (**2**): 020505. DOI: 10.1088/1674-1056/ac3cb2

Fractal sorting vector-based least significant bit chaotic permutation for image encryption

Yong-Jin Xian(咸永锦), Xing-Yuan Wang(王兴元), Ying-Qian Zhang(张盈谦), Xiao-Yu Wang(王晓雨), and Xiao-Hui Du(杜晓慧)
Chin. Phys. B, 2021, 30 (**6**): 060508. DOI: 10.1088/1674-1056/abda35

An image encryption algorithm based on improved baker transformation and chaotic S-box

Xing-Yuan Wang(王兴元), Huai-Huai Sun(孙怀怀), and Hao Gao(高浩)
Chin. Phys. B, 2021, 30 (**6**): 060507. DOI: 10.1088/1674-1056/abdea3

Synchronously scrambled diffuse image encryption method based on a new cosine chaotic map

Xiaopeng Yan(闫晓鹏)[1,†], Xingyuan Wang(王兴元)[1,2,‡], and Yongjin Xian(咸永锦)[1,§]

[1] *School of Information Science and Technology, Dalian Maritime University, Dalian* 116026, *China*
[2] *Guangxi Key Laboratory of Multi-source Information Mining & Security, Guangxi Normal University, Guilin* 541004, *China*

(Received 12 January 2022; revised manuscript received 2 March 2022; accepted manuscript online 3 March 2022)

We present a new cosine chaotic mapping proved by chaos theory test and analysis such that the system has good cryptography properties, wide chaos range, simple structure, and good sensitivity to initial value, and the mapping can meet the needs of chaotic image encryption. Based on the cosine chaotic system, we propose a new encryption method. First, according to the cyclic characteristics of the mapping, the cyclic information wave is simulated. Second, the quasi-Doppler effect is used to synchronously scramble and diffuse the image to obfuscate the original pixel. Finally, the XOR diffusion of image pixels is carried out by information wave to further enhance the encryption effect. Simulation experiment and security analysis show that the algorithm has good security, can resist the common attack mode, and has good efficiency.

Keywords: chaos mapping, cosine mapping, cyclic information wave, doppler effect, image encryption

PACS: 05.45.–a, 95.75.Mn, 95.10.Fh, 05.45.Ac **DOI:** 10.1088/1674-1056/ac5a43

1. Introduction

Nowadays, the explosive development of the information age has led to a lot of security problems. No matter whether it is information itself or the process of information transmission, there are many security risks. As a kind of widely used information carriers, digital image plays a decisive role in the process of the modern information transmission. In a network, there are a large number of images per second by transmission, processing and sharing. Therefore, digital image information security problem is also gradually attractive. In order to protect the privacy and the safety of materials and non-public information, image security has become an important information security problem.

In the traditional information transmission, most of the information is text information, so the traditional encryption algorithm is mainly used to encrypt the text information. The volume of this algorithm is large, and the correlation of the algorithm itself is strong. Therefore, in the direction of image encryption, this type of algorithm is unsuitable.[1–3] In order to develop algorithms suitable for image encryption, many researchers began to develop corresponding encryption algorithms based on the characteristics of digital images. Among them, chaotic system encryption,[4–7] biological DNA simulation coding,[8,9] transformation method based on optical characteristics,[10–12] quantum cryptography[13–15] and other methods have been gradually applied in image encryption. In image hiding,[16–18] information security,[19–21] watermarking,[22–24] digital image security,[25–28] and other aspects, these basic theories have played an important role. Among them, chaotic systems gradually attracted more and more attention because of their good characteristics. Due to their pseudo-randomness, unpredictability, ergodic property and initial value sensitivity, chaotic systems have good applications in the field of encryption, so many encryption methods based on chaotic systems began to be proposed.

Because of its adaptability to the encryption field, chaotic mapping is widely used in encryption algorithms. We classified the systems according to the number of system parameters, and we did this for both high-dimensional chaotic systems and low-dimensional chaotic systems. Low-dimensional chaotic systems have relatively simple structures and use very little resources, However, its chaotic behavior only exists in a limited range, so it can be predicted.[29–31] High-dimensional systems, on the other hand, exhibit excellent chaotic behavior and unpredictability. As a result, their structures are more intricate, consume more resources, and take longer to operate. It is challenging to put many high-dimensional systems into practice. Finding a chaotic system with good chaos and a straightforward structure is now a crucial step in developing encryption techniques.[32]

Many researchers have also proposed numerous stronger chaotic systems, such as one-dimensional chaotic systems based on the design of sine and inverse sine functions. Although it is still easier to predict than other systems, its encryption efficiency has greatly improved over other systems in recent years. Many classical chaotic systems were used as

[†]Corresponding author. E-mail: karasyxp@126.com
[‡]Corresponding author. E-mail: xywang@dlmu.edu.cn
[§]Corresponding author. E-mail: marsxyj@163.com

© 2022 Chinese Physical Society and IOP Publishing Ltd

a base structure to encrypt algorithms. Hua and Zhou[33] put forth a brand-new two-dimensional chaotic system that effectively fixed the two-dimensional chaotic system's flaws. To create a new chaotic system and incorporate it into an encryption algorithm, some researchers suggested combining the conventional sinusoidal mapping with logistic mapping.[34–37] A custom color image encryption technique based on various types of coupling mapping was proposed by Wang *et al.*[38] Although the algorithm has strong security, it encrypts data slowly.

A new low-dimensional chaotic mapping relying on cosine function with good chaos effect is proposed in this paper because of the limitations of the low-dimensional chaotic system and the complexity of the high-dimensional chaotic system, and it is named as the one-dimensional cosine system (C-LS). The new chaotic mapping is put to the test using the conventional theoretical analysis method, and it is demonstrated to have excellent chaotic performance in the scope of infinite real parameters. Additionally, we use the C-LS system in the domain of encryption to further strengthen the security of the encryption algorithm due to its excellent characteristics. Thus, we suggest a fresh encryption scheme. In this algorithm, the scrambling and diffusion of the image are realized by simulating the information wave model based on cosine chaos mapping, generating the cyclic information wave, and using the information wave diffusion model. The circular information wave has a doppler-like effect that simultaneously diffuses and scrambles the image matrix. Additionally, the secondary XOR diffusion is used to deepen the encryption effect in order to further ensure it. Following a thorough experimental analysis of the algorithm's experimental results, we demonstrate that the algorithm can effectively withstand common attack types and that it has good security on its own.

2. Basic theory of algorithm

2.1. Chaotic system

2.1.1. Logistic chaotic maps

The chaos map has excellent initial value sensitivity, and the initial value and control parameters can be slightly modified to obtain two completely different results. Therefore, the chaotic system is very suitable for applications in encryption. Among the existing few nonlinear systems, the logistic map is a well-known 1-D chaotic system that is used in cryptography. According to mathematics, they can be defined as follows:

$$x_{i+1} = 4\delta x_i(1-x_i), \tag{1}$$

where δ and ϕ represent the control parameters, $\delta \in [0,1]$ and $\phi \in [0,1]$. They lead to an iterate x_{i+1} from the previous one x_i and generate the chaotic sequences $x_i \in (0,1)$.

2.1.2. Sine chaotic map

The sine chaotic system is based on sinusoidal function. As a result, the input angle is converted to the output angle within the range of $[0,1/\pi]$. In terms of mathematics, sine mapping is defined as follows:

$$x_{i+1} = Q(x_i) = t\sin(\pi x_i), \tag{2}$$

where t represents the control parameter, and $Q(x_i)$ stands for the sine mapping.

2.2. Cosine chaotic mapping

The cosine chaotic maps take the structure shown in Fig. 1.

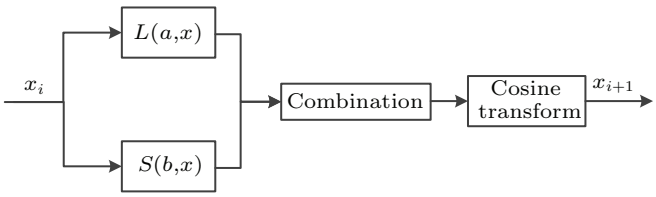


Fig. 1. Cosine chaotic mapping construction.

Here $L(a,x_i)$ and $S(a,x_i)$ represent chaotic mapping models with control parameters, $L(a,x_i)$ and $S(a,x_i)$ are improved and combined. Using the weighted model, a new chaotic mapping model is constructed using a nonlinear cosine transform. As a result of the Logistic chaotic mapping model and the sine chaotic mapping model, we construct a new one-dimensional cosine chaotic mapping model as follows:

$$x_{i+1} = \cos[(L(a,x_i) \times S(a,x_i)) \times n \times T]. \tag{3}$$

The control parameters of the system are retained, and π in the sine mapping is replaced by period T, and a new one-dimensional C-LS chaotic mapping model is finally constructed as follows:

$$\begin{aligned} x(n) = \cos[&(r \times x(n-1) \times (1-x(n-1)) \\ &\times \sin(x(n))) \times i \times T]. \end{aligned} \tag{4}$$

Here, r represents the control parameter of chaotic mapping, i is the length of the mapping information wave, and T is the period of the cosine mapping.

In the system mapping, we take r as the control parameter. Based on the cosine function, the new chaotic map can be derived by ignoring the negative value of the parameter μ.

2.2.1. Chaos trajectory

The C-LS chaotic system exhibits a very high chaotic state within the parameter range and has a very wide range of chaos. The positive real number space is covered by its chaotic area because it is based on the cosine function. For cryptography, a system with sufficient key space, sufficient complexity,

and unpredictability can better meet the needs of encryption. Later, we test the new cosine chaotic system using the corresponding dynamic analysis techniques.

When parameters in a dynamic system change, the output value range is described using a system trajectory bifurcation diagram. It can be an important tool for understanding the causes of instability and chaos as well as how different states of the system relate to one another and change over time. The relationship between bifurcation and the system's structural stability is very close. The bifurcation graph produced by logistic mapping, sine mapping, and C-LS mapping with a change in control parameters is shown in Figs. 2 and 3.

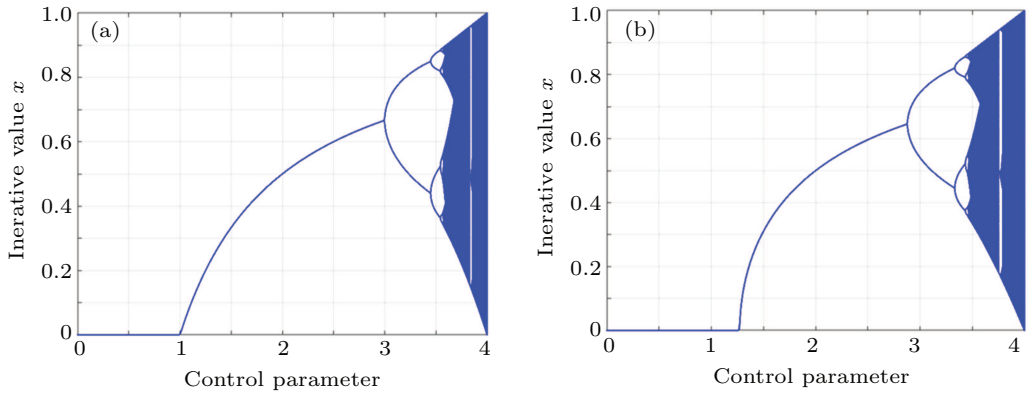


Fig. 2. Chaotic map bifurcation graph: (a) logistic mapping, (b) sine mapping.

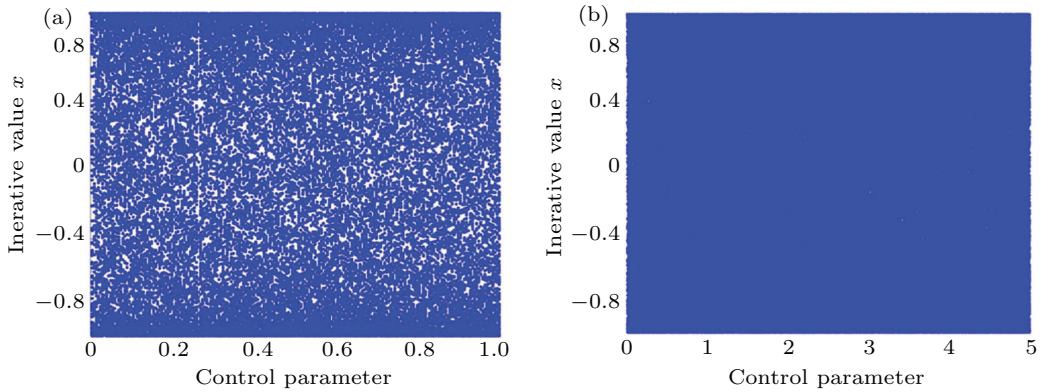


Fig. 3. Bifurcation graph of C-LS mapping in different parameter ranges: (a) bifurcation diagram with control parameters between (0,1), (b) bifurcation diagram with control parameters between (0,5).

As seen in Fig. 3, the C-LS mapping's bifurcation graphs are evenly and randomly distributed within the parameter's norm, covering the entire region. This shows that the newly generated chaotic mapping exhibits robust chaotic behavior across the entire parameter range.

2.2.2. Lyapunov exponent

The initial state sensitivity and unpredictability of one chaotic mapping are its most prominent dynamical characteristics, and these characteristics can be measured using the Lyapunov exponent (LE). The average exponent rate of convergence or divergence for two orbits of a chaotic mapping that are close to each other in the phase plane can be described by the LE using the formula[39]

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln \left| f'(x_i) \right|. \tag{5}$$

Their chaos phenomenon gradually becomes worse as the LE increases. If the LE is positive, it means that regardless of how close or far apart the two trajectories are from each other, they will exhibit completely different incremental states over time. Therefore, the system is in a chaotic state when the LE is positive. The LE maximum can be used to assess the predictability of a high-dimensional system, which typically has two or more LE values. As a result, the system is in a chaotic state when its maximal LE is greater than 0. The hyperchaotic phenomenon is identified when the system has more than one positive LE and its orbits diverge in multiple directions. A larger LE indicates that the MD displays better hyperchaotic behaviors, which are much more complex and difficult to predict.

Comparatively and elaborately using the Lyapunov exponent can make the issue more obvious. We use the Lyapunov exponent as the benchmark value to evaluate whether the system exhibits chaotic properties. Using the LE maximum, we can determine if the system exhibits chaotic behavior.

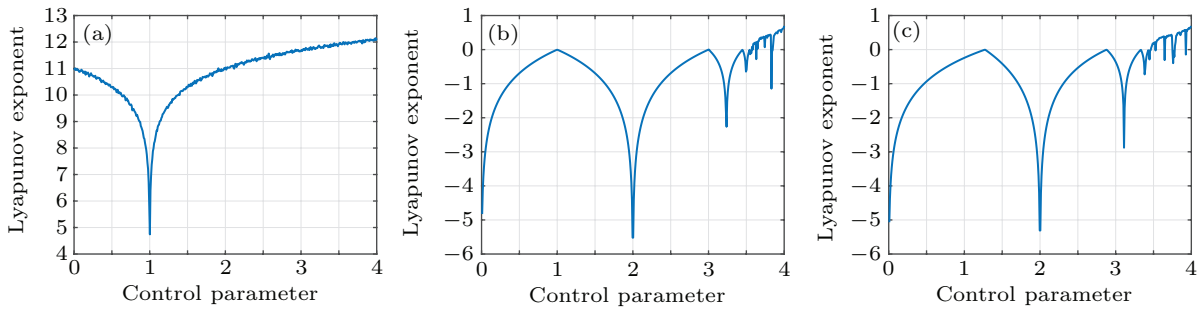


Fig. 4. The Lyapunov exponent of chaotic maps: (a) Lyapunov exponent of C-LS mapping, (b) Lyapunov exponent of logistic mapping, (c) Lyapunov exponent of sine mapping.

2.2.3. Initial state sensitivity

One of the most crucial characteristics of chaotic systems is their sensitivity to initial values. It symbolizes the sensitivity of an orbit whose initial values are almost infinitesimal and diverge exponentially following a set number of iterations. We create two tracks with initial value differences of 10^{-15}, as shown in Fig. 5(a), and control parameter differences of 10^{-15}, as shown in Fig. 5(b), to further analyze the sensitivity of the map (b). The orbits diverge after five to six iterations, as depicted in the figure, as a result of the system's highly chaotic behavior.

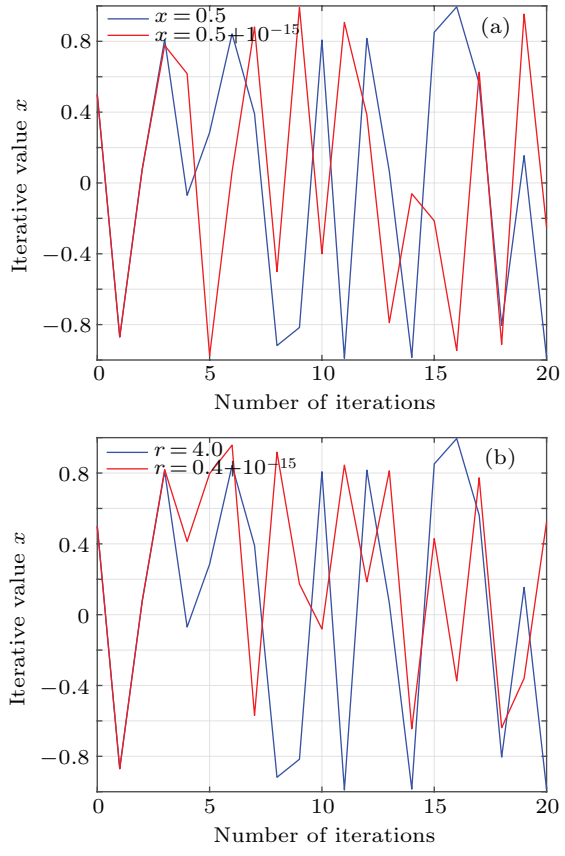


Fig. 5. Chaotic mapping initial value sensitivity: (a) initial value sensitivity, (b) control parameter sensitivity.

2.3. Cosines map circular information waves

The term "cyclic information wave" describes a model of ripples with a set frequency of occurrence and an ongoing diffusion cycle. Doppler effect and water surface ripple are included in the traditional model.

The Doppler effect is a frequent occurrence in nature that affects almost all types of waves, including sound, light, and electric ones. When the wave source and the observation position move together, a Doppler wave occurs, and when this happens, the signal state that the observation position receives will differ in frequency characteristics, depending on how the wave source and observation position move. The frequency of the received signal from the moral wave source will be higher and the wavelength will shorten as the observation position moves closer to the position of the wave source, indicating that the information wave is compressed. On the other hand, the wavelength lengthens as the frequency rises. The effect increases with increasing source velocity. The Doppler wave model can be described mathematically as follows: if the wave source's frequency is F, its motion speed is V, the sound speed in air is U, and the distance between the stationary observer P and the wave source's motion direction is L, then the frequency model that the observer receives is expressed as

$$f = \frac{u}{u - \dfrac{v^2(t-t_0)}{\sqrt{t^2+v^2(t-t_0)^2}}} f_0, \tag{6}$$

where t_0 denotes the time center that corresponds to the observer's location; when $t < t_0$ and $f > f_0$, t_0 denotes the wave source's proximity to the observer; when $t > t_0$ and $f < f_0$, t_0 denotes the wave source's distance from the observer.

In order to simulate the Doppler effect and create an information wave model, we use the C-LS chaotic model as the generating function. The cyclic diffusion effect, period and frequency of C-LS mapping are good. Using chaos to build a cyclic information wave model, pseudo-random sequences are generated based on C-LS mapping:

(1) The information wave's length is given as n, and the circular information wave's polynomial is given as m.

(2) Different pseudo-random sequences are generated in multiple columns using C-LS chaotic mapping, and the sequences are chosen as frequency and parameter sequences in the polynomial.

(3) The circular information wave model is created using the C-LS mapping as the generation system:

$$e(n) = \cos[(r \times x_i \times (1 - x_{i-1}) \times \sin(x_i)) \times n \times T], \quad 1 \le i \le m, \tag{7}$$

where T is the period.

The high frequency shifts to the low frequency as the distance grows. To achieve the goals of synchronous scrambling and diffusion of the image, it is possible to use the frequency shift property of the circular information wave to change the gray value and position of the image pixel. The appropriate information wave polynomial is chosen based on the image size, and the frequency array of the circular information wave is generated using a chaotic system simulation. The necessary information wave can then be generated after a number of cycle iterations based on various periods.

When scrambling an image, the wave used to generate the information is dependent on the size of the image because the generated cycle information wave length is inversely proportional to the image size. As a result, when the image is larger, the wave used to generate the information will take more time, which has a significant negative impact on how quickly the scrambling process proceeds, so the algorithm adopted for chunking thoughts, according to the size of the block to generate a wave doppler and scrambling, will greatly improve the execution efficiency of this algorithm.

2.4. Key generation

We decide to use the hash function as the secret key generation technique. The compression length of a given message sequence can be specified by the hash algorithm. This algorithm has a very high safety factor and can withstand the majority of brute force attacks, but some algorithms have recently been broken, including SHA-1 and others. Thus, as the primary part of key generation, we opt for the more popular SHA-512 function.

Due to the peculiarity of the hash function, if the plaintext has a pixel value transformed, then the generated hash sequence group will be completely different, so it has extremely high security and sensitivity. We operate the SHA-512 function to hash the unencrypted image to obtain hash array, from which we select the appropriate sequence value for corresponding processing to obtain the secret key value we need.

The algorithm's complexity of 2^{512} makes it robust enough to fend off brute force attacks. We select a 128-bit hash sequence and transform it into an array:

$$H = [h_1, h_2, \ldots, h_{128}]. \tag{8}$$

In the following, we describe the hash function-based secret key generation process.

Step 1 The hash algorithm is used to calculate the plaintext image. The parameter used to iterate the chaotic system is chosen to be the corresponding hash value. We initialize the sequence value to conform to the requirements of the chaotic system's correlation coefficient. The formula for calculating the initial value and control parameters is as follows:

$$\begin{cases} x_1(0) = \text{Key}_1, \ u_1 = 3.59 + 0.11\text{Key}_7, \\ x_2(0) = \text{Key}_2, \ u_2 = 3.59 + 0.11\text{Key}_8, \\ x_3(0) = \text{Key}_3, \ u_3 = 3.69 + 0.11\text{Key}_9, \\ x_4(0) = \text{Key}_4, \ u_4 = 3.69 + 0.11\text{Key}_{10}, \\ x_5(0) = \text{Key}_5, \ u_5 = 3.79 + 0.11\text{Key}_{11}, \\ x_6(0) = \text{Key}_6, \ u_6 = 3.79 + 0.11\text{Key}_{12}. \end{cases} \tag{9}$$

Step 2 The obtained parameters are initialized to produce those that satisfy the requirements of the chaotic system. We produce the necessary pseudo-random sequence using the C-LS cyclic information wave generation system. The cyclic information wave's sequence is transformed into a matrix with the same size as the matrix that will be diffused during the diffusion stage. The components of the pseudo-random sequence A must first be converted before being normalized. The normalized processing formula of circulating information wave is given as follows:

$$W_i = \bmod(\text{floor}(T_i \times 10^{14}), 100). \tag{10}$$

Convert the normalized sequence obtained into the key matrix K for diffusion.

$$W = \text{reshape}(W_i, M, N). \tag{11}$$

3. Encryption algorithm

3.1. Cyclic information waves are simultaneously scrambled and diffused

The synchronous scrambling and diffusion process is realized as follows:

Step 1 Obtain the median element value of P as P (mid), the maximum element value as P, and the original image matrix as P (max). Utilize the P matrix to perform a traversal comparison operation. If $p(u,v) \le p(\text{mid})$, record $L(u,v) = 0$; otherwise, record $L(u,v) = 1$, and get the position record matrix L.

Step 2 Using Eq. (7) and matrix P, the cyclic information wave is produced. Information sequence Z is then obtained, and the initial operation is performed on the sequence Z:

$$z_2 = \text{floor}(\bmod(z \times 10^{14}, 100)). \tag{12}$$

Converts the initialized sequence to matrix z_3 of the same size as matrix P.

Step 3 Depending on the different intensities R, the information wave is embedded and diffused to matrix P. At the same time, the position of the matrix element is modified, and the position of the matrix element of P is scrambled.

$$z_4 = p(u,v) \otimes (r \times z_3(u,v)), \tag{13}$$

$$z_5(u,v) = z_4(z_3(u,v)). \tag{14}$$

The image is finally obtained after synchronous scrambling and diffusion.

3.2. Image encryption process

According to the needs of the algorithm, the target image matrix is first divided into $N \times N$ small blocks, then into smaller blocks, and finally block-after-block division is carried out on the synchronized scrambling diffusion operation. Using an 256×256 image as an example, this article chooses images of various sizes for experiments. The block 8×8 is a matrix block. The steps for encryption are as follows:

Step 1 Using C-LS chaotic mapping, six rows of chaotic pseudo-random sequences are created, and the sequences are initialized:

$$\begin{aligned} AA1(i) &= \text{floor}(A1(i) \times 100) + 1, \\ BB1(i) &= \text{floor}(A2(i) \times 10) + 1, \\ AA2(i) &= \text{floor}(A3(i) \times 100) + 1, \\ BB2(i) &= \text{floor}(A4(i) \times 10) + 1, \\ AA3(i) &= \text{floor}(A5(i) \times 100) + 1, \\ BB3(i) &= \text{floor}(A6(i) \times 10) + 1. \end{aligned} \tag{15}$$

Step 2 Choose the $AA1$ and $BB2$ sequence, apply Eq. (7) in period T generated wave doppler information, convert information sequence of the same size as matrix p wave information matrix, and then utilize the information matrix for the block to apply Eqs. (13) and (14) to sync block image scrambling and diffusion, after the completion of the merger block image, and the output, as the first phase encryption results for P_1.

Step 3 Use Eq. (7), the sequences $AA2$ and $BB2$ were chosen to produce Doppler information waves with the period T_1, which were then transformed into a matrix with the same size P_1. In accordance with Eq. (5), P_1 undergoes traversal sorting and scrambling, and the scrambling matrix P_2 is produced.

Step 4 Using Eq. (7), the $AA3$ and $BB3$ are chosen to produce information waves with the period T_2 that are then transformed into a matrix with the same size P_2. To achieve diffusion operation, the matrix P_2 is used in the XOR operation, and the final encrypted image is output.

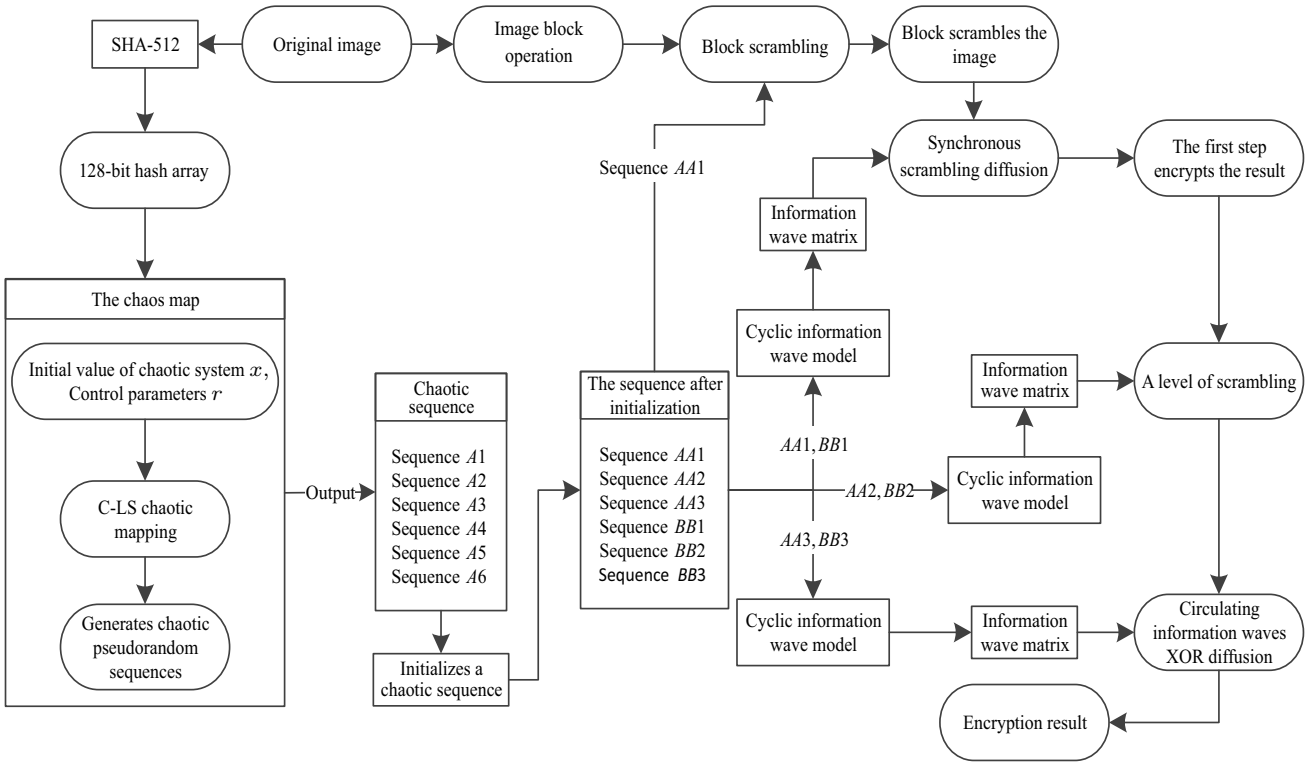


Fig. 6. Encryption process flow chart.

The reverse of encryption is decryption. The precise operational flow of the encryption algorithm suggested in this paper is shown Fig. 6.

4. Simulation results

The simulation-based safety verification algorithm is presented in algorithm, we select a representative target image, analyze it comprehensively according to different resolutions and colors, write and implement the code using MATLAB software, and conduct the simulation and experimental analysis of the algorithm under the Window 10 operation system.

We use the images "Lena" in color, "boat" in grayscale, "TestPat-1K," and "Lena" in grayscale to conduct an encryption simulation experiment. The results are then subjected to the necessary security analysis. Figure 7 displays the encrypted and unencrypted versions of the image.

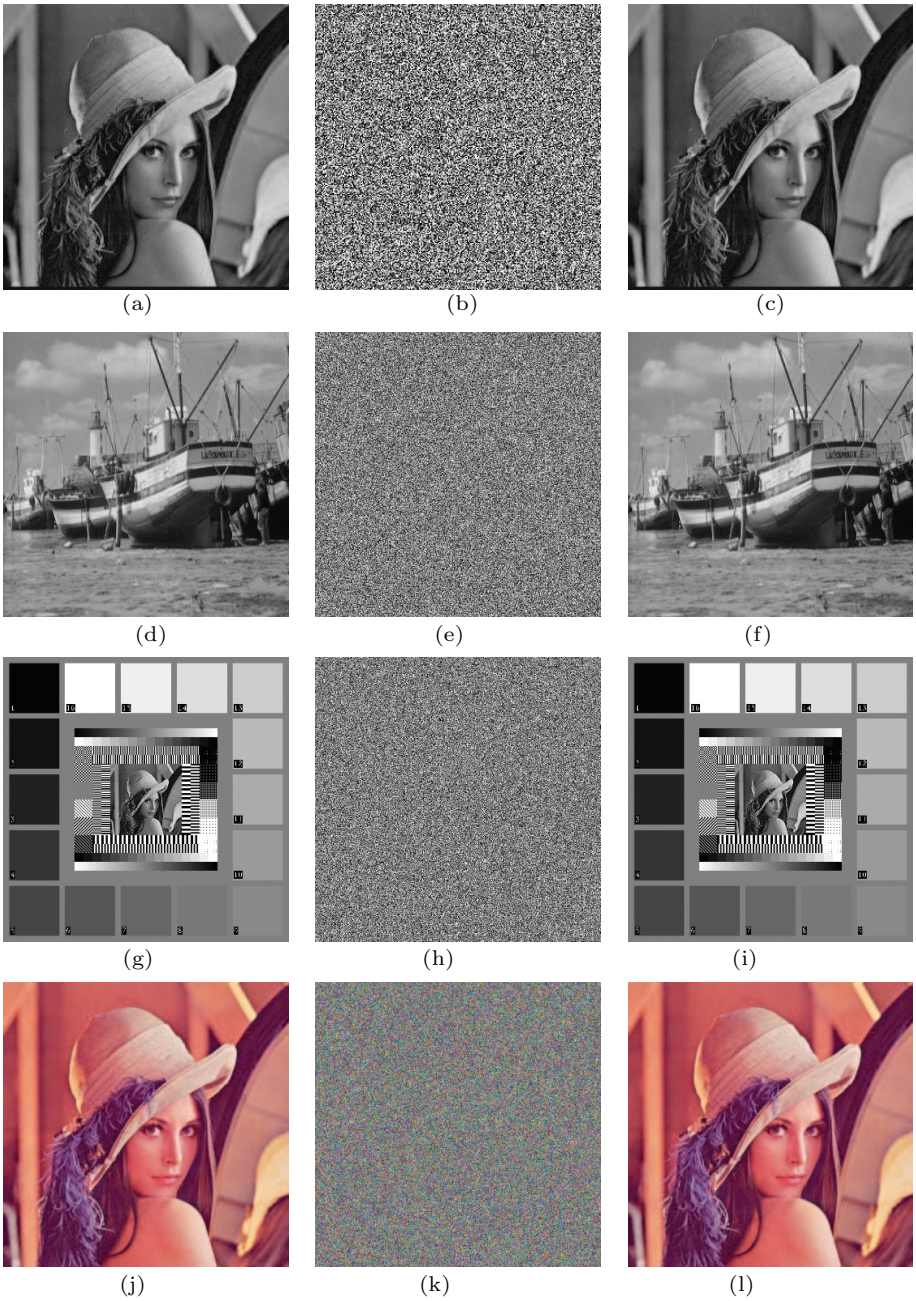


Fig. 7. Experimental results. (a) Lena, (b) encryption result, (c) decrypted, (d) boat, (e) encryption result, (f) decrypted, (g) TestPat-1k, (h) encryption result, (i) decrypted, (j) color Lena, (k) encryption result, (l) decrypted.

5. Security analysis

In terms of security, there are a number of security requirements such that our algorithm should meet in order to comply with safety standard requirements. To determine whether the algorithm has reliable security through verification, we should conduct the appropriate security verification on the simulation results and the algorithm itself. We should compare numerical results to verify the encryption effect for encryption methods.

On the algorithm, we analyze common attacks, brute force attacks, statistical attacks, robustness attacks, and some plaintext attacks. The results show that the proposed theory has a high degree of reliability when compared to both experimental and numerical simulation results.

5.1. Key analysis

Large key spaces used in the encryption techniques make them resistant to brute-force attacks. The resistance of the key space increases with its size. Therefore, the design algorithm should choose the secret key space with the larger size. There are various components to the algorithm's key space. This paper's key space $2^6 \times 2^{512} \times 10^{14\times 6}$ is much larger than 2^{100}. Because the algorithm's key is 6 bits, the computer's precision is 10^{-14}. It takes SHA-512 as its hash function, and the space size is 2^{512}. Thus, in our proposed algorithm, the key space is sufficient to resist all kinds of brute-force attacks.

5.2. Key sensitivity analysis

In order to estimate the sensitivity and security of the algorithm, our model achieves high key sensitivity. A small perturbation can significantly change the reconstruction output, and the current encryption result obtained is very different from the result prior to the key change.

In the simulation, we first choose a secret key value, change it from 0.3801 to 0.380000000001, and then use the two keys to get the two encrypted images of Figs. 8(a) and 8(b). Make a distinction using two encrypted images. In Fig. 8(c), the image difference is displayed. The two encryption results are very dissimilar, as shown in Fig. 8(c). Finally, we decrypt Fig. 8(a) using the modified key, and the result in Fig. 8(d) shows that the modified key is unable to decrypt the original key encryption result.

We again change the secret key information, choose a pixel from the original image matrix, add or subtract 1, modify the pixel value, and then encrypt the image before and after the change, respectively. Figure 8(d) is the pixel value after modification encrypted image. Figure 8(e) is the difference between Figs. 8(a) and 8(d). This result shows the extremely strong key sensitivity of the algorithm script in this paper.

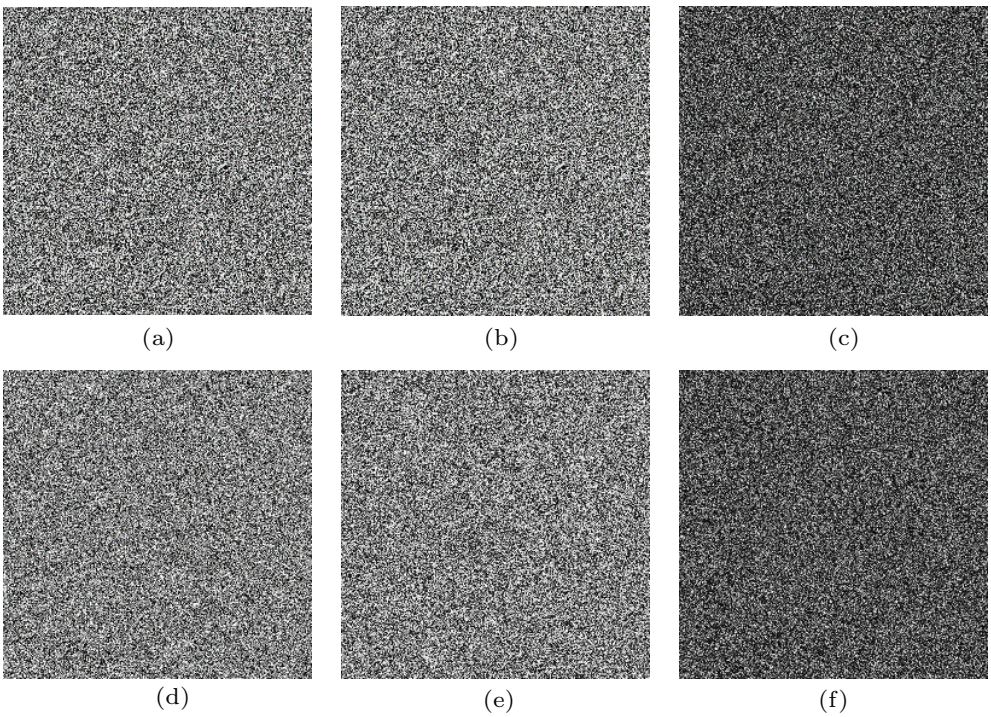


Fig. 8. Sensitivity test. (a) Encrypted with $x_1(0)$, (b) encrypted with modified $x_1(0)$, (c) difference between (a) and (b), (d) decrypted with modified $x_1(0)$, (e) encrypted with modified1-bit pixel, (f) difference between (e) and (a).

5.3. Statistical analysis

A series of simulation experiments and numerical analyses are conducted in this section in order to verify the reliability of the algorithm.

(1) Histogram

The unprocessed image's pixel distribution is more concentrated, and because of this, the overall pixel distribution is not uniform, which causes the histogram of the image to be very wavy. The image's pixels are evenly distributed after encryption, and the histogram can be used to visualize this distribution. The histogram ought to be flat as a result. Inequalities in the distribution of image pixels will be targeted by statistical attacks. A flat and uniform distribution of pixels can therefore withstand statistical analysis well.

The histogram results of the three different images chosen for the experiment are displayed in Fig. 9. The histogram of the encrypted image can be seen in Fig. 9, and exhibits a pixel distribution that is remarkably uniform.

(2) Correlation comparison

The unprocessed image has strong pixel correlation, and a statistical analysis attack on a strongly correlated image can easily leak or lose information content. In contrast, the encrypted image breaks up the pixel correlation of the original image, making it well resistant to the statistical type of attack. The encrypted image's pixel correlation can be decreased through encryption operation. The formulas (16) and (17)[40] are used to calculate the correlation of adjacent pixels in the encrypted image using the Lena graph as the experimental target. Figure 10 displays the correlation's numerical results. We have

$$t_{xy} = \frac{\operatorname{cov}(x,y)}{\sqrt{F(x)}\sqrt{F(y)}}, \tag{16}$$

with

$$\mathrm{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - G(x))(y_i - G(y)),$$
$$F(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - G(x))^2, \quad G(x) = \frac{1}{N}\sum_{i=1}^{N}x_i. \tag{17}$$

Calculating the correlation of the ciphertext image yields corresponding data. In the literature, data results have been compared.[41–44] Figure 11 and Table 1 display the comparison results. We can see from the comparison that the correlation coefficient obtained by the algorithm in this paper is actually smaller than the correlation coefficient produced by the algorithm in a number of other documents. Therefore, it can be inferred from the experimental findings and numerical analysis that the encryption algorithm suggested in this paper performs exceptionally well in resisting statistical analysis.

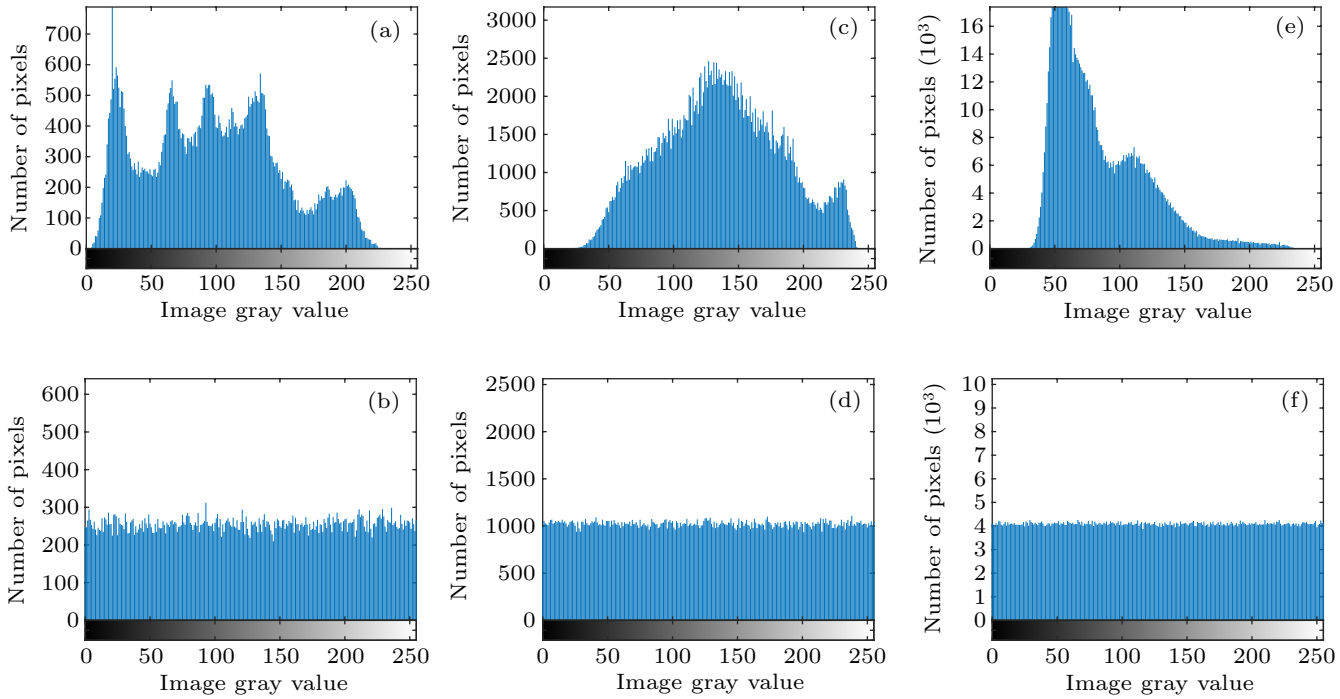


Fig. 9. Histogram of experimental images. (a) Original image of Lenna, (b) encryption image of Lenna, (c) original image of Elaine, (d) encryption image of Elaine, (e) original image of airport, (f) encryption image of airport.

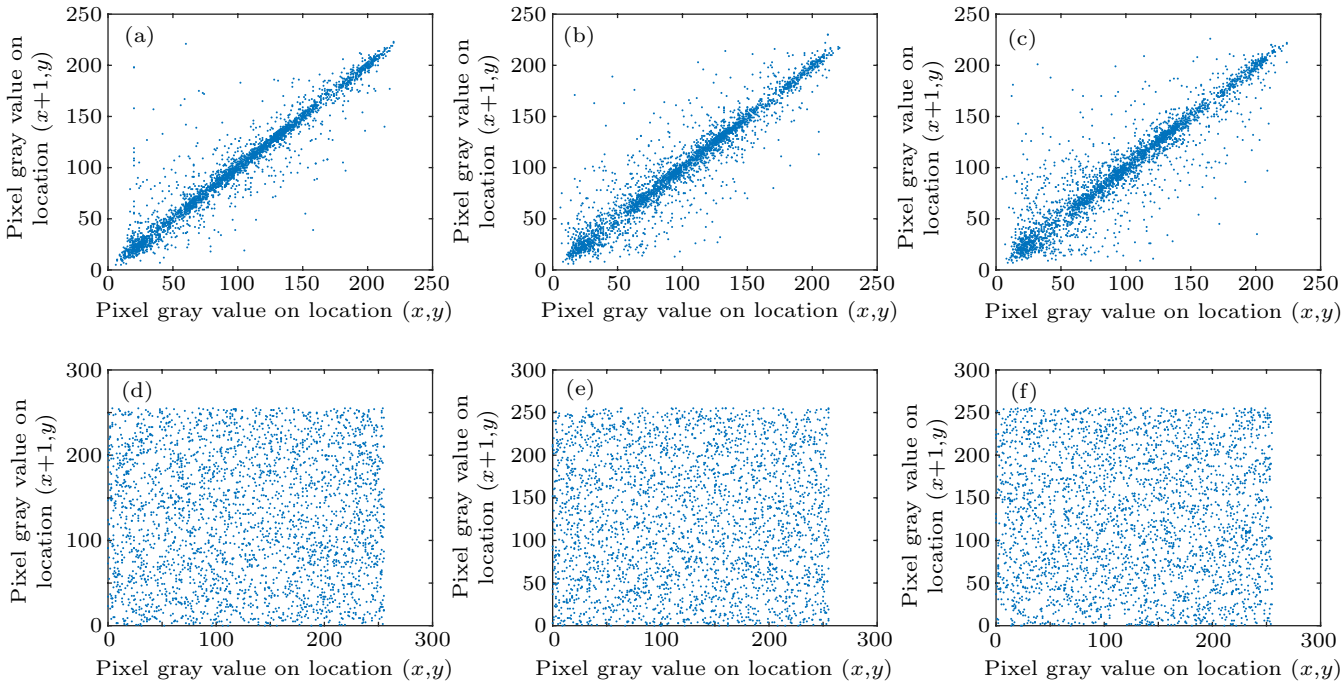


Fig. 10. Correlation of adjacent pixels: (a)–(c) plaintext image correlation, (d)–(f) ciphertext image correlation. (a) Horizontal correlations, (b) vertical correlations, (c) diagonal correlations, (d) horizontal correlations, (e) vertical correlations, (f) diagonal correlations.

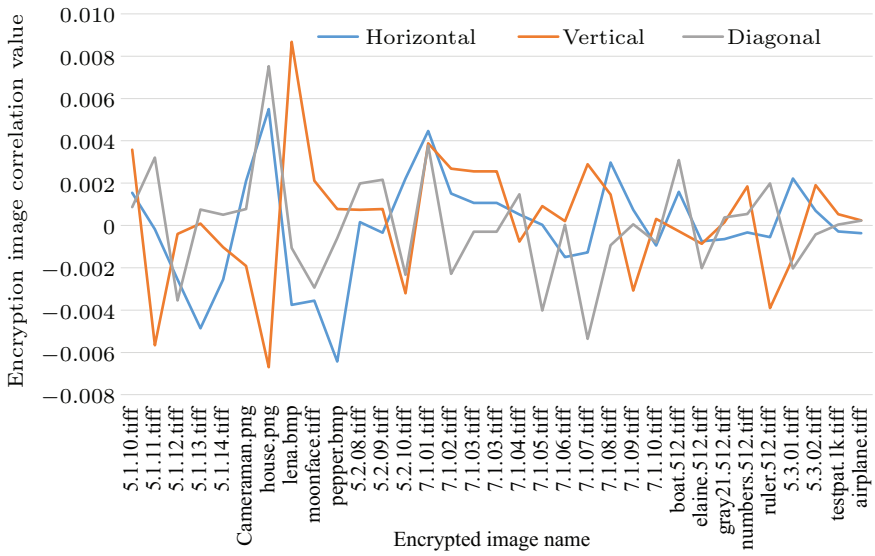


Fig. 11. Ciphertext correlation line graph.

Table 1. Correlation comparison results of adjacent pixels.

Image	Type	Proposed	Ref. [41]	Ref. [42]	Ref. [43]	Ref. [44]
			256×256			
Cameraman	Horizontal	0.005544399	–0.0211	0.0063	–0.0047	–0.0009
	Vertical	0.006040846	–0.0103	–0.0142	–0.0195	–0.0223
	The diagonal	0.003396314	0.0054	0.0168	0.0279	0.0025
Lena	Horizontal	–0.003755791	–0.0086	–0.0066	0.0011	–0.0063
	Vertical	0.008675043	–0.102	–0.0089	0.0098 -	0.0109
	The diagonal	–0.001064676	0.0125	0.0424	–0.0227	–0.0154
			512×512			
Elaine	Horizontal	–0.00056863	–0.0065	–0.0191	–0.0066	–0.0062
	Vertical	–0.001613027	–0.0096	–0.0130	–0.0019	–0.0197
	The diagonal	0.004815933	–0.0148	–0.0096	0.0007	–0.0169
			1024×1024			
Airport	Horizontal	–0.000251172	0.0040	–0.0061	0.0094	–0.0142
	Vertical	0.000211174	–0.0174	–0.0079	–0.0107	–0.0141
	The diagonal	–0.000535451	–0.0135	–0.0001	–0.0007	0.0002
Average	Horizontal	0.000242202	–0.00805	–0.00638	–0.0002	–0.0069
	Vertical	0.003328509	–0.03483	–0.011	–0.0107	–0.0113
	The diagonal	0.00165303	–0.0026	0.012375	0.0013	–0.0074

(3) Information entropy

Determine the image's information entropy and, using the information entropy's specific value, assess the likelihood of information leakage.

(i) Global information entropy

The calculation formula of global information entropy is as follows:[39]

$$H(s) = \sum_{i=0}^{2^n-1} p(m_i) \log_2 \frac{1}{p(m_i)}, \tag{18}$$

where $p(s_i)$ is the probability of s_i happening.

Global information entropy should typically be around 8 wirelessly. The likelihood of leakage decreases with proximity. By comparing the encryption results of the algorithm in this paper with the values in Refs. [41–44], we can see from Tables 2 and 3 that for the encryption results of the algorithm in this paper, the value of global information entropy is better than other similar algorithms, and it is very close to 8, so the probability of information leakage of this algorithm is very low.

(ii) Local Shannon entropy

To determine the algorithm's local information entropy, we use the equation

$$H_{k,T_B}(S,L) = \sum_{i=1}^{k} \frac{H(S_{T_B},L)}{k}. \tag{19}$$

The Shannon entropy must be within the range of [7.901515698, 7.903422936] after the algorithm has encrypted the images that satisfy the experimental requirements. This is known as a pass test. Table 4 displays the Shannon entropy values determined by the aforementioned formula following the encryption of the image using the algorithm suggested in this paper.

Table 2. Information entropy of encrypted image.

Image	Information entropy
Lena	7.9973
5.1.10	7.997428221
5.1.11	7.997163847
5.1.12	7.996849343
5.1.13	7.997181058
5.1.14	7.997504818
5.2.08	7.999279192
5.2.09	7.99929413
5.2.10	7.999234134
7.1.01	7.952500612
7.1.02	7.999351526
7.1.03	7.999364342
7.1.04	7.999212943
7.1.05	7.996934027
7.1.06	7.999279655
7.1.07	7.999290792
7.1.08	7.999151755
7.1.09	7.999249112
7.1.10	7.999264915
Boat.512	7.999314587
Gray21.512	7.999254663
Ruler.512	7.999330925
5.3.01	7.999820634
5.3.02	7.999831011

Table 3. Entropy comparison results of encrypted image information.

Image	Proposed	Ref. [41]	Ref. [42]	Ref. [43]	Ref. [44]
256×256					
5.1.09	7.9973	7.9991	7.9951	7.9965	7.9964
Cameraman	7.997403587	7.9966	7.9955	7.9964	7.9990
512×512					
Elaine	7.999254663	7.9972	7.9939	7.9971	7.9951
5.2.08	7.999279192	7.9987	7.9951	7.9980	7.9956
1024×1024					
5.3.02	7.999831011	7.9966	7.9966	7.9969	7.9957

Table 5. Local Shannon entropy.

Image	Proposed
256×256	
5.1.10	7.90176933
5.1.11	7.90264426
5.1.12	7.90318455
5.1.13	7.90318211
5.1.14	7.90248489
512×512	
5.2.08	7.90297607
5.2.09	7.90206809
5.2.10	7.90293824
7.1.01	7.90118411
7.1.02	7.89797925
7.1.03	7.90107048
7.1.03	7.90325206
7.1.04	7.90306191
7.1.05	7.84435505
7.1.06	7.90174174
7.1.07	7.9028045
7.1.08	7.90259253
7.1.09	7.90173687
7.1.10	7.90173687
Boat.512	7.90103272
Gray21.512	7.90128544
Ruler.512	7.90187515
1024×1024	
5.3.01	7.89830566
5.3.02	7.90210333
PASS/ALL	**21/24**

5.4. The χ^2 test

In this section, we examine the ciphertext images' pixel distribution. Chi-square detection tests the target quantitatively and yields numerical results that are quantitative, helping to prevent visual misperception. For comparative analysis, we use the formula provided in Ref. [39] as follows:

$$\chi^2 = \sum_{i=0}^{255} \frac{(q_i - q)^2}{q}, \tag{20}$$

where q is defined as

$$q = \frac{M \times N}{256}. \tag{21}$$

The encrypted images produced by our algorithm are all less than the limit value of 293.2483 after the chi-square detection, as can be seen from the numerical results in Table 6. As a result, the experimental findings demonstrate that the algorithm can withstand attacker-conducted statistical attacks.

Table 6. Uniformity evaluation by chi-square test.

Image	Result	Decision
5.1.10	232.703	ADOPT
5.1.11	257.437	ADOPT
5.1.12	286.023	ADOPT
5.1.13	255.953	ADOPT
5.1.14	226.367	ADOPT
5.2.08	262.072	ADOPT
5.2.09	256.775	ADOPT
5.2.10	278.066	ADOPT
7.1.01	282.324	ADOPT
7.1.02	235.908	ADOPT
7.1.03	241.177	ADOPT
7.1.03	230.517	ADOPT
7.1.04	286.482	ADOPT
7.1.05	257.611	ADOPT
7.1.06	262.042	ADOPT
7.1.07	257.578	ADOPT
7.1.08	248.509	ADOPT
7.1.09	272.575	ADOPT
7.1.10	267.253	ADOPT
Boat.512	248.398	ADOPT
Gray21.512	270.152	ADOPT
Ruler.512	243.429	ADOPT
5.3.01	245.337	ADOPT
5.3.02	248.071	ADOPT

5.5. Resistance differential attack analysis

Differential attack is one of the plaintext attacks, by modifying the relevant information of the plaintext image, comparing its encryption results, and analyzing the correlation. The calculation formulas are as follows:[40]

$$D(i,j) = \begin{cases} 0, & c_1(i,j) = c_2(i,j), \\ 1, & c_1(i,j) \neq c_2(i,j), \end{cases} \tag{22}$$

$$\mathrm{NPCR} = \frac{1}{W \times H} \sum_{i=1}^{W} \sum_{j=1}^{H} D(i,j) \times 100\%, \tag{23}$$

$$\mathrm{UACI} = \frac{1}{W \times H} \left(\sum_{i=1}^{W} \sum_{j=1}^{H} \frac{|c_1(i,j) - c_2(i,j)|}{255} \right) \times 100\%. \tag{24}$$

The standard value of NPCR is calculated by

$$N_{\alpha}^{*}=\frac{L-\Phi^{-1}(\alpha)\sqrt{L/MN}}{L+1}. \tag{25}$$

The standard boundary of UACI is divided into two values on the upper line, and the two standard boundaries are calculated by[45]

$$\begin{cases} U_{\alpha}^{*-}=\mu_u-\Phi^{-1}(\alpha/2)\times\sigma_u, \\ U_{\alpha}^{*+}=\mu_u+\Phi^{-1}(\alpha/2)\times\sigma_u, \end{cases} \tag{26}$$

where

$$\mu_u=\frac{L+2}{3L+3}, \tag{27}$$

$$\sigma_u^2=\frac{(L+2)(L^2+2L+3)}{18MNL(L+1)^2}. \tag{28}$$

Table 7 compares and analyzes the NPCR and UACI of the encrypted image. In the differential attack evaluation, the closer the NPCR and UACI are to the standard value, the more it proves that the algorithm has higher resistance to attack. Through the data comparison in Table 7, Figs. 12 and 13, it can be seen that the algorithm proposed in this paper is relatively excellent in the experimental results of NPCR and UACI. In addition, by comparing with the literature,[46–48] it can be seen that the NPCR and UACI values and pass rate of our algorithm are the best.

Table 7. Comparison of NPCR(%) values and UACI(%) values.

Image	Proposed	Ref. [46]	Ref. [47]	Ref. [48]	Proposed	Ref. [46]	Ref. [47]	Ref. [48]
256×256	$N_{0.05}^{*}\geq 99.5693$				$U_{0.05}^{*-}=33.2824$, $U_{0.05}^{*+}=33.6447$			
5.1.09	99.6068	99.6338	99.6109	99.6124	33.4552	33.5119	33.5527	33.4652
5.1.10	99.6136	99.6017	99.5987	99.5972	33.4877	33.4263	33.4381	33.5448
5.1.11	99.6091	99.5956	99.5697	99.5956	33.4500	33.4192	33.4390	33.4162
5.1.12	99.6101	99.6292	99.6338	99.6017	33.5187	**33.2672**	33.4373	**33.2152**
5.1.13	99.6004	99.6109	99.6201	99.6552	33.4508	33.4252	33.3488	33.4699
5.1.14	99.6108	99.6185	99.6094	99.6002	33.4439	33.2919	33.5133	33.5554
512×512	$N_{0.05}^{*}\geq 99.5893$				$U_{0.05}^{*-}=33.3730$, $U_{0.05}^{*+}=33.5541$			
5.2.08	99.6115	99.6059	99.6056	99.6220	33.4694	33.4509	33.4377	33.4575
5.2.09	99.6087	99.6029	99.6410	99.6208	33.4610	33.4543	33.4939	33.4175
5.2.10	99.6105	99.6010	99.6067	99.5968	33.4566	33.4365	33.3888	33.4315
7.1.01	99.6086	99.6040	99.6132	99.6181	33.4886	33.4811	**33.5553**	33.5150
7.1.02	99.6095	99.5941	99.6124	99.6140	33.4487	33.4762	33.4342	33.5221
7.1.03	99.6113	99.6132	99.5983	99.6166	33.4708	33.5346	33.4585	33.4777
7.1.04	99.6098	99.6098	99.6052	99.6227	33.4680	**33.3450**	33.4830	33.4721
7.1.05	99.6105	99.5995	**99.5842**	99.5960	33.4630	33.5380	33.4393	33.4757
7.1.06	99.6078	99.6109	99.6086	99.6212	33.5036	33.4766	**33.5634**	33.5035
7.1.07	99.6115	99.5934	99.6193	99.6113	33.4596	33.4695	33.5241	33.4317
7.1.08	99.6104	99.6098	**99.5869**	99.5914	33.4662	33.4258	33.4251	33.4274
7.1.09	99.6091	**99.5815**	99.6094	99.6067	33.4565	33.4954	33.4606	33.4452
7.1.10	99.6079	**99.5850**	99.6063	99.6056	33.4368	33.4389	33.4119	33.4434
Boat.512	99.6097	99.6284	99.6132	99.6021	33.4924	33.4693	33.4993	33.4059
Gray21.512	99.6085	99.6014	99.6162	99.6239	33.4704	33.4667	33.4634	33.4554
Ruler.512	99.6088	99.6151	99.6189	99.5930	33.4694	33.4509	33.4377	33.4575
1024×1024	$N_{0.05}^{*}\geq 99.5994$				$U_{0.05}^{*-}=33.4183$, $U_{0.05}^{*+}=33.5088$			
5.3.01	99.6094	99.6132	99.6169	99.6100	33.4741	33.4973	33.4698	33.4516
5.3.02	99.6088	99.6107	99.6010	**99.5964**	33.4767	33.5109	33.4820	33.4579
Pass rate	24/24	22/24	22/24	23/24	24/24	21/24	22/24	23/24

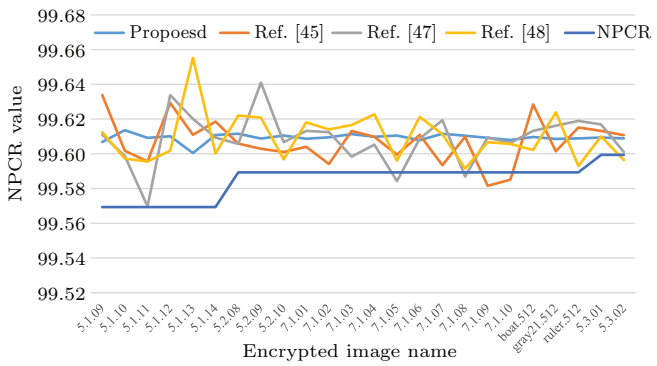


Fig. 12. NPCR test results.

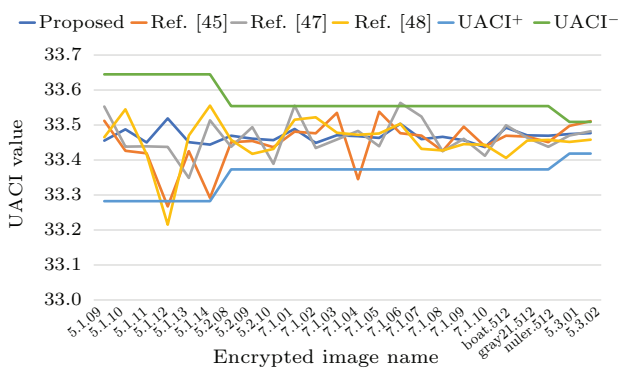


Fig. 13. UACI test results.

5.6. Resistance to noise attacks and cropping attacks

When the data we send includes digital images, the attacker can directly attack the encrypted image to compromise the data's integrity, obstructing the receiver's decryption process and preventing the acquisition of accurate decryption information. Through experiments, we simulate various degrees of noise, cropping, and loss attacks, and by decrypting the images that have undergone the attacks, we can obtain images with recognizable information.[49,50] The decryption results through various levels of clipping and noise attacks are shown in Figs. 14 and 15, demonstrating how well the algorithm can resist these attacks.

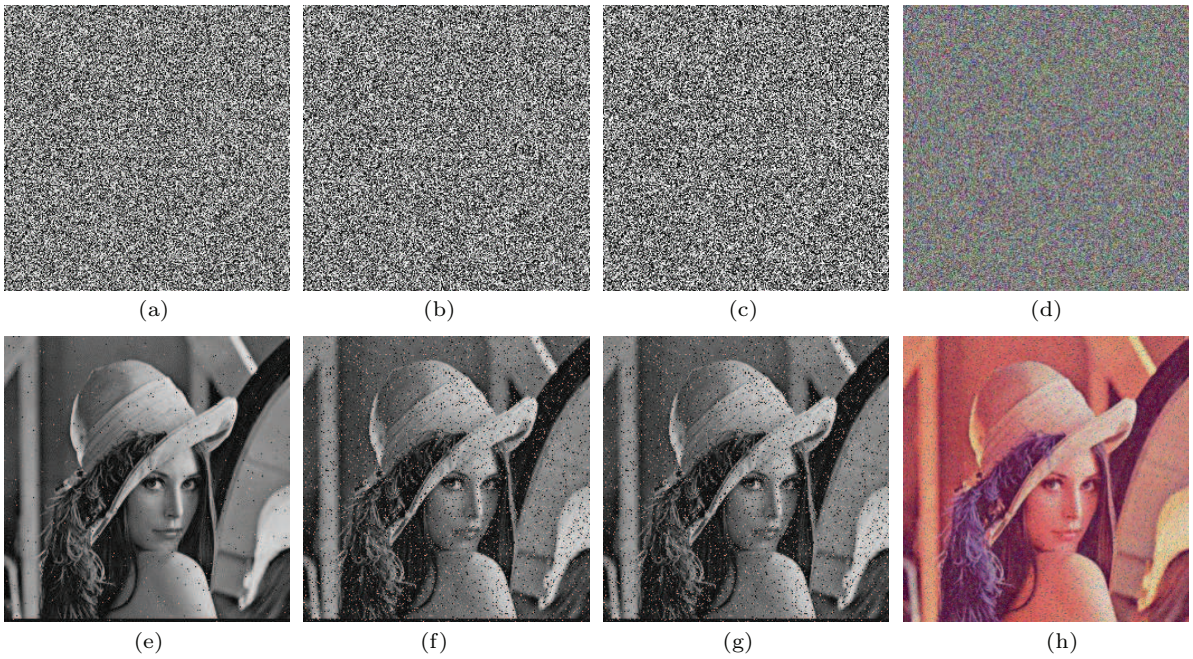


Fig. 14. Noise experiment. (a) Noise intensity 0.01, (b) noise intensity 0.05, (c) noise intensity 0.1, (d) noise intensity 0.05, (e) 0.01 noise picture decryption, (f) 0.05 noise picture decryption, (g) 0.1 noise picture decryption, (h) 0.01 noise picture decryption.

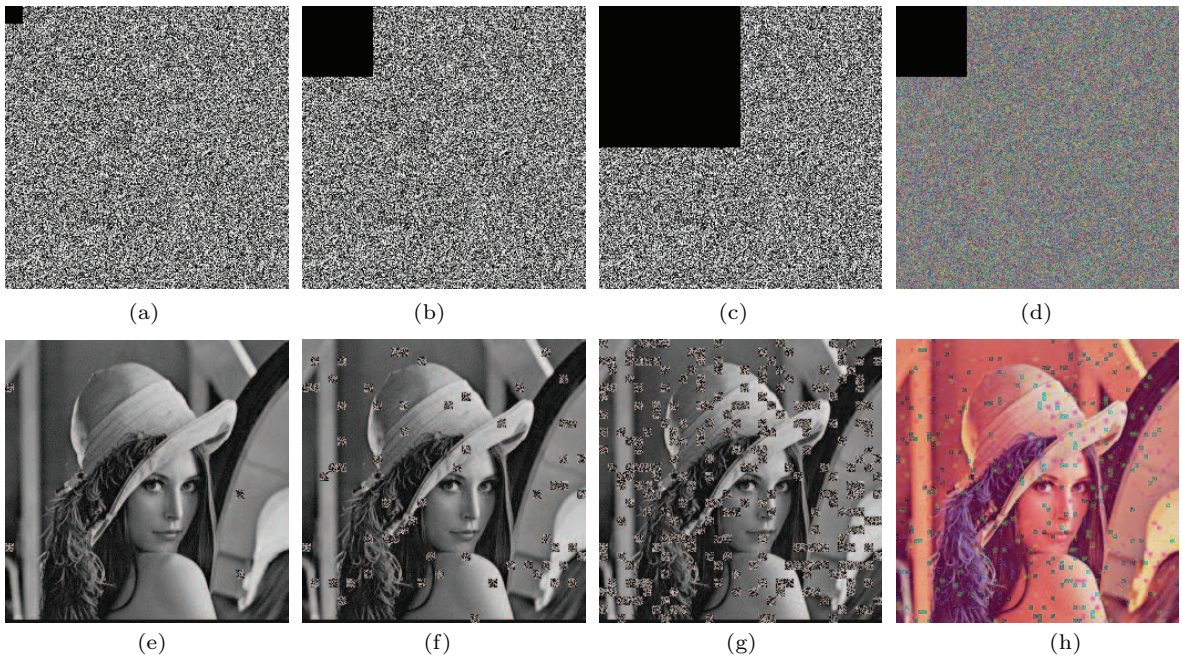


Fig. 15. Cropping attack experiment: (a) 1.526%, (b) 6.25%, (c) 25%, (d) 25%, (e) 1.526%, clipping decryption (f) 6.25% clipping decryption, (g) 25% clipping decryption, (h) 25% clipping decryption.

6. Conclusion

This paper proposes a novel cosine-based chaotic one-dimensional mapping. The chaotic map can meet the requirements of cryptography because of its highly chaotic behavior, wide range of control parameters, and numerous fixed points. In light of the issues in the field of image encryption, we propose a new image encryption scheme based on one-dimensional cosine chaos mapping and doppler wave to

synchronous operation of diffusion of image, which improves encryption efficiency and reduces system complexity, and the associated with the same type of algorithm is not found. The plan put forth in this paper is more efficient at encrypting data. The scheme proposed in this paper has better security and can withstand common attacks, which has some industrial value and significance, according to simulation experiments, data analysis, and comparison.

Acknowledgements

This project was supported by the National Natural Science Foundation of China (Grant No. 61672124), the Password Theory Project of the 13th Five-Year Plan National Cryptography Development Fund (Grant No. MMJJ20170203), the Liaoning Provincial Science and Technology Innovation Leading Talents Program (Grant No. XLYC1802013), the Key R&D Project of Liaoning Province (Grant No. 2019020105-JH2/103), Jinan City '20 Universities' Funding Projects Introducing Innovation Team Program (Grant No. 2019GXRC031), Research Fund of Guangxi Key Lab of Multi-source Information Mining & Security (Grant No. MIMS20-M-02).

References

[1] Wang X Y and Liu P B 2022 *IEEE Trans. Circuit. Syst.* **69** 1291
[2] Xian Y J, Wang X Y, Teng L, *et al.* 2021 *IEEE Transactions on Circuits and Systems for Video Technology* **32** 4028
[3] Rivest R L, Shamir A and Adleman L 1978 *Commun. ACM* **21** 120
[4] Wang X Y, Feng L and Zhao H Y 2019 *Inf. Sci.* **486** 340
[5] Artiles J A P and Chaves D P B 2019 *Signal Processing-Image Commun.* **79** 24
[6] ElAssad S and Farajallah M 2016 *Signal Processing-Image Commun.* **41** 144
[7] Li Y P, Wang C H and Chen H 2017 *Optics and Lasers in Engineering* **90** 238
[8] Chen J X, Zhu Z L, Zhang L B, *et al.* 2018 *Signal Process.* **142** 340
[9] Fu X Q, Liu B C, Xie Y Y, *et al.* 2018 *IEEE Photon. J.* **10** 3900515
[10] Wang X Y and Gao S 2020 *Inf. Sci.* **539** 195
[11] Wang X, Zhou G, Dai C, *et al.* 2017 *IEEE Photon. J.* **9** 7801908
[12] Wang M Y, Wang X Y, Zhao T Y, *et al.* 2021 *Inf. Sci.* **544** 1
[13] Wang X Y and Gao S 2020 *Inf. Sci.* **507** 16
[14] Zhou N R, Hua T X, Gong L H, *et al.* 2015 *Quantum Inf. Process.* **14** 1193
[15] Yang Y G, Tian J, Lei H, *et al.* 2016 *Inf. Sci.* **345** 257
[16] Wang C, Wang H X and Ji Y F 2018 *Opt. Commun.* **407** 1
[17] Yang Z, Guo X, Chen Z, *et al.* 2019 *IEEE Trans. Inf. Forensics and Security* **14** 1280
[18] Zhou R G, Luo J, Liu X A, *et al.* 2018 *Int. J. Theoret. Phys.* **57** 1848
[19] Ding H, Zhen L I, Yang Y, *et al.* 2018 *Chin. J. Electron.* **27** 150
[20] Liu Z L and Pun C M 2018 *Inf. Sci.* **433** 188
[21] Xu J, Mao X, Jin X, *et al.* 2015 *Visual Computer* **31** 1653
[22] Cao L J, Men C G and Ji R R 2013 *Visual Computer* **29** 231
[23] Liu S T and Zhang L 2021 *Surface Chaos and Its Applications* (Singapore: Springer) pp. 30–32
[24] Ernawan F and Kabir M N 2020 *Visual Computer* **36** 19
[25] Huang L, Cai S, Xiao M, *et al.* 2018 *Entropy* **20** 535
[26] Kaur M and Kumar V 2018 *Mod. Phys. Lett. B* **32** 1850115
[27] Muhammad K, Hamza R, Ahmad J, *et al.* 2018 *IEEE Trans. Industrial Informat.* **14** 3679
[28] Seyedzadeh S M and Mirzakuchaki S 2012 *Signal Process.* **92** 1202
[29] Vaidyanathan S, Akgul A, Kaçar S, *et al.* 2018 *Eur. Phys. J. Plus* **133** 46
[30] Liu S T and Wang P 2018 *Fractal Control Theory* (Singapore: Springer Nature) pp. 97–111
[31] Liu S T, Zhang Y P and Liu C A 2020 *Fractal Control and Its Applications* (Switzerland: Springer Nature) pp. 61–80
[32] Liu S T, Wang Y P, Bi Z M and Wang Y 2021 *Mathematical Principle and Fractal Analysis of Mesoscale Eddy* (Singapore: Springer) pp. 121–125
[33] Hua Z and Zhou Y 2019 *IEEE Trans. Systems, Man, Cybernetics: Systems* **51** 3713
[34] Hua Z, Zhou Y and Bao B 2019 *IEEE Trans. Industrial Inform.* **16** 887
[35] Boriga R, Dascalescu A C and Diaconu A V 2014 *Adv. Multimedia* **2014** 409586
[36] Hua Z, Zhang Y and Zhou Y 2020 *IEEE Trans. Signal Process.* **68** 1937
[37] Hua Z and Zhou Y 2016 *Inf. Sci.* **339** 237
[38] Wang X, Qin X and Liu C 2019 *Multimedia Tools Appl.* **78** 6191
[39] Zhou S, Wang X, Wang Z, *et al.* 2019 *Chaos* **29** 033125
[40] Abd El-Latif A A, Wang N, Han Q, *et al.* 2013 *Signal Process.* **93** 2986
[41] Rakheja P, Vig R and Singh P 2019 *Optik* **198** 163289
[42] Chai X, Fu X, Gan Z, *et al.* 2019 *Signal Process.* **155** 44
[43] Wu J, Liao X and Yang B 2017 *Signal Process.* **141** 109
[44] Hua Z Y, Zhou Y, Pun C M, *et al.* 2015 *Inf. Sci.* **297** 80
[45] Wang X, Wang Q and Zhang Y 2015 *Nonlinear Dyn.* **79** 1141
[46] Alawida M, Samsudin A, Teh J S, *et al.* 2019 *Signal Process.* **160** 45
[47] Xian Y J and Wang X Y 2021 *Inf. Sci.* **547** 1154
[48] Liu W H, Sun K H and Zhu C X 2016 *Opt. Lasers Eng.* **84** 26
[49] Zhou Y, Bao L and Chen C L P 2013 *Signal Process.* **93** 3039
[50] Wu Y, Zhou Y, Noonan J P, *et al.* 2014 *Inf. Sci.* **264** 317