IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 22 August 2023, accepted 29 August 2023, date of publication 1 September 2023, date of current version 7 September 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3311038

RESEARCH ARTICLE

Image Encryption Based on Hyperchaotic System and Improved Zigzag Diffusion Method

DONGYAO ZOU, TENGDA PEI, GUANGYONG XI, AND LIPING WANG
School of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou 450000, China
Corresponding author: Dongyao Zou (zdy@zzuli.edu.cn)

ABSTRACT Classical two-dimensional chaotic systems are not safe enough due to few control parameters and limited chaotic range. To cope with this problem, a new wide-range 2D-Logistic-Sine hyperchaotic map (2D-LSHM) is proposed in this paper. By analyzing the bifurcation map and Lyapunov exponent of 2D-LSHM, the results prove that the map has good ergodicity and unpredictability. In addition, this paper proposes a 2D-LSHM-based image encryption scheme, LSHM-IES, to solve the problem that the dislocation diffusion algorithm based on specific rules is vulnerable to attacks. The scheme uses a 3×3 convolutional kernel to replace the pixel values in the dislocation process. An improved Zigzag transform is developed in the diffusion phase to make the algorithm more secure and the key space larger. Experimental results from a variety of performance tests on different images indicate that the LSHM-IES encryption scheme possesses favorable encryption performance, low time cost, and high robustness against data missing attacks and noise effects.

INDEX TERMS Chaotic systems, image security, image encryption, security evaluation.

I. INTRODUCTION

As data exchange on open networks and the Internet continues to rise, the boundaries between the physical and virtual worlds are increasingly blurred, and safeguarding data has become a crucial issue. Images are commonly utilized in diverse domains for their visual representation. However, images in the context of Internet of Things and mobile devices may encompass substantial personal information. Especially, the 5G era is expected to boost the use of images, making it even more crucial to ensure their secure storage and transmission. The main drawbacks of traditional image encryption techniques are slow encryption speed and low security [1]. For example, for larger images, DES encryption can take minutes or even hours. AES algorithm encryption is several times faster than DES, but it still cannot meet the current demand and is difficult to cope with today's computer attacks in terms of security [2]. To solve the problem, researchers are constantly exploring new encryption algorithms and techniques, including chaos theory, deep learning based and quantum techniques [3], [4], [5], which have been introduced into encryption schemes. Chaotic systems exhibit random behavior and unpredictable trajectories in nonlinear systems, and are sensitive to initial values and control parameters, which makes their trajectories difficult to replicate. As such, they offer a fresh perspective for the design of cryptosystems, and have therefore become an important aspect of modern cryptography [6], [7], [8].

The chaotic image encryption algorithm leverages the sequence produced by chaotic systems to modify the image, creating a visual discrepancy between the original and modified versions, thereby achieving image encryption [9]. In practice, the effectiveness of image encryption techniques relies heavily on the performance of chaotic maps, as per the chaos theory. Chaotic maps can be categorized as one-dimensional (1D) or multidimensional (MD) [10]. 1D chaotic maps possess a simple structure and minimal parameters, which can make their chaotic behavior predictable in certain scenarios. In contrast, MD chaotic maps exhibit complex structures and numerous parameters, making it challenging to predict their chaotic trajectories. While MD chaotic map offers superior characteristics, it can be impractical and costly to implement in real-world scenarios. As such, two-dimensional (2D) chaotic map has emerged as a more

The associate editor coordinating the review of this manuscript and approving it for publication was Walid Al-Hussaibi.

viable option, given its favorable features and implementation cost [11], [12].

In this work, an enhanced two-dimensional logical hyperchaotic map is designed and an LSHM-IES encryption scheme is developed based on it. The main contributions are the following three:

- An enhanced two-dimensional logistic hyperchaotic map is proposed. Compared with the 1D chaotic map, it can demonstrate more complex dynamical behavior, generate more random and complex chaotic sequences, easier to regulate and control and handle larger amounts of data.
- An encryption scheme LSHM-IES is proposed based on 2D-LSHM chaotic system. 2D-LSHM generates chaotic sequence based on the key, uses convolution kernel to convolve with the chaotic sequence to disrupt the pixel values in the permutation stage, and uses a modified Zigzag transform to diffuse the image pixels.
- According to the evaluation of LSHM-IES, the proposed encryption scheme demonstrates improved performance and practicality.

Specifically, the work of this paper is organized as follows: Section I introduces the background related to the research of chaotic image encryption. Section II presents the current state of research related to chaotic image encryption systems. Section III introduces the new chaotic map model 2D-LSHM proposed in this paper. section IV presents the algorithms of the dislocation and diffusion phases of LSHM-IES; section V simulates and compares LSHM-IES; section VI summarizes the research of this paper and briefly explains the next work schedule.

II. RELATED STUDIES

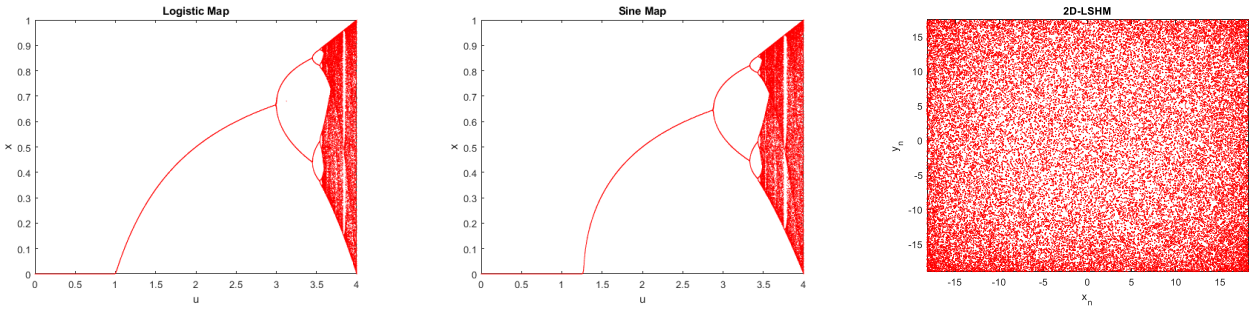
The chaotic map used by Fridrich is a two-dimensional logistic map that maps two-dimensional coordinates to new coordinates. The logistic map is iterated many times to generate a series of pseudo-random numbers that are used as keys for the encryption process. This has sparked the development of numerous image encryption methods grounded in chaos theory by other scholars [13]. For instance, Man et al. [14] employed a five-dimensional hyperchaotic system to generate chaotic sequences as weights for convolutional neural networks, successfully scrambling plaintext image pixels and effectively thwarting plaintext attacks. This approach yielded dynamic adaptive capability and high security. The study by Muthu and Murali [15] combines a one-dimensional chaotic map system with a shuffling algorithm that divides the plaintext image into multiple blocks and performs mismatch operations using the shuffling algorithm, and finally performs heteroscedastic operations in the diffusion phase. Although this scheme is faster in encryption, the diffusion performance is poor, resulting in lower security. On the other hand, Orhan [16] proposed an encryption algorithm based on Fibonacci polynomials and matrices, which increases the randomness and unpredictability of the encryption algorithm through mathematical operations such as modulo and shift operations, but the high computational complexity and storage space requirements lead to inefficient encryption. Hua [17] et al. proposed a method to design S-boxes using a complete Latin square, which can improve the security of cryptographic algorithms without increasing the complexity too much.

Lai et al. proposed two important schemes: a novel Hopfield neural network structure [18] for real-time encryption applications with high encryption strength and attack resistance while realizing fast encryption and decryption operations, and a cross-channel two-dimensional hyperchaotic map-based algorithm [19] with high security and efficiency against illegal attacks. In addition, they proposed a pixel segmentation image encryption scheme based on 2D Salomon map [20], which generates the key by segmenting the image and Salomon map, which is further enhanced in security. They also extended the dynamic properties and applications of neural networks by adjusting the parameters and introducing memory resistive elements to generate and control attractors with complex dynamical behavior [21]. Meanwhile Qian et al. [22] improved on this by introducing bidirectional bit-level cyclic shifting and dynamic DNA level diffusion techniques to enhance the obfuscation and diffusion of encryption. Wei et al. proposed various image encryption algorithms. First, they designed an algorithm based on image filtering and discrete logarithmic transformation [23] by reducing redundant information and increasing image complexity, and then utilized scrambling code perturbation technique and keystream generator for encryption and decryption. Secondly, they improved the scheme based on disambiguation perturbation technique [24] to enhance the obfuscation and diffusion of encryption and improve the encryption strength. For the pixel-level filtering and DNA diffusion problem with low encryption strength, they also proposed an improved scheme based on cyclic replacement and nonlinear replacement [25] to enhance the obfuscation and diffusion of encryption and improve the encryption strength. In addition, they utilized two different chaotic maps to enhance the security of image data [26].

As information technology continues to evolve, the issue of image security becomes increasingly important. Various attacks and jamming methods continue to emerge to assess the confidentiality of algorithms. These methods include [27], [28], and [29]. While encryption algorithm design has made some headway, certain algorithms remain vulnerable to deciphering techniques that have evolved [30], [31]. Thus, the quest to discover more secure and efficient encryption schemes must persist.

III. 2D-LOGISTIC-SINE CHAOTIC MAP

This section introduces the classical one-dimensional logistic map and Sine map, and then leads to the 2D-LSHM chaotic map proposed in this paper.



(a) (b) (c)

FIGURE 1. Bifurcation diagram:(a) Logistic map;(b) Sine map;(c)2D-LSHM map.

A. CLASSICAL CHAOTIC MAPS

A common drawback of many one-dimensional chaotic maps is their limited chaotic range and weak output sequence randomness, often due to their restricted control parameters. To address this issue, multiple chaotic maps can be combined. The 2D logistic-Sine hyperchaotic map (2D-LSHM) introduces cosine variations and offers an improved solution. The logistic map is a classic and extensively researched example of one-dimensional chaotic map, known for its intricate nonlinear behavior and defined by Eq. (1).

$$x_{n+1} = \mu x_n(1 - x_n) \tag{1}$$

The sine map is also a high-quality random sequence generator, which is widely used in chaotic encryption and pseudo-random number generation, and the mathematical expression is Eq. (2).

$$x_{n+1} = \delta \sin(\pi x_n)/4 \tag{2}$$

Fig.1(a) shows the bifurcation of the Logistic map, while Fig.1(b) displays that of the Sine map. Due to the small chaotic ranges and multiple period windows, the Logistic and Sine maps exhibit discontinuous chaotic ranges. The cosine transform is a nonlinear map function that maps the input values to the range $[-1,1]$, and it can be used in chaotic maps, chaotic encryption, and pseudo-random number generation to produce more complex dynamical behavior and higher quality random sequences. Thus, to address this issue, we propose 2D-LSHM, which involves applying cosine variation to the logistic and sine maps using Eq. (3).

$$\begin{cases} x_{n+1} = k_1[1 + \alpha \cos(\pi x_n)^{\beta}] \bmod 1 \\ y_{n+1} = k_2 \cos(y_n(1 - x_n)) \end{cases} \tag{3}$$

where the control parameters $\alpha = 3, \beta = 5, k_1 = 20, k_2 = 20$. From Fig. 1(c), respectively, 2D-LSHM can produce chaotic states over a fairly wide range, which means it has a high flexibility and adjustability to adjust the parameters as needed to achieve better encryption.

B. PERFORMANCE EVALUATION OF 2D-LSHM

The attractor of a chaotic map is a set of values, and they are important factors to guide the system into the chaotic state. The attractor is a stable state to which the chaotic map converges after continuous evolution, and it has a highly complex structure and unpredictable trajectory.

Specifically, the better the chaotic performance of a chaotic map, the more complex and higher the fractal dimension of its attractor is usually, and the larger the region in the phase space it occupies. This is because the chaotic performance of a chaotic map requires its iterative sequence to cover as many states as possible in the phase space in order to exhibit randomness and unpredictability. In this paper, we choose two existing chaotic maps, 2D-TM and 2D-ICM, for comparative analysis. Firstly, the initial conditions are set and a point (0.6, 0.8) is chosen randomly, secondly, 20,000 iterations are computed, and by tracking the iterative trajectories of the chaotic maps, the trajectory images of the attractors can be drawn.

In Figure 2, the attractor trajectories of the 2D- LSHM are compared with those of the two 2D chaos maps.

According to Fig. 2(c), it can be seen that the attractors of 2D-LSHM completely occupy a two-dimensional phase space in the range of (-20,20), which means that the attractors of 2D-LSHM form a highly complex geometric structure. And it has better ergodicity than 2D-ICM (2D infinite collapse map) [32] and 2D-TM (triangular map) [33].

Chaotic systems exhibit a crucial feature called sensitivity to initial conditions, which can be analyzed by studying the growth or decay rate of small perturbations over time in a dynamical system using the Lyapunov exponent (LE). In chaotic systems, the Lyapunov exponent (LE) measures both the stability and degree of chaos in a system. A larger LE exponent indicates greater unpredictability and sensitivity to initial conditions, which leads to more erratic behavior within the system. A positive value of the Lyapunov exponent (LE) indicates chaos in a dynamical system, with the distance between phase trajectories increasing over time. Hyperchaotic systems are different from chaotic systems in that their Lyapunov exponent is an infinite function, indicating an even greater sensitivity to initial conditions. The phase space structure of hyperchaotic systems is also more complex. Hyperchaotic phenomena occur in many natural and technological systems, for example, in the fields of weather

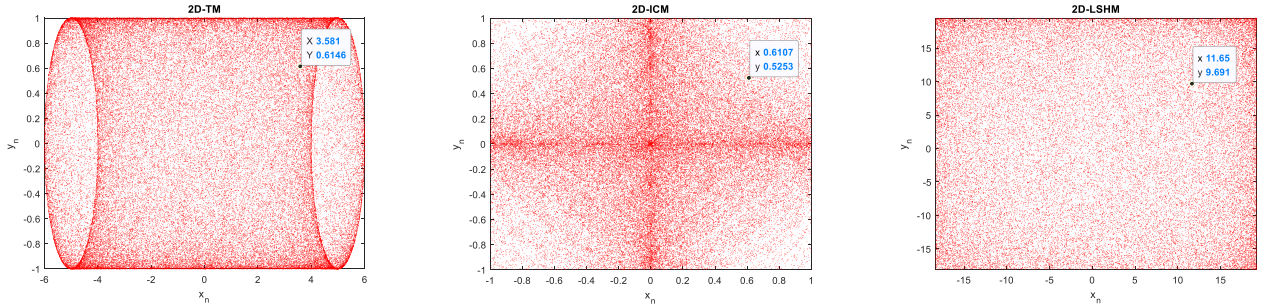


FIGURE 2. Attractors of different 2D chaotic maps:(a) 2D-TM; (b) 2D-ICM; (c) 2D-LSHM.

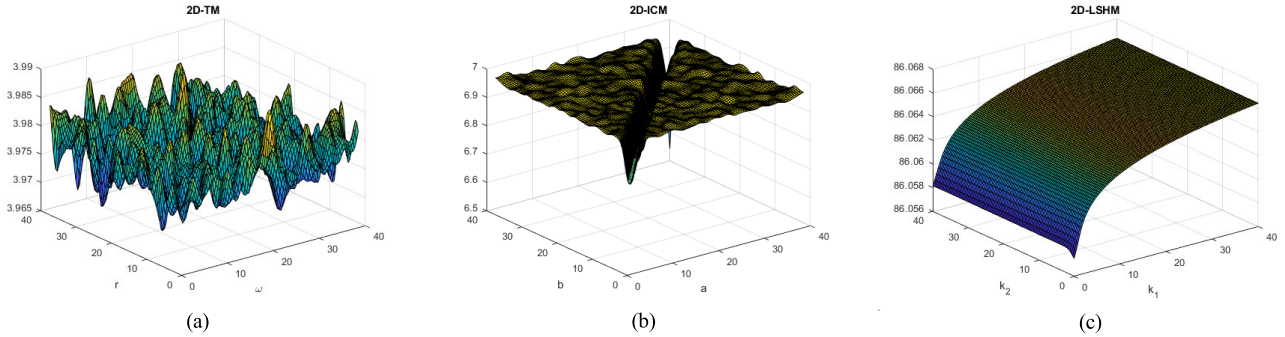


FIGURE 3. LE Index Comparison:(a) 2D-TM; (b) 2D-ICM; (c) 2D-LSHM.

forecasting, biological systems, and communications. Let the chaotic system be. The LE index is calculated by Eq. (4) [34] Fig. 3 compares the 2D- LSHM proposed in this study with two other 2D chaotic maps: 2D-TM and 2D-ICM. As shown in the figure, the Lyapunov exponent of our proposed 2D chaotic map is larger, which means that its dynamical behavior is more chaotic and unpredictable. Moreover, the relative trend is smoother and more stable in the graph, which also indicates that the nature of this chaotic system is better than the existing 2D chaotic graphs.

$$LE = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln \left| f'(x_i) \right| \tag{4}$$

Our proposed 2D-LSHM graph possesses several advantages based on the above metrics. First, it shows a continuous hyperchaotic range, which is crucial in cryptographic applications because it avoids falling into the cycle range that could lead to dynamical disruptions and serious security problems. In addition, LSHM has almost no cycle range, which further improves its performance. Second, LSHM has a maximum Lyapunov exponent of up to 80, which is highly random and facilitates message encryption. Finally, the structure of LSHM is scalable, and we can derive completely novel two-dimensional hyperchaotic maps by replacing one-dimensional maps.

C. NIST SP800-22 TEST

The security of stream cipher is closely related to the randomness of the generated sequence. Therefore, when designing stream ciphers, pseudo-random sequence generation algorithms with good statistical properties need to be selected to ensure that the generated key streams are sufficiently random and unpredictable. Currently, the linear congruence generator is one of the most commonly used pseudo-random number generators. It can be described as

$$X_{n+1} = (aX_n + c) \bmod m \tag{5}$$

where m is the modulus, a is the multiplier, and c is the increment. Both the linear congruence generator as well as the 2D-LSHM are capable of generating pseudo-random sequences in floating-point form. After amplitude expansion, rounding, and modulation, these generated pseudo-random sequences are quantized to values in the range (0, 1).

The NIST SP800-22 test suite is a widely adopted industry standard and contains 15 different test items. According to the official documentation, if the P-VALUE of a test result is greater than 0.01, the test has been successfully passed. Meanwhile, the larger the value of P-VALUE, the better the test result is. We conducted the NIST SP800-22 test on the above pseudo-random sequences, and the test results are shown in Table 2. As shown in Table 2, both pseudo-random sequences successfully passed all 15 test items. It is worth noting that the P-VALUE of the 2D-LSHM pseudorandom sequence is larger than that of the linear congruence pseudorandom sequence in all 10 tests. This indicates that the pseudo-random sequence generated by 2D-LSHM has better randomness.

TABLE 1. The comparison between the proposed 2D-LSHM and existing 2D chaotic maps.

Name	Chaotic maps	Parameters	Attractors
2D-TM	$\begin{cases} x_{n+1} = \sin(\omega x_n) - r\sin(\omega y_n) \\ y_{n+1} = \cos(\omega x_n) \end{cases}$	$\omega = 100\pi$; $r = 5$.	Fig.2(a)
2D-ICM	$\begin{cases} x_{n+1} = \sin(\frac{a}{y_n}) \cdot \sin(\frac{b}{x_n}) \\ y_{n+1} = \sin(\frac{a}{x_n}) \cdot \sin(\frac{b}{y_n}) \end{cases}$	$a = 10$; $b = 21$.	Fig.2(b)
2D-LSHM	$\begin{cases} x_{n+1} = k_1[1 + \alpha\cos(\pi x_n)^{\beta}] \bmod 1 \\ y_{n+1} = k_2\cos(y_n(1 - x_n)) \end{cases}$	$\alpha = 3$; $\beta = 5$; $k_1 = 20$; $k_2 = 20$.	Fig.2(c)

TABLE 2. NIST test results of linear congruence and hyperchaotic pseudorandom sequences.

statistical results	linear congruence	pseudorandom sequence	hyperchaotic	pseudorandom sequence
	P-VALUE	PROPORTION	P-VALUE	PROPORTION
Frequency	0.185566	1.00	0.190836	1.00
Block Frequency	0.965295	1.00	0.970673	1.00
Cumulative Sums	0.486646	1.00	0.563382	1.00
Runs	0.147094	1.00	0.162706	1.00
Longest Run	0.351485	0.99	0.437374	0.96
Rank	0.586209	0.99	0.654367	0.99
FFT	0.885137	0.99	0.105518	0.98
Non-Overlapping Template	0.948602	1.00	0.911313	1.00
Overlapping Template	0.074277	1.00	0.242886	1.00
Universal	0.875639	0.98	0.895263	0.99
Approximate Entropy	0.862544	1.00	0.048616	1.00
Random Excursions	0.947657	0.98	0.976684	0.98
Random Excursions Variant	0.934218	1.00	0.865797	1.00
Serial	0.551226	1.00	0.122425	1.00
Linear Complexity	0.195263	0.99	0.232860	0.99

IV. 2D-LSHM BASED IMAGE ENCRYPTION SCHEME

In a typical image, individual pixel values are often strongly correlated, and this correlation may be used by an attacker to break the encryption algorithm or extract the image information. Therefore, a reliable algorithm should be developed that combines chaotic sequences to further ensure security. LSHM-IES, an image encryption scheme depicted in Fig 4, is introduced in this section.

The IES encryption scheme comprises three primary components: key generation, scrambling, and diffusion. The scrambling process of IES involves modifying pixel values primarily through convolution, the diffusion component of the encryption scheme propagates changes made to a few pixels in the plaintext image throughout the entire ciphertext image. IES encryption scheme can efficiently transform a standard image into a chaotic and unidentifiable image in a relatively short duration, resulting in enhanced security and efficiency.

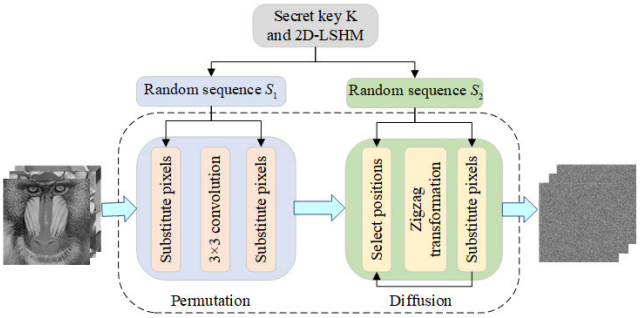


FIGURE 4. The structure of the system for encrypting images.

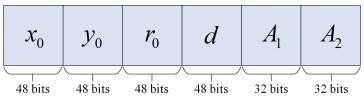


FIGURE 5. Key structure.

A. KEY CREATION

Generating chaotic sequences using 2D-LSHM requires determining an initial value, also referred to as the seed value or key. The generated chaotic sequences are usually highly unpredictable and random, so they can be used to encrypt and decrypt data. To resist brute-force attacks [35] and ensure a balance between encryption efficiency and security, the key space must exceed 2^{100}. In this paper, a 256-bit key is used, Fig.5 depicts the structure of the key, which consists of the original initial value (x_0, y_0) of length 48 bits and the original control parameters r_0, the perturbation coefficients d, and the correlation coefficients A_1 and A_2 of the original initial value. Where the variables (x_0, y_0, r_0) and d are floating point numbers between [0-1) and can be calculated by Eq. (6). The parameters work in tandem to determine the size of the key space and the strength of the encryption algorithm. Among them, (x_0, y_0) and r_0 define the dynamical behavior of the chaotic system, while d perturbs initial values to increase randomness, while A_1 and A_2 are used to control the nature of the chaotic system. By properly selecting and tuning these

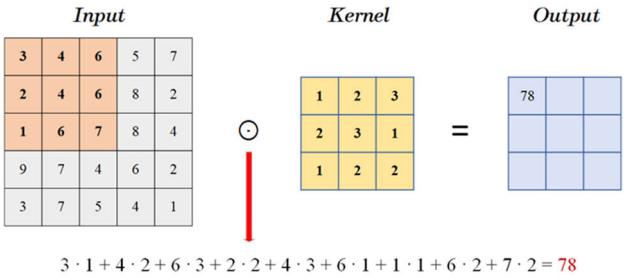


FIGURE 6. How convolution works.

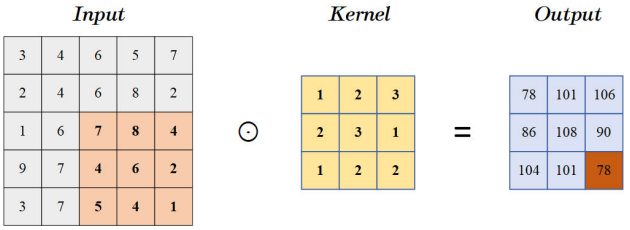


FIGURE 7. Convolutional changes of the dislocation process.

parameters, keys with high randomness and security can be generated.

$$FN = \sum_{i=1}^{48} Bin_i \times 2^{-i} \tag{6}$$

The variables A_1 and A_2 are 32-bit integers and can be calculated by Eq. (7).

$$IN = \sum_{i=1}^{32} Bin_i \times 2^{i-1} \tag{7}$$

Eq. (8) can be used to calculate the seed value for generating the chaotic sequence.

$$\begin{cases} x_0^{(i)} = (x_0 \times A_1 + d) \bmod 1 \\ y_0^{(i)} = (y_0 \times A_2 + d) \bmod 1 \\ r_0^{(i)} = (r_0 \times A_i + d) \bmod 1 \end{cases} \tag{8}$$

where $i = (1, 2)$, using the initial state (x_0, y_0, r_0), 2D-LSHM can generate chaotic sequences for efficient permutation and random number permutation diffusion.

B. DISRUPTION PROCESS

In image processing, convolutional filtering is a common technique used to modify spatial frequency features. Typically, a fixed kernel matrix, either 3 × 3 or 5 × 5 in size, is selected, and the central pixel value is determined by adding the weighted values of its neighboring elements. The weights are calculated by multiplying the neighboring pixel values with the corresponding entries in the kernel matrix, and this process is used to replace the pixel values. In this section, we use 3 × 3 convolution kernels. The use of a 3 × 3 convolution kernel can increase network depth, decrease convolution kernel parameters, increase the number of nonlinear maps, simplify the model, and improve the efficiency of operations. Defining the convolutional operation can be achieved using Eq. (9).

$$\begin{aligned} h(\mathrm{a}, b) &= f(a, b) * g(a, b) \\ &= \sum_{i=-\infty}^{\infty} \sum_{j=-\infty}^{\infty} f(i, j) \cdot g(a - i, b - j) \end{aligned} \tag{9}$$

where h denotes the output, f denotes the input, and g denotes the convolution kernel. Fig.6 shows the working principle of convolution. In this paper, the plaintext index is calculated using a convolution operation. A chaotic sequence, $f(\mathrm{a}, b)$, generated by a chaotic system, and the plaintext pixel value of the pure image, $g(a, b)$, are used as inputs for the convolutional operation, which outputs the dislocated ciphertext image, $h(\mathrm{a}, b)$. The convolution process can effectively destroy the pixel size of the image and reduce the pixel correlation. Fig.7 clearly illustrates the convolutional changes of the dislocation process.

Step 1: The sequence $A = [a_1, a_2, \cdots, a_{m\times n}]$ of length $m \times n$ is generated by putting the image $R_{m\times n}$ in the order of first and then the column. The chaotic sequence is generated by substituting the original initial values, x_0 and y_0, into the chaotic system for $m \times n + 1000$ iterations. To remove any transient effects, the first 1000 terms are discarded to obtain the chaotic sequence $B = [b_1, b_2, \cdots, b_{m\times n}]$. The elements of B in the sequence correspond to the elements of A one by one.

Step 2: Converting the sequences A and B into two-dimensional matrices produces A_1 and B_1, both of size $m \times n$,where the elements of B_1 correspond one-to-one with those in A_1. Through the convolution process, the matrix B_1 composed of chaotic sequences is convolved with the corresponding part of the 3 × 3 convolution kernel matrix A_1 to obtain the convolution result, and it is composed of the matrix $C(m \times n)$. The matrix C is the image after pixel size dislocation, and the encryption processing of the image is realized.

C. IMPROVED ZIGZAG DIFFUSION

The Zigzag transform is a process of scanning and storing two-dimensional matrix elements in a "Z" shape into a one-dimensional array. A specific rearrangement method [36] can convert the 1D array into a 2D matrix. The Zigzag transform is a useful tool for aligning image pixels in encryption. The process of the Zigzag transform, which rearranges pixels in a "Z" shape into a 2D matrix based on specific requirements, is illustrated in Fig.8. The pixel traversal order may begin from other corners of the image, resulting in eight Zigzag fold transform patterns, as depicted in Fig.9, which scan either horizontally or vertically from the four corners. Enhancing randomness can be achieved by shifting the one-dimensional array and arranging the scan order array in a ring. The Zigzag arrangement offers the advantages of simplicity and speed while enabling each pixel to be traversed for rearrangement.

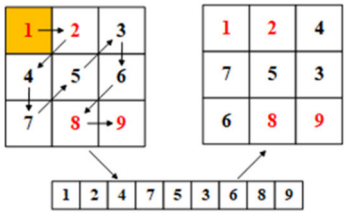


FIGURE 8. Zigzag folding line change.

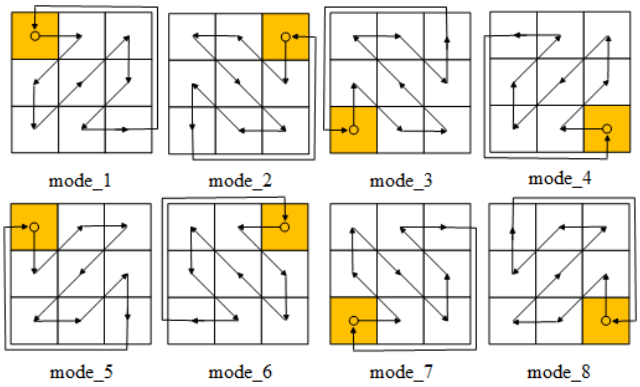


FIGURE 9. Eight modes of Zigzag transformation.

Similarly, Zigzag diffusion can create a butterfly effect by altering only a few pixels, resulting in the modification of the entire encrypted image.

The eight Zigzag fold patterns discussed above begin from the four corners of the image and utilize both vertical and horizontal patterns, resulting in a total of eight patterns. Nonetheless, this approach has a drawback: it only utilizes one round of Zigzag transformations for diffusion, and the key space of the encryption scheme is not sufficiently large to withstand brute force attacks. Effectively breaking down the high correlation between adjacent elements is also a challenge for the encryption scheme.

The eight Zigzag fold patterns discussed above begin from the four corners of the image and utilize both vertical and horizontal patterns, resulting in a total of eight patterns. Nonetheless, this approach has a drawback: it only utilizes one round of Zigzag transformations for diffusion, and the key space of the encryption scheme is not sufficiently large to withstand brute force attacks. Effectively breaking down the high correlation between adjacent elements is also a challenge for the encryption scheme.

Introducing a modified Zigzag fold transform allows us to tackle these challenges and obtain more randomized outcomes. In contrast to the existing Zigzag variation, which arranges each pixel in a fixed order based on its Zigzag on the new coordinates, the modified Zigzag transform determines the transformation pattern based on the initial coordinates determined by the chaotic sequence. After a single round of alterations, the next initial point and transformation mode are determined using the chaotic sequence. The cycle involves three rounds of transformations since the position of the initial coordinates is random in each round, and each change has eight modes. Thus, the overall change employs a power-increasing mode, resulting in an extensive key space. The enhanced Zigzag transform is governed by a parameter that alters only the pixel positions, considerably enhancing the transform's efficiency and security level. The chaotic system used in this approach is the enhanced two-dimensional logistic chaotic map introduced in the preceding section.

TABLE 3. Scan map.

p	q	
	1	2
1	mode_1	mode_5
2	mode_2	mode_6
3	mode_3	mode_7
4	mode_4	mode_8

We divide the modified Zigzag transform into five steps to operate on a matrix D of size $m \times n$:

Step 1: Eq. (8) is used to generate four chaotic sequences with a length of L, and each chaotic sequence is sorted to obtain the corresponding index vector. R_1, R_2, C_1 and C_2 are used as row indexes, and R_1 and R_2 are used as column indexes, which can generate the coordinate matrices C_1 and C_2, respectively, to generate the coordinate matrices O_1 and O_2.

Step 2: Set $q(i) = (R_i(1) \bmod 2) + 1$, $p(i) = (C_i(1) \bmod 4)+1$, $x(1) = R_1(2)$, $y(1) = C_1(N)$, $x(2) = R_2(2)$, $y(2) = C_2(N)$, where p is the control parameter, $p \in [1, 2, 3, 4]$. $p(i)$ and $q(i)$ are used to determine the scan selection mode of O_i shown in Fig.10. Determination of the starting point for each scan is based on $x(i)$ and $y(i)$. Correspondence between p, q, and scan mode O_i is illustrated in Table 3.

Step 3: Perform scanning on O_1 and O_2 using the selected scan method from Step 2, as illustrated in Fig.10-(a). Then, record each coordinate on their scan paths into the cache matrices c_1 and c_2.

Step 4: Swap the elements in matrix M with coordinates $c_1(i)$ and $c_2(i)$.

Step 5: Repeat Step 2 and scan Fig.10-(b),10-(c) in turn.

According to the above steps, we provide an original matrix of size 5×5 to demonstrate the process of three scans and further illustrate the revised Zigzag changes, allowing us to understand the details more intuitively. First, according to the coordinate matrix, (a) scan with mode_1, (b) scan with mode_8, and (c) scan with mode_5. After three rounds of scanning, we can get the final coordinate map as (1,1) → (4,1), (1,2) → (3,1), (1,3) → (3,2), (1,4) → (2,3), (1,5) → (4,3), (2,1) → (2,4), (2,2) → (1,5), (2,3) → (1,3), (2,4) → (3,3) and (2,5) → (2,1).

To obtain the final swap matrix W, pixel swapping is performed on the matrix D based on the coordinate map.

In order to test the advantages and disadvantages of the proposed zigzag transform algorithm, as shown in Table 4 we use a 6×6 pixel digital model using correlation analysis and other methods to compare and test the four characteristics

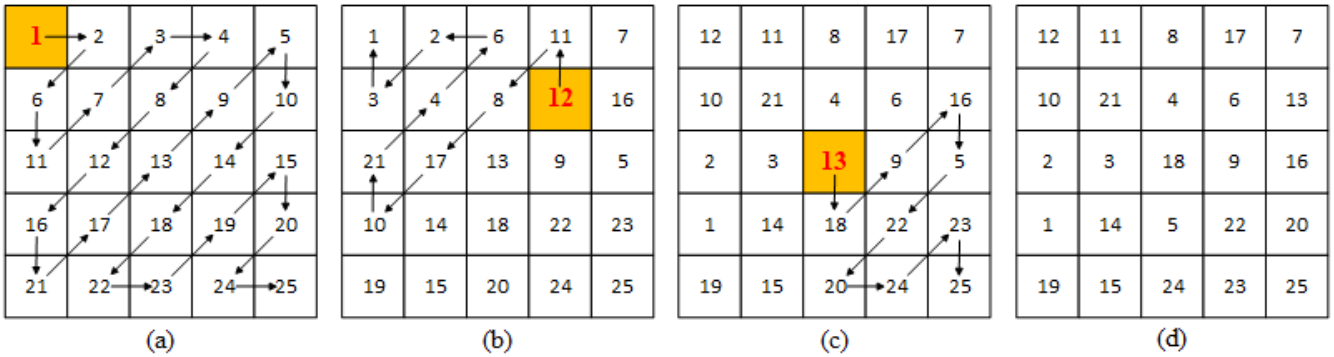


FIGURE 10. Three scans of the diffusion process.

TABLE 4. Comparative analysis of Zigzag diffusion methods.

Zigzag Transformation Method	Ours	Guo.[37]	Zheng.[38]
Diffusion effect	0.9515	0.8132	0.7527
Diffusion efficiency	0.0032s	0.0028s	0.0025s
Diffusion quality	1	1	1
Security	0.9846	0.8527	0.7641

of Guo et al. [37] and Zheng and Lv [38] Zigzag transform methods. From the data in Table 4, it can be obtained that the encryption efficiency and encryption security of the proposed Zigzag algorithm is higher than the other two algorithms.

In comparison to the current Zigzag algorithm for image encryption, this paper presents an improvement in which the scanning method is dynamically selected by altering the initial state of the chaotic system and disrupting the order determined by the previous scan through multiple scans. This enhances the security of diffusion. Additionally, the scanning diffusion process only necessitates four chaotic sequences of length L to determine the initial position and scanning mode. This is more efficient than most diffusion algorithms utilizing chaos encryption that require chaotic sequences of length L × L.

V. SIMULATION AND PERFORMANCE ANALYSIS

A comprehensive analysis of the LSHM-IES encryption scheme's performance is presented in this section, considering several perspectives. To assess the algorithm's effectiveness, speed, and flexibility, various tests are conducted, including pixel distribution, histogram, information entropy, local information entropy, NPCR, UACI, image sensitivity, key sensitivity analysis, and encryption speed [39], [40] and [41]. Moreover, robustness analysis is a critical indicator for evaluating the algorithm's reliability and security, and for determining its ability to withstand various attacks. The combination of these test methods can provide a comprehensive performance evaluation of the LSHM-IES encryption scheme.

A. HISTOGRAM ANALYSIS

In image encryption, the histogram is a crucial tool for evaluating the effectiveness and security of encryption algorithms. It displays the distribution of image brightness or color and can detect whether the distribution of the encrypted image is similar to that of the original image. If the encryption algorithm effectively scrambles and obfuscates the image, the histogram of the encrypted image should differ significantly from that of the original image. Conversely, if the encryption algorithm has vulnerabilities or is insufficiently secure, an attacker can use the histogram of the encrypted image to deduce information about the image or reconstruct the original image. Figs. 12(a)-(f) display the histograms of the Lena, Pepper, and Baboon plaintext images, as well as their corresponding encrypted images.

With the purpose of identifying deviations, the chi-square examination may be employed, in which χ^2 measures the extent of discrepancy between the picture pixel arrangement and the entirely even distribution. Eq. (10) outlines the definition of χ^2.

$$\chi^2 = \sum_{i=0}^{255} \frac{(p_i - \bar{p})}{\bar{p}} \tag{10}$$

where p_i is the frequency of image pixel i. $\bar{p}$ represents the average frequency of all pixels, $\bar{p} = (M \times N)/256$. $M \times N$ denotes the size of the image. As χ^2 decreases, the pixel distribution becomes more uniform in the image, so the closer the image is to a uniform distribution. Table 5 presents the detection outcomes for Lena, Pepper, Baboon, Barbara, Flintstones, black plaintext, and ciphertext images. The value of χ^2 for ciphertexts is considerably lower than that of plaintexts, indicating that the pixel values in each ciphertext image are more uniformly distributed. Cardinality testing results demonstrate the uniform pixel value distribution in ciphertext images, thereby affirming the feasibility and effectiveness of LSHM-IES in safeguarding image privacy information.

B. ADJACENT PIXEL POINT CORRELATION ANALYSIS

To enhance resistance to statistical analysis, a reliable encryption algorithm must effectively minimize the correlation between neighboring pixels in the plaintext image. To evaluate the algorithm's security in this aspect, we conduct tests on the plaintext and ciphertext images in the horizontal, vertical, and diagonal directions, using the calculation method

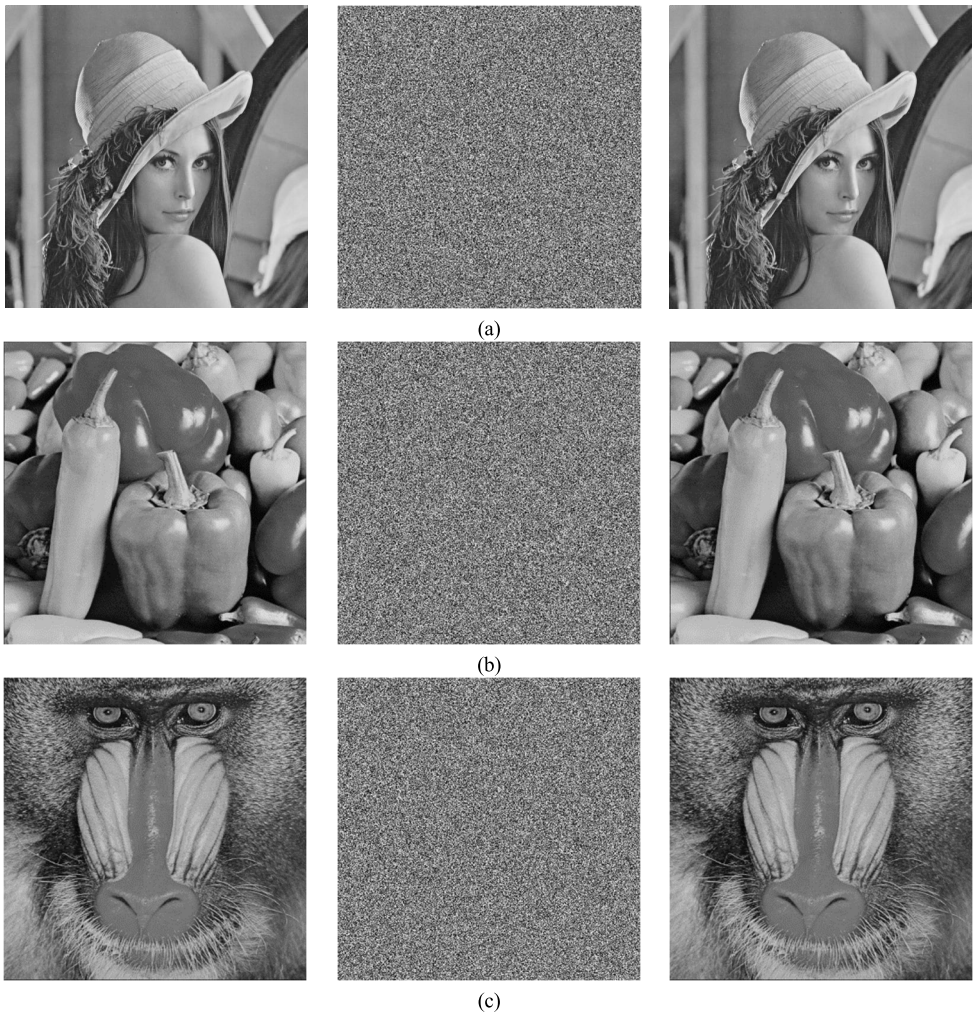


FIGURE 11. Image encryption and decryption. (a) Lena, (b) Peppers, (c) Baboon.

illustrated in Eq. (11). It's important to exclude the first row and column in the calculation.

$$\begin{cases} E(x) = \dfrac{1}{N}\sum_{i=1}^{N} x_i, D(x) = \dfrac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \\ r_{xy} = \dfrac{\mathrm{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \\ \mathrm{cov}(x, y) = E((x - E(x))(y - E(y))) \end{cases} \tag{11}$$

The correlation distribution of adjacent pixels in plaintext and ciphertext images is presented in Fig. 13, indicating that the correlation is more concentrated and stronger in the plaintext image, whereas the distribution is more uniform in the ciphertext image. Table 6 displays the numerical representation of the correlation between adjacent pixels in each direction of the image, revealing that the correlation of the ciphertext image is almost zero. The comparison results are shown in Table. 7, the APC value of the encrypted image is closer to 0 than the original image, but it is in the middle of the range compared to other encryption schemes in this test. These findings demonstrate the effectiveness of the proposed encryption algorithm in resisting statistical analysis, and indicate that the chaotic system employed is well-suited for image encryption. In short, LSHM-IES is able to protect the image security well.

While the pixel distribution of the encrypted image is more uniform. In Fig.12(a), the distribution of pixel values in the plaintext image is more prominent, whereas the distribution of pixels in the encrypted image in Fig.12(b) is more uniform and lacks distinctive features. This uniform pixel distribution helps prevent attacks aimed at obtaining the plaintext information of the image.

Figures that are meant to appear in color, or shades of black/gray. Such figures may include photographs, illustrations, multicolor graphs, and flowcharts.

C. INFORMATION ENTROPY

To evaluate the randomness and uniformity of the pixel value distribution in the encrypted image, we can compute its information entropy. A higher information entropy of pixel values indicates that the encryption algorithm introduces sufficient randomness and noise, thereby enhancing the

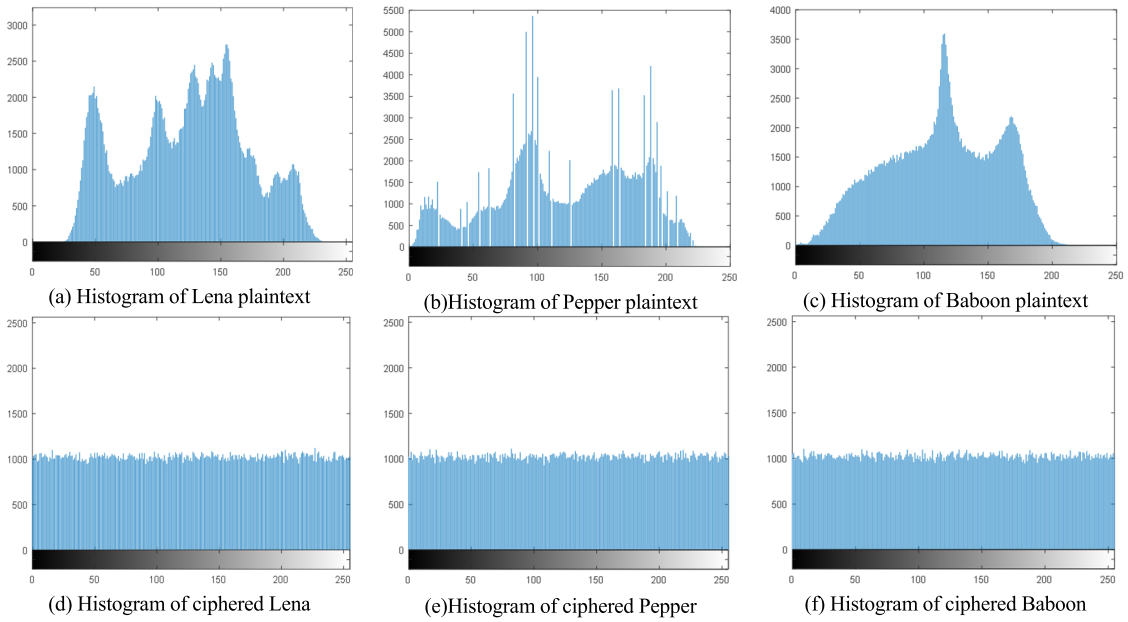


FIGURE 12. Histograms of plaintext and ciphered images.

TABLE 5. χ^2 test results.

Image	Lena	Pepper	Baboon	Barbara	Flintstones	Black
Plaintext	160001	204333	180257	95549	790768	66846720
Ciphered	259.2266	278.0703	261.7754	255.9199	252.0762	251.2148
Change P(1,1)	229.1523	219.6133	252.5820	275.7559	237.7969	272.0430

difficulty of cracking the image and improving the security of the encryption algorithm. The formula for information entropy is provided in Eq. (12).

$$H(S) = \sum_{i=0}^{2^{N-1}} p(s_i) \log_2 \frac{1}{p(s_i)} \tag{12}$$

In Eq. (12), S represents the image, s_i represents the pixel in image S, and $p(s_i)$ represents the probability of occurrence of pixel s_i. The ideal information entropy of a grayscale image is 8, indicating a more uniform pixel distribution as it approaches 8. Table 8 shows that the information entropy of the ciphertext images is close to the ideal value of 7.99, indicating that the encryption effect is satisfactory. This suggests that the encryption algorithm has effectively introduced sufficient randomness and noise to enhance the image security. As shown in Table 9, the $H(S)$ value of the encrypted image is larger in our proposed scheme compared to other encryption schemes, indicating that our scheme is more secure.

D. LOCAL INFORMATION ENTROPY

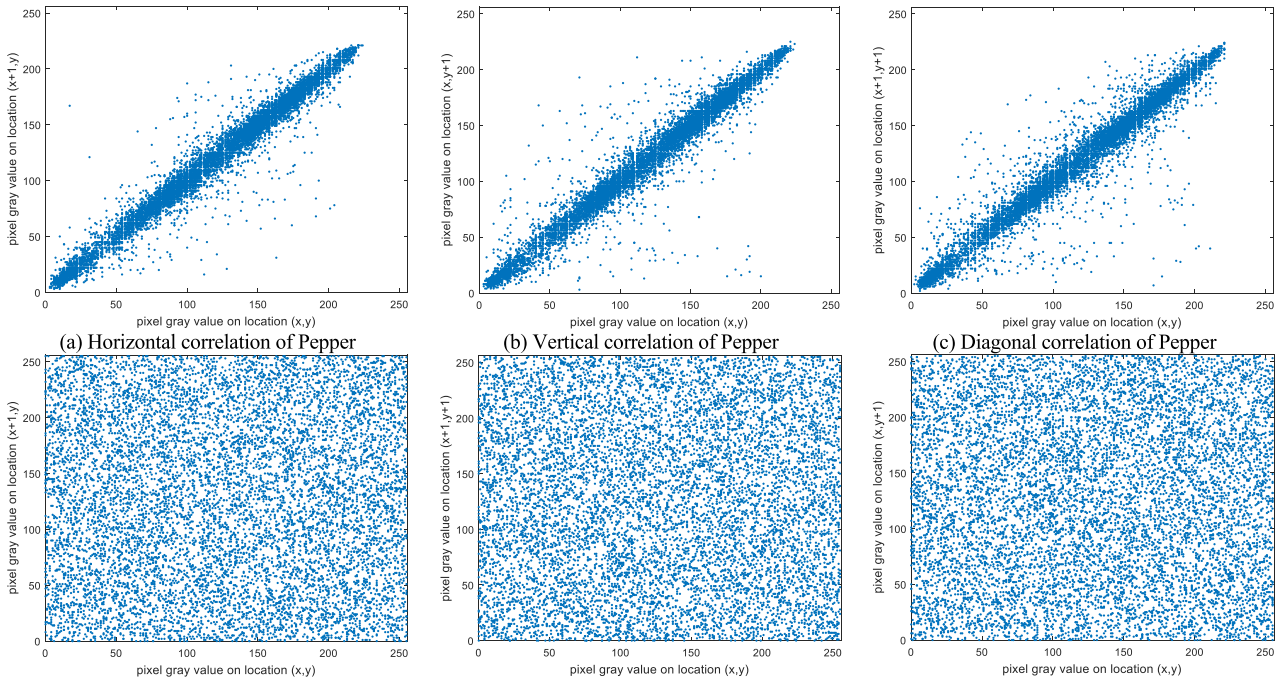
The local information entropy evaluates the distribution state of the local information of the ciphertext image and is defined as Eq. (13).

$$\overline{H_{k,T_B}}(C) = \sum_{i=1}^{k} \frac{H(C_i)}{k} \tag{13}$$

where C represents the ciphertext image, k and T_B represent the random selection k groups of T_B pixels from C. $H(C_i)$ represents the information entropy of C_i composed of T_B pixels. when $k = 30$, $T_B = 1936$ and confidence level $\alpha = 0.001$, the local information entropy of ciphertext image is located at [7.901902305, 7.903036329], then the algorithm passes the test and is secure. Table 10 shows the test results of Lena, Pepper and other cipher images, all the local information entropy values of cipher images are within the required interval, all pass the test, so the encryption scheme proposed in this paper is secure.

E. IMAGE SENSITIVITY ANALYSIS

To measure the sensitivity of the encryption algorithm to slight changes in the plaintext image, we define image sensitivity as the degree of difference in the ciphertext image produced by slightly different plaintext images under the same key encryption. A higher degree of difference indicates higher sensitivity of the image to small changes in the plaintext. To quantify this difference, we use two metrics, NPCR and UACI, which respectively measure the number of adjacent pixel changes and the average intensity of pixel value changes. These metrics assist in evaluating the sensitivity and reliability of the encryption algorithm to image changes and enhancing its security and robustness. The calculation of



(a) Horizontal correlation of Pepper (b) Vertical correlation of Pepper (c) Diagonal correlation of Pepper

(d)Horizontal correlation of ciphered Pepper (e) Vertical correlation of ciphered Pepper (f) Diagonal correlation of ciphered Pepper

FIGURE 13. Correlation coefficients of Pepper.

TABLE 6. Correlation coefficients.

Image	plain image			ciphered image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena	0.9742	0.9872	0.9624	–0.0012	6.1635e-04	8.0547e-05
Pepper	0.9384	0.9723	0.9233	–0.0026	–2.1149e-06	1.5492e-04
Baboon	0.8628	0.7532	0.7238	0.0025	–0.0033	–9.8454e-04
Barbara	0.8947	0.9579	0.8837	–0.0032	1.3354e-06	–0.0015
Flintstones	0.9502	0.9437	0.9072	0.0024	7.5727e-05	0.0012

TABLE 7. The APC under different encryption schemes (Using the average value of "Baboon.").

Method	Cao.[8]	Zhang.[28]	Teng.[29]	Wei.[26]	Ours
Cipher image	-0.0082	-0.0009	-0.0039	-0.0020	-0.0029

TABLE 8. Information entropy comparison.

Images	Lena	Pepper	Baboon	Barbara	Flintstones	Black
Plain image	7.4575	7.3964	7.3833	7.6353	6.5786	-
Proposed	7.9993	7.9991	7.9993	7.9992	7.9992	7.9994
Change P (1, 1)	7.9992	7.9993	7.9992	7.9991	7.9993	7.9993

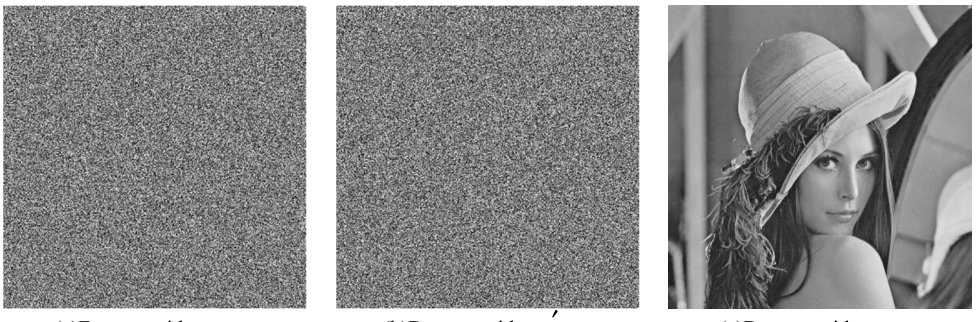
NPCR and UACI is presented in Eq. (14).

$$\begin{cases} NPCR = \dfrac{\sum_{ij} d(i,j)}{w \times h} \times 100\% \\ UACI = \dfrac{1}{w \times h}\left[\sum_{ij} \dfrac{|z_1(i,j) - z_2(i,j)|}{255}\right] \times 100\% \end{cases} \tag{14}$$

We conducted 100 sets of tests, where each set comprised two images, F_1 and F_2. F_1 is the original ciphertext image, while F_2 is the ciphertext image generated after changing a single plaintext pixel. Table 11 displays the average NPCR and UACI of each image, while Table 12 compares the results with other algorithms. The experimental findings reveal that the NPCR and UACI values of all tested images are close

TABLE 9. The $H(S)$ under different encryption schemes (Using the average value of "Baboon.").

Method	$H(S)$
Cao.[8]	7.9896
Zhang.[28]	7.9992
Teng.[29]	7.9913
Wei.[26]	7.9993
Ours	7.9993



(a)Encrypt with x_0 (b)Decrypt with x_0' (c)Decrypt with x_0

FIGURE 14. Key sensitivity analysis.

TABLE 10. Local entropy of different images.

Image	Lena	Pepper	Baboon	Barbara	Flintstones	Black
Local entropy	7.902439	7.901972	7.902347	7.903196	7.902073	7.902238
Fail or Pass	Pass	Pass	Pass	Pass	Pass	Pass

TABLE 11. NPCR and UACI.

	Change $P(1, 1)$		Change $P(256, 256)$		Change $P(512, 512)$	
	NPCR (%)	UACI (%)	NPCR (%)	UACI (%)	NPCR (%)	UACI (%)
Lena	99.5957	33.4762	99.6214	33.4505	99.6023	33.4664
Pepper	99.5963	33.4578	99.6056	33.5174	99.5934	33.4523
Baboon	99.6182	33.4963	99.6063	33.5012	99.5942	33.4458
Barbara	99.6313	33.4962	99.6165	33.4724	99.6159	33.4365
Boat	99.6107	33.4746	99.5973	33.4228	99.6163	33.4585
Flintstones	99.6115	33.4474	99.6102	33.4450	99.6224	33.4357
Black	99.6083	33.4959	99.5975	33.4632	99.6269	33.5325
House256	99.6276	33.4404	99.6302	33.4294	-	-
Object256	99.6364	33.4532	99.5928	33.4518	-	-
fabio256	99.6123	33.4346	99.6122	33.4263	-	-
Pass	10	10	10	10	7	7

to the ideal values, indicating that the LSHM-IES algorithm is relatively effective in protecting against selected plaintext attacks.

F. KEY SENSITIVITY ANALYSIS

In chaotic encryption, the key plays a vital role as it is the key information used to encrypt and decrypt the data. For chaotic encryption algorithms, a small change in the key may lead to completely different results. For key sensitivity, we take Fig. 14(a) as an example and change $x_0 = 0.677615301413672$ to $x_0' = 0.677615301413673$ and then decrypt the ciphertext image, the decrypted image is Fig. 14(b), and the decrypted image using x_0 is Fig. 14(c). It can be observed that even with extremely small changes in the key, the block disambiguation and diffusion strategies change dramatically and the algorithm is highly sensitive to the key.

G. ENCRYPTION SPEED ANALYSIS

The encryption speed is a critical metric for evaluating the performance of a chaotic image encryption algorithm, and

TABLE 12. Comparison of NPCR and UACI.

Lena	Ours	Chen.[34]	Cao. [8]	Liu. [35]
NPCR (%)	99.6074	99.23	99.25	99.46
UACI (%)	33.4645	33.48	36.35	33.34

TABLE 13. Time analysis of the proposed and existing algorithms.

Image size	Algorithms				
	Ours	Chen.[34]	Cao.[8]	Liu.[35]	N.[41]
128×128	0.0164	0.0201	0.0199	0.1934	0.1253
256×256	0.0673	0.0791	0.0832	0.7314	2.3261
512×512	0.3382	0.3706	0.3778	2.8625	10.8785

it is also a key factor in determining its suitability for widespread use. Typically, the speed of encryption is determined by the design of the algorithm and the software and hardware employed.

We performed a test by encrypting "Peppers (128 × 128)", "Lena (256 × 256)", and "Cameraman (512 × 512)" plaintext images 100 times and computed the average encryption time. Table 13 presents a comparison of our algorithm's encryption speed with those of algorithms from the literature [8], [34], [35], and [41]. Table 13 analysis indicates that LSHM-IES is more appropriate for real-time applications due to its shorter encryption time in comparison to other algorithms.

Additionally, algorithm complexity has a significant impact on speed performance. In our proposed algorithm, the alignment diffusion phase is the primary factor affecting computational complexity. This phase involves moving pixels a maximum of 3 × (M × N) times. Thus, the computational complexity of the LSHM-IES algorithm in this paper is O (M × N).

H. ROBUSTNESS ANALYSIS

During image transmission, noise or data loss may corrupt the image, making it necessary for the encryption algorithm to possess robustness. The algorithm's robustness is evaluated through simulation experiments with shear and noise attacks.

Figures 15(a) and (c) depict intercepted ciphertext images, while Figures 15(b) and (d) display the corresponding

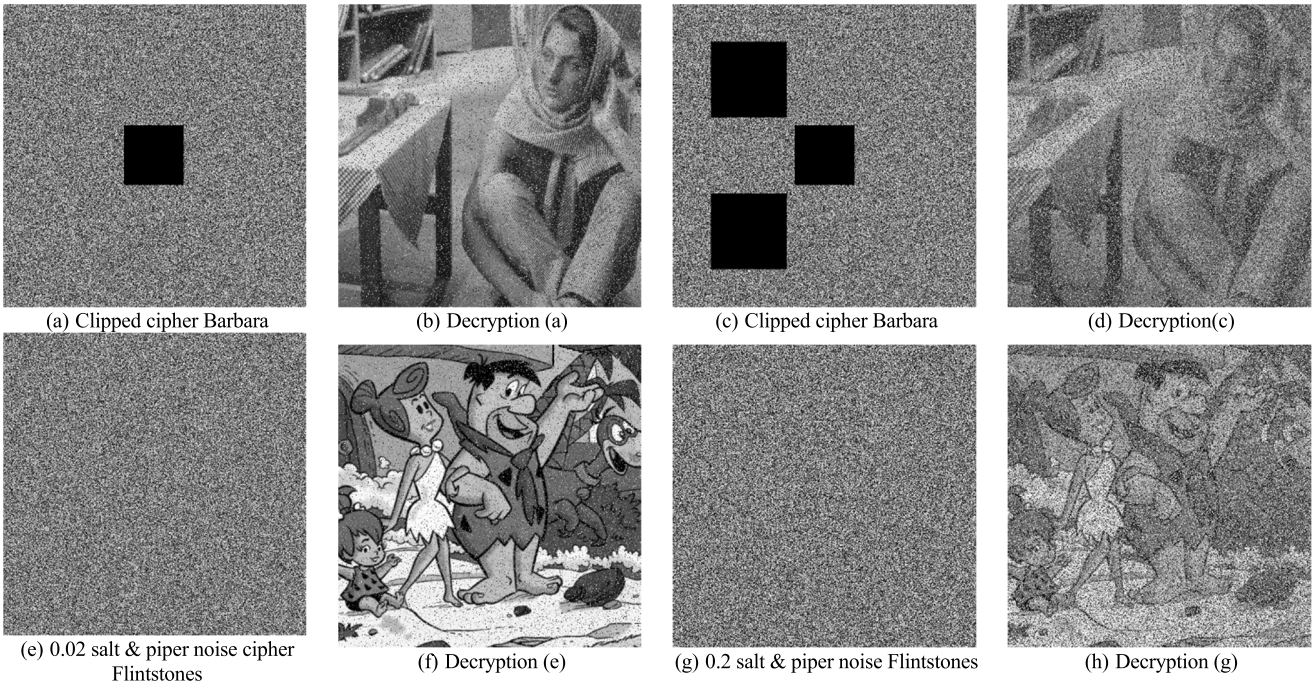


FIGURE 15. Anti-noise and data loss analysis.

decrypted intercepted ciphertext images. These images serve as an example of an interception attack. Taking pepper noise as an example, Figures 15(e) and (g) show the pepper noise with 0.02 and 0.2 ratio added respectively, and Figures 15(f) and (h) show the decrypted images after adding noise. Even when ciphertext is subjected to varying degrees of attacks and noise, the decrypted image remains visible.

Additionally, algorithm complexity has a significant impact on speed performance. In our proposed algorithm, the alignment diffusion phase is the primary factor affecting computational complexity. This phase involves moving pixels a maximum of $3 \times (M \times N)$ times. Thus, the computational complexity of the LSHM-IES algorithm in this paper is $O(M \times N)$.

VI. CONCLUSION

This paper proposes a novel two-dimensional Logistic-Sine hyperchaotic map (2D-LSHM) that incorporates classical one-dimensional maps via cosine variation. It features more parameters and stronger sensitivity. The chaotic properties are evaluated using LE indices and outperform the current 2D chaotic system. Based on this, we propose a dislocation-based encryption scheme (LSHM-IES) comprising convolutional altered pixel values and an improved Zigzag variation diffusion method. To begin with, the initial state and parameters of 2D-LSHM are generated using a 256-bit binary key. Then the image is encrypted by this system generating chaotic sequence combined with the algorithm of permutation and diffusion. Through simulation performance analysis, LSHM-IES has good encryption performance and the encryption time is better than other algorithms under the same conditions. By security performance analysis, LSHM-IES has strong robustness against data missing attacks and noise effects.

This paper focuses on examining the encryption process of a single grayscale image. Nevertheless, in real-world scenarios, it is often necessary to transmit multiple images simultaneously. So how to transmit multiple images efficiently and securely with encryption becomes an important issue. The next work plan is to study the encryption process of multiple images in depth, including how to manage and encrypt multiple images in a unified way, and how to improve the efficiency and security of transmission of multiple images.

REFERENCES

[1] Y. Wu and X. Dai, "Encryption of accounting data using DES algorithm in computing environment," *J. Intell. Fuzzy Syst.*, vol. 39, no. 4, pp. 5085–5095, Oct. 2020.
[2] C.-H. Yang and Y.-S. Chien, "FPGA implementation and design of a hybrid chaos-AES color image encryption algorithm," *Symmetry*, vol. 12, no. 2, p. 189, Jan. 2020.
[3] S. D. Watt, H. S. Sidhu, A. C. McIntosh, and J. Brindley, "Chaotic flow in competitive exothermic–endothermic reaction systems," *Appl. Math. Lett.*, vol. 115, May 2021, Art. no. 106960.
[4] D. Ghosh and J. Singh, "Spectrum-based multi-fault localization using chaotic genetic algorithm," *Inf. Softw. Technol.*, vol. 133, May 2021, Art. no. 106512.
[5] P. Paknejad, R. Khorsand, and M. Ramezanpour, "Chaotic improved PICEA-g-based multi-objective optimization for workflow scheduling in cloud environment," *Future Gener. Comput. Syst.*, vol. 117, pp. 12–28, Apr. 2021.
[6] G. Qi, L. Xu, and X. Yang, "Energy mechanism analysis for chaotic dynamics of gyrostat system and simulation of displacement orbit using COMSOL," *Appl. Math. Model.*, vol. 92, pp. 333–348, Apr. 2021.
[7] M. Z. Talhaoui, X. Wang, and A. Talhaoui, "A new one-dimensional chaotic map and its application in a novel permutation-less image encryption scheme," *Vis. Comput.*, vol. 37, no. 7, pp. 1757–1768, Jul. 2021.
[8] C. Cao, K. Sun, and W. Liu, "A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map," *Signal Process.*, vol. 143, pp. 122–133, Feb. 2018.

[9] W. J. Jun and T. S. Fun, "A new image encryption algorithm based on single S-box and dynamic encryption step," *IEEE Access*, vol. 9, pp. 120596–120612, 2021.
[10] X. Q. Zeng and R. S. Ye, "Chaotic image encryption algorithm based on improved logistic map," *Comput. Eng.*, vol. 47, no. 11, pp. 158–165, 2021.
[11] Z. Hua, Y. Chen, H. Bao, and Y. Zhou, "Two-dimensional parametric polynomial chaotic system," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 52, no. 7, pp. 4402–4414, Jul. 2022.
[12] J. Liu, Y. Wang, Z. Liu, and H. Zhu, "A chaotic image encryption algorithm based on coupled piecewise sine map and sensitive diffusion structure," *Nonlinear Dyn.*, vol. 104, no. 4, pp. 4615–4633, Jun. 2021.
[13] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurcation Chaos*, vol. 8, no. 6, pp. 1259–1284, Jun. 1998.
[14] Z. Man, J. Li, X. Di, Y. Sheng, and Z. Liu, "Double image encryption algorithm based on neural network and chaos," *Chaos, Solitons Fractals*, vol. 152, p. 111318, Nov. 2021, doi: 10.1016/j.chaos.2021.111318.
[15] J. S. Muthu and P. Murali, "A novel DICOM image encryption with JSMP map," *Optik*, vol. 251, p. 168416, Feb. 2022, doi: 10.1016/j.ijleo.2021.168416.
[16] K. U. Shahna and A. Mohamed, "Novel hyper chaotic color image encryption based on pixel and bit level scrambling with diffusion," *Signal Process., Image Commun.*, vol. 99, p. 116495, Nov. 2021.
[17] Z. Hua, J. Li, Y. Chen, and S. Yi, "Design and application of an S-box using complete Latin square," *Nonlinear Dyn.*, vol. 104, no. 1, pp. 807–825, Mar. 2021.
[18] Q. Lai, Z. Wan, H. Zhang, and G. Chen, "Design and analysis of multiscroll memristive Hopfield neural network with adjustable memductance and application to image encryption," *IEEE Trans. Neural Netw. Learn. Syst.*, early access, Feb. 10, 2022, doi: 10.1109/TNNLS.2022.3146570.
[19] Q. Lai and Y. Liu, "A cross-channel color image encryption algorithm using two-dimensional hyperchaotic map," *Expert Syst. Appl.*, vol. 223, Aug. 2023, Art. no. 119923.
[20] Q. Lai, G. Hu, U. Erkan, and A. Toktas, "A novel pixel-split image encryption scheme based on 2D Salomon map," *Expert Syst. Appl.*, vol. 213, Mar. 2023, Art. no. 118845.
[21] Q. Lai, Z. Wan, and P. D. K. Kuate, "Generating grid multi-scroll attractors in memristive neural networks," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 70, no. 3, pp. 1324–1336, Mar. 2023.
[22] K. Qian, W. Feng, Z. Qin, J. Zhang, X. Luo, and Z. Zhu, "A novel image encryption scheme based on memristive chaotic system and combining bidirectional bit-level cyclic shift and dynamic DNA-level diffusion," *Frontiers Phys.*, vol. 10, Aug. 2022, Art. no. 963795.
[23] W. Feng, X. Zhao, J. Zhang, Z. Qin, J. Zhang, and Y. He, "Image encryption algorithm based on plane-level image filtering and discrete logarithmic transform," *Mathematics*, vol. 10, no. 15, p. 2751, Aug. 2022.
[24] W. Feng, Z. Qin, J. Zhang, and M. Ahmad, "Cryptanalysis and improvement of the image encryption scheme based on Feistel network and dynamic DNA encoding," *IEEE Access*, vol. 9, pp. 145459–145470, 2021.
[25] W. Feng and J. Zhang, "Cryptanalzing a novel hyper-chaotic image encryption scheme based on pixel-level filtering and DNA-level diffusion," *IEEE Access*, vol. 8, pp. 209471–209482, 2020.
[26] W. Feng, J. Zhang, and Z. Qin, "A secure and efficient image transmission scheme based on two chaotic maps," *Complexity*, vol. 2021, pp. 1–19, Nov. 2021.
[27] Z. Hua and Y. Zhou, "Exponential chaotic model for generating robust chaos," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 6, pp. 3713–3724, Jun. 2021.
[28] S. N. Zhang and Q. M. Li, "Color image encryption algorithm based on logistics-sin-cosine mapping," *Comput. Sci.*, vol. 49, no. 1, pp. 353–358, 2022.
[29] L. Teng, X. Wang, and Y. Xian, "Image encryption algorithm based on a 2D-CLSS hyperchaotic map using simultaneous permutation and diffusion," *Inf. Sci.*, vol. 605, pp. 71–85, Aug. 2022.
[30] J. Yu, W. Xie, Z. Zhong, and H. Wang, "Image encryption algorithm based on hyperchaotic system and a new DNA sequence operation," *Chaos, Solitons Fractals*, vol. 162, Sep. 2022, Art. no. 112456.
[31] J. Zheng and T. Bao, "An image encryption algorithm using cascade chaotic map and S-box," *Entropy*, vol. 24, no. 12, p. 1827, Dec. 2022.
[32] W. Cao, Y. Mao, and Y. Zhou, "Designing a 2D infinite collapse map for image encryption," *Signal Process.*, vol. 171, p. 107457, Jun. 2020, doi: 10.1016/j.sigpro.2020.107457.
[33] N. Tsafack, S. Sankar, B. Abd-El-Atty, J. Kengne, K. C. Jithin, A. Belazi, I. Mehmood, A. K. Bashir, O.-Y. Song, and A. A. A. El-Latif, "A new chaotic map with dynamic analysis and encryption application in Internet of Health Things," *IEEE Access*, vol. 8, pp. 137731–137744, 2020.
[34] H. Chen, E. Bai, X. Jiang, and Y. Wu, "A fast image encryption algorithm based on improved 6-D hyper-chaotic system," *IEEE Access*, vol. 10, pp. 116031–116044, 2022.
[35] S. Liu, C. Li, and Y. Li, "A novel image encryption algorithm based on exponent-cosine chaotic mapping," *J. Electron. Inf. Technol.*, vol. 44, no. 5, pp. 1754–1762, 2022.
[36] Z. Hua, J. Li, Y. Li, and Y. Chen, "Image encryption using value-differencing transformation and modified ZigZag transformation," *Nonlinear Dyn.*, vol. 106, no. 4, pp. 3583–3599, Dec. 2021.
[37] Z. Guo and P. Sun, "Improved reverse ZigZag transform and DNA diffusion chaotic image encryption method," *Multimedia Tools Appl.*, vol. 81, no. 8, pp. 11301–11323, Mar. 2022.
[38] J. Zheng and T. Lv, "Image encryption algorithm based on cascaded chaotic map and improved zigzag transform," *IET Image Process.*, vol. 16, no. 14, pp. 3863–3875, Dec. 2022.
[39] S. Zhu, X. Deng, W. Zhang, and C. Zhu, "Image encryption scheme based on newly designed chaotic map and parallel DNA coding," *Mathematics*, vol. 11, no. 1, p. 231, Jan. 2023.
[40] J. Wang, X. Song, and A. A. A. El-Latif, "Single-objective particle swarm optimization-based chaotic image encryption scheme," *Electronics*, vol. 11, no. 16, p. 2628, Aug. 2022.
[41] N. Charalampidis, C. Volos, L. Moysis, H. E. Nistazakis, and I. Stouboulos, "A novel piecewise chaotic map for image encryption," in *Proc. 11th Int. Conf. Modern Circuits Syst. Technol. (MOCAST)*, Bremen, Germany, Jun. 2022, pp. 1–4.

DONGYAO ZOU received the Ph.D. degree in circuits and systems from the Beijing University of Posts and Telecommunications, in 2008. He is currently an Associate Professor with the Zhengzhou University of Light Industry. He has published more than ten research papers in journals and conferences. His research interests include chaotic image encryption, artificial intelligence, and indoor positioning technology.

TENGDA PEI received the bachelor's degree in the Internet of Things engineering from the Zhengzhou University of Light Industry, China, in 2019, where he is currently pursuing the degree with the School of Computer and Communication Engineering. His research interests include information security, chaotic systems, and chaotic image encryption.

GUANGYONG XI received the Ph.D. degree in engineering surveying from Hohai University, in 2011. He is currently an Associate Professor with the Zhengzhou University of Light Industry. He has published more than ten research papers in journals and conferences. His research interests include information security, artificial intelligence, and indoor positioning technology.

LIPING WANG received the Ph.D. degree in electronic technology from the Huazhong University of Science and Technology, Wuhan, Hubei, in 2016. Since 2017, she has been teaching and conducting research with the School of Computer and Communication Engineering, Zhengzhou University of Light Industry. Her research interests include embedded systems and artificial intelligence.