IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 25 June 2023, accepted 10 August 2023, date of publication 15 August 2023, date of current version 30 August 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3305637

RESEARCH ARTICLE

A Fast Image Encryption Algorithm Based on Logistic Mapping and Hyperchaotic Lorenz System for Clear Text Correlation

DANDAN HE[1,2], RAJAMOHAN PARTHASARATHY[2], HONG LI[1], AND ZEXUN GENG[1]

[1]School of Information Engineering, Pingdingshan University, Pingdingshan 467000, China
[2]Faculty of Engineering, Built Environment and Information Technology, SEGi University, Kota Damansara 47810, Malaysia

Corresponding author: Hong Li (2650@pdsu.edu.cn)

This work was supported by the Pingdingshan University Horizontal Project, Audio and Video Resource Processing System Development, under Grant PXY-HX-2022067.

ABSTRACT Image encryption (IE) technology is vital to privacy, but the parameter range of the traditional image encryption technology is limited. So it is important to enhance the performance of IE methods. In this study, a plaintext associative IE based on the improved logistic map and hyperchaotic system is proposed. The improved logistic map scrambles the pixels of the image. Then the hyperchaotic system performs diffusion and confusion operations on the image. For parameters μ and r, the sequence generated by the improved logistic map can traverse and uniformly distribute in the space (0,1). The Lyapunov exponent of the improved logistic map is greater than 21.5. The correlation coefficients of the encrypted image pixels after encryption are all less than 0.05. The UACI and NPCR indices of the improved encryption method are close to their theoretical values of 98.6133 and 33.1287, respectively, which are higher than those of the reference methods. The improved encryption method overcomes the limitations in the parameter range of traditional image and text encryption techniques, slow encryption speed, and uneven chaotic sequences. This method has higher security and sensitivity, andit can be used to establish a plaintext associative IE method.

INDEX TERMS Logistic mapping, hyperchaotic systems, plaintext associative image, encryption algorithm.

I. INTRODUCTION

In the era of big data, information has great value. Images are an important carrier of information, and the information hidden in certain images is crucial. In fields such as urbanization construction and robotics research, a large amount of image information processing is involved [1], [2]. It will involve some important information that needs to be protected to avoid damaging the interests of relevant institutions. Research has shown that using machine learning such as neural networks for feature extraction and information estimation can obtain relevant image information [3]. In order to ensure the safe and reliable transmission, storage, access, and other processes of digital images, it is also necessary to adopt certain image information protection methods. Image encryption technology can ensure the privacy and confidentiality of multimedia data, and is currently one of the most effective methods to protect image security. Cryptographers found that chaotic systems have inherent properties such as extreme sensitivity to Initial condition and parameters, aperiodicity and ergodicity, which are very suitable for the Scrambling and diffusion ideas in cryptography [4]. Therefore, Scholars have encrypted the data using pseudo random sequences generated by chaotic systems. Hyperchaotic systems have better chaotic characteristics and orbital complexity, and can effectively generate chaotic sequences [5]. Although these methods can resist selection or known-plaintext attack. Due to the involvement of loop operations and plaintext related diffusion operations during the operation process, the encryption time is very slow. So these two types of algorithms cannot meet the requirements of actual communication. In order to improve the encryption speed of plaintext image encryption systems without compromising security, this paper proposes a new plaintext image encryption system. Therefore, in this study, logistic mapping was improved and combined with chaotic systems for the study of plaintext

The associate editor coordinating the review of this manuscript and approving it for publication was Abdullah Iliyasu.

associated image encryption algorithms. This experiment innovatively proposes a plaintext image encryption algorithm that performs both Scrambling and diffusion simultaneously. In this experiment, the bits of the sequence generated by the improved mapping are rearranged, so that the sequence has better chaotic characteristics, ergodicity, initial value sensitivity, and Pseudo-randomness. At the same time, an improved Logistic mapping was used to perform position scrambling on image pixels. And three randomly generated pseudo random sequences and a hyperchaotic Lorenz system were used to perform plaintext independent diffusion and plaintext related scrambling operations on the image. Through MATLAB simulation experiments and comparison with some image encryption system algorithms, it can be concluded that this encryption system has advantages. They include fast encryption/decryption speed, large key space, good statistical characteristics of cryptographic images, strong key sensitivity, strong plaintext sensitivity, strong ciphertext sensitivity, and high information entropy.

II. RELATED WORKS

Chaotic System (CS)isa common used encryption method in IE algorithms [6]. CS exhibits good application characteristics in IE technology. With the basic characteristics of image CSs, researchers have made improvements to address the flaws and vulnerabilities in the basic methods. By introducing the concept of two-dimensional space and related technologies, they have finally established an encryption method that can be used for color images. The result proves that the security of the new method is much higher than that of the existing IE methods [7]. Traditional one-dimensional CSs are useful for encryption and decryption work. However, the key in one-dimensional CSs is limited by space, leading to a decrease in security. Therefore, Akif et al. introduced the concept of two-dimensional space to improve CSs. They used the new concept to re-perform logical mapping and bit reordering, resulting in a new sequence. In statistical tests, the keys and their cycles generated by this method have high capacity and have passed multiple rigorous tests [8]. Based on the one-dimensional CS, Khokhar et al. used the two-dimensional CS to control the load frequency of the power grid. Whenimproving the method, they optimized the mapping methodwith cosine function. The experimental results prove that this method has better convergence and effectively controls the running time while having higher sensitivity [9]. Wang et al. improved the diffusion and scrambling operations in IEwith a new CS. In this stage, the new method displayed the image in binary and processed the sub-images into bits and changes the pixel values. The result proved that the new method couldexhibit better chaotic characteristics and high security [10]. IE methods in optics have been deeply researched. In related research work, researchers proposed using neural networks and hyperchaotic systems combined to perform scrambling operations in encryption algorithms. At the same time, they conducted experimental validation of the newly established method for IE. The result showed that the new method could effectively improve the security of optical images and provide new ideas for IE methods [11].

The logistic mapping is one of the methods applied in CSs. CSs based on logistic mapping exhibit good chaotic properties, and have been successfully applied in encryption algorithms. Yan et al. combined the logisticwith other mappings to establish CSs. The new systems can overcome the drawbacks of traditional methods in terms of uneven chaotic sequences and have higher encryption performance. In cryptography-related research, the new systems demonstrate high chaotic performance, which is beneficial for the cryptography improvement [12]. Studies have shown that combining the improved logistic mapping method with chaotic models can enhance the security of cryptographic systems. This method can decrease the computation complexity, improve the limitations of parameter space, and increase the key space. The new model can effectively resist various cryptographic attacks [13]. In medical applications, logistic mapping can enhance the traversal and sensitivity of systems. CSs based on logistic mapping can effectively protect patients' personal information. This method has also been effectively validated in IE research. In the experiment, two CSs based on logistic mapping were combined to resist cryptographic attacks. The data in the results indicate that this method has higher security and hyperiority [14]. For numerical calculations in encryption, logistic mapping can reduce the calculation errors, thereby increasing the computational accuracy. CSs based on logistic mapping exhibit high logical mapping capability. In the experiment, the pseudo-random numbers are subjected to binary processing. This method can enhance the performance of pseudo-random numbers [15].

In the above research, the main contributions can be drawn as follows. Firstly, chaotic systems demonstrate good application characteristics in image encryption technology. Through method improvements, chaotic systems can effectively improve the security of images and provide new ideas for image encryption methods. Secondly, the combination of Logistic mapping and other mapping methods can overcome the shortcomings of traditional methods, and its encryption characteristics are relatively high. The combination of logistic mapping method and Chaos model can improve the security of cryptographic system. So in this experiment, they were combined for use in IE algorithms. To improve the security and sensitivity of the method, logistic mapping was improved and combined with the hyper CS to establish a plaintext-related IE method in the experiment. It is hoped that this can provide technical reference for encryption technology in the field of IE.

III. PLAINTEXT ASSOCIATIVE IE BASED ON LOGISTIC MAPPING AND HYPERCHAOTIC SYSTEM

A. CSS BASED ON IMPROVED LOGISTIC MAPS

For initial values, chaotic systems have high sensitivity and pseudo-randomness [16], [17]. The diffusion and Scrambling operations in IE are similar to chaos theory [18]. Therefore, chaotic theory is applied in IE algorithms. Logistic mapping is a simple one-dimensional CS that has a simple sequence calculation form [19]. Logistic mapping exhibits pseudo-random sequence characteristics, which can be well-applied in IE. Although high-dimensional chaotic systems have high security, they have high computational costs and are not easy to implement. In order to balance the security and implementation possibility of chaotic mapping, the traditional one-dimensional logistic mapping was used as the basic research method and improved in this experiment. Formula (1) is the calculation method for one-dimensional logistic mapping.

$$X_n = -\mu X_{n-1}(X_{n-1} - 1) \tag{1}$$

In formula (1), μ is the control parameter, and its range is within (0,4]. Only when it falls within [3.569945627,4], the sequence X_n is in a chaotic state. The one-dimensional logistic mapping has limitations in its control parameter range and uneven point distribution. In order to solve these problems, the traditional one-dimensional logistic mapping was optimized and improved in this experiment. Formula (2) is the improved method.

$$X_{n+1} = \mathrm{mod}(r \times X_n \times (1 - X_n), 1) \tag{2}$$

In formula (2), r is the control parameter, and its value is not equal to 0. The range of X_n is within (0,1). mod() is the mod function, which is used to take the modulus and return the remainder. Althoughthe mod operation may increase the time and computational complexity of the system, it can allow the parameter r to break through the limitation of the range of (0,4]. In the parameter range of (0,4], to improve the chaotic characteristics of the sequence generated by logistic mapping, bit-reversal is performed in this experiment. This method can rearrange the sequence generated by the mapping, thereby improving the pseudo-randomness, chaotic characteristics, the initial value sensitivity andthetraversal properties of the method. Figure 1 is a schematic diagram of bit-reversal.

In the bit-reversal, the first step is to substitute r and the initial value X0 of the sequence into Formula (2), so a new X1 can be obtained. Sincethebinary processing can improve the computational efficiency of the method [20], in the second step, X1 needs to be converted into binary form. The binary form is represented as an L-bit number, where L can be any positive integer. It is assumed that X1 is 0.75 and L is 16, the 16-bit binary form of 0.75 is represented as 0.75→0.1100000000000000. In the second step, a bit-reversal of the binary sequence is performed, which means that the bit values after the decimal point need to be rearranged. In this process, the bit values of the odd and even positions need to be rearranged. That is, the values of the odd positions are arranged at the front of the sequence, and the values of the even positions are arranged at the end of the sequence, resulting in a new number, i.e., 0.0000000100000001. In the third step, the binary number obtained in step 2 needs to be converted into a decimal number. Then this decimal number is taken as the initial X1 value, which is substituted into Formula (2) so as to obtain the next value. By repeating steps 2 and 3, a chaotic sequence with a length of n can be obtained.

B. IMPROVED LOGISTIC MAPPING AND HYPERCS BASED PLAINTEXT ASSOCIATIVE IE

CSs exhibit extremely high sensitivity to initial values, and generate many pseudo-random sequences [21]. The Scrambling and diffusion operations in CSs correspond to the scrambling and diffusion operations in IE algorithms. Therefore, CSs can contribute the encryptionof digital images. The key used in encryption operations based on CSs is the same, which belongs to the category of symmetric encryption. The advancement of technology has led to the expansion of the use and exchange of digital data, which places great importance on the security of these data. In text and image encryption technology, researchers use techniques such as DNA encoding and 4D conservative chaos to enhance their ability to resist plaintext and other attacks [22], [23]. Chaos system is an important encryption strategy in image encryption methods. Figure 2 shows the block diagram of classical chaotic image encryption and decryption.

In Figure 2, this encryption method requires two inputs, namely a plaintext image and a key. The key is a password generated through a chaotic system, which serves as a participant in Scrambling and spreading the ciphertext image, ultimately generating the ciphertext image. In the process of confusion and diffusion of plaintext images, chaotic systems generate Keystream. Cryptographic images are mainly transmitted through public channels, while keys are transmitted through secret channels. The decryption process is the opposite of the encryption process, which requires the use of a key to perform reverse diffusion and scrambling operations on the ciphertext image, ultimately outputting the plaintext image. This encryption method uses a cryptographic algorithm generated based on chaotic systems to ensure the privacy and security of data during transmission, ensuring the protection of encrypted data during transmission on public networks. The development of IE technology has promoted the improvement of encryption methods [18]. The most commonly used encryption methods include pixel scrambling, pixel gray value diffusion, and scrambling and diffusion [24]. The commonly used passive attack methods mainly include chosen-plaintext attacks, chosen-ciphertext attacks, known-plaintext attacks, and ciphertext-only attacks [25]. Researchers have proposed the plaintext associative IE method, which has high security [26]. However, its encryption speed is slow and its practical application is limited. To address this problem, the plaintext IE method has been improved in this experiment. In the improved encryption method, there are two diffusion operations that are not correlated with the plaintext, one scrambling operation that is correlated with the plaintext, and one scrambling operation that is not correlated with the plaintext. Since there is only one scrambling operation that is correlated with the

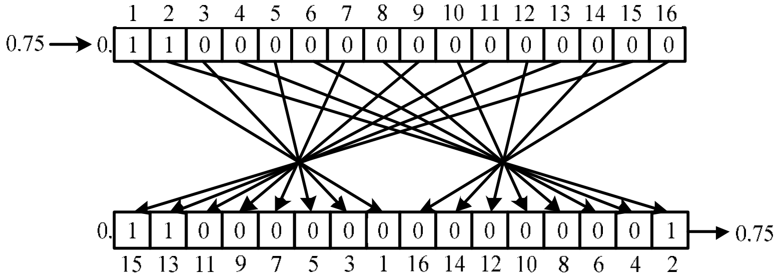


FIGURE 1. CShematic diagram of bit rearrangement.

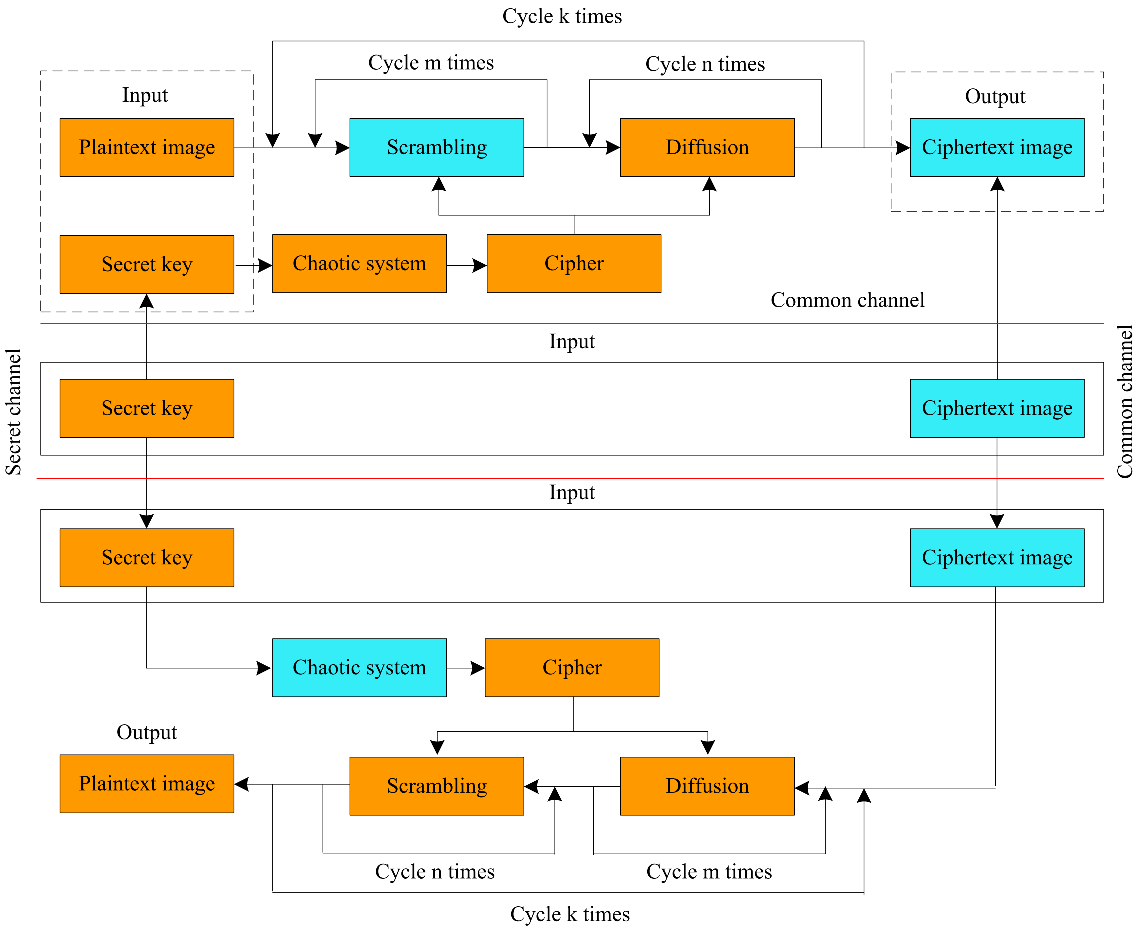


FIGURE 2. Encryption and decryption block diagram of classical chaotic images.

plaintext in this encryption method, the speed of the entire encryption method has been effectively improved. At the same time, this encryption method can resist chosen-plaintext attacks and known-plaintext attacks. Since the Lyapunov exponent of the hyperchaotic Lorenz system is a positive value, the chaotic characteristics of this system are better, and the complexity of the orbit is higher. Thissystem can generate better chaotic sequences, so the hyperchaotic Lorenz system is chosen for improving the encryption method in this experiment. Figure 3 shows the specific process of the improved encryption method.

The improved plaintext associative IE algorithm proposed in the experiment mainly includes seven steps. Firstly, a plaintext image P is input into the encryption method, with a length of M and width of N. Then, the larger value of the length and width, K=max(M,N), is taken. Next, the image scrambling process is performed once using the improved logistic mapping function, which generates pseudo-random numbers r1, r2 and r3. These pseudo-random numbers are all 8-digit numbers. In the fourth step, {x0, y0, z0, w0} represent the initial values of the hyperchaotic Lorenz system. Through further iteration, the pseudo-random matrices X, Y, and Z can

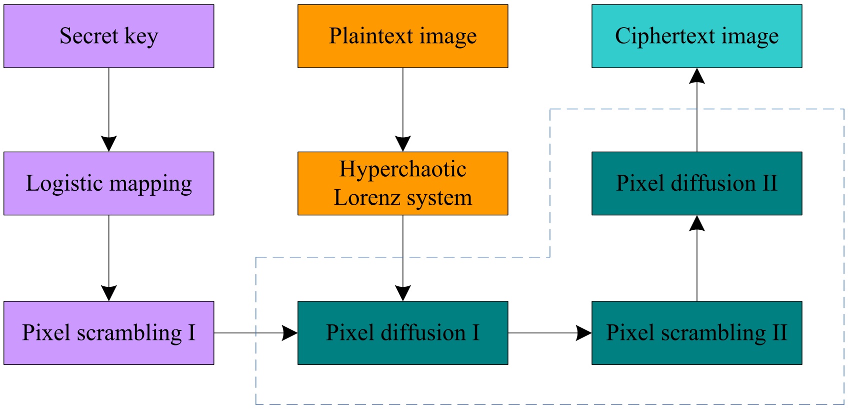


FIGURE 3. Encryption flowchart of plaintext associative Scrambling images.

be obtained. These matrices can be used for scrambling and diffusion operations in the plaintext IE process, as shown in Formulas (3)-(5).

$$X(i,j) = floor((x_{(i-1)\times N+j} + z_{(i-1)\times N+j} + 100 \bmod 1) \times 10^{13}) \bmod 256 \quad (3)$$

$$Y(i,j) = floor((y_{(i-1)\times N+j} + z_{(i-1)\times N+j} + 100 \bmod 1) \times 10^{13}) \bmod K \quad (4)$$

$$Z(i,j) = floor((x_{(i-1)\times N+j} + w_{(i-1)\times N+j} + 100 \bmod 1) \times 10^{13}) \bmod 256 \quad (5)$$

In formulas (3) to (5), i=1,2,…,M, j=1,2,…,N. It denotes the maximum integer that is less than or equal to t. The use of the "+100" modular operation can convert the possible negative state variables of the hyperchaotic Lorenz system into positive values.

In the fifth step, matrix X is used to transform P into a new matrix A, where the pixel values in P are all changed. Formula (6) to (7) can be used to transform P(1,1) into A(1,1).

$$A(1,1) = P(1,1) + X(1,1) + r_1 \bmod 256 \quad (6)$$

$$A(1,j) = P(1,j) + A(1,j-1) + X(1,j) \bmod 256 \quad (7)$$

Formula (8) can be used to transform P(i,1) into A(i,1).

$$A(i,1) = P(i,1) + A(i-1,1) + X(i,1) \bmod 256 \quad (8)$$

Formula (9) can be used to transform P(i,j) into A(i,j).

$$A(i,j) = P(i,j) + A(i,j-1) + A(i-1,j) + X(i,j) \bmod 256 \quad (9)$$

In Formula (9), i=2,3,…,M and j=2,3,…,N. The diffusion algorithm using formulas (6) to (9) can generate matrix A.

In the sixth step, matrix Y is used to transform A into a new matrix D, without changing the values in matrix A. Formulas(10) to (11) can be used to transform A into D

$$m = Y(i,j) + Y(i,N) + A(i,N) + A(M,N) \bmod M \quad (10)$$

$$n = Y(i,j) + Y(M,j) + A(M,j) + A(M,N) \bmod M \quad (11)$$

In formulas (10) to (11), i=1,2,…,M-1, and j=1,2,…,N-1. When the calculated value of m or n is equal to 0, the corresponding position of A(i,j) remains unchanged.

Finally,thematrix Z is used to transform B into the ciphertext image C, completing the encryption of the image. Formula (12) to (13) can be used to transform B(M,j) into C(M,j).

$$C(M,N) = B(M,N) + Z(M,N) + r_3 \bmod 256 \quad (12)$$

$$C(M,j) = B(M,j) + C(M,j+1) + Z(M,j) \bmod 256 \quad (13)$$

In formulas (12) to (13), j=N-1,N-2,…,2,1. Formula (14) can be used to transform B(i,N) into C(i,N).

$$C(i,N) = B(i,N) + C(i+1,N) + Z(i,N) \bmod 256 \quad (14)$$

In formula (14), i=N-1,N-2,…,2,1. Formula (15) can be used to transform B(i,j) into C(i,j).

$$C(i,j) = B(i,j) + C(i,j+1) + C(i+1,j) + Z(i,j) \bmod 256 \quad (15)$$

By using formulas (12) to (15), the ciphertext image, i.e. matrix C, can be obtained

IV. VERIFICATION AND ANALYSIS OF PLAINTEXT ASSOCIATIVE IE ALGORITHM BASED ON LOGISTIC MAPPING AND HYPERCHAOTIC SYSTEM

The operating system used for verification was Windows 10, the processor was an Intel Core i7-4720HQ CPU @2.60 GHz, and the memory size was 8G. The simulation software used for the experiments was MATLAB 2016. To ensure the objectivity and comparability of the verification analysis, all operations should be conducted under the same hardware and software environment [27], [28]. In the simulation experiments, the performance of the improved logistic mapping was first compared and analyzed. The bifurcation diagram of the two types oflogistic mappings is Figure 4.

From Figure 4, the traditional Logistic mapping only exhibits chaotic behavior within the range of [4, 3.5699]. However, the improved logistic mapping breaks through

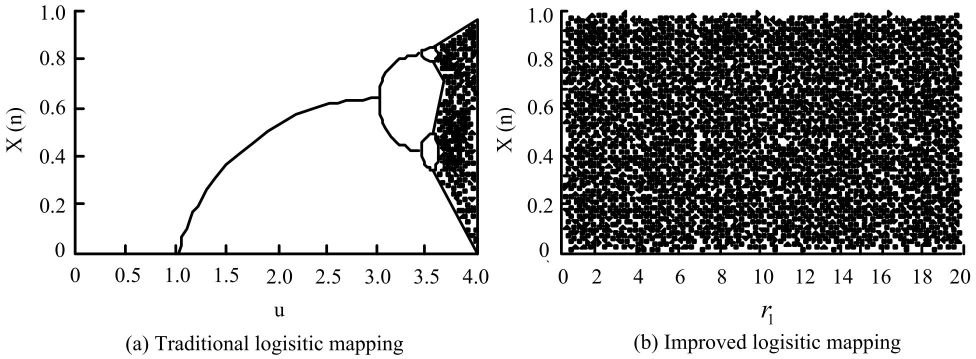


FIGURE 4. Bifurcation diagram of two maps.

the limitations of the parameters and exhibits good chaotic characteristics within the range of (0,4]. For parameters μ and r, sequences generated by the improved logistic mapping can traverse and be evenly distributed in the (0,1) space. This is because when scrambling and diffusion processing are carried out simultaneously, this experiment uses the modular operations to increase the range of parameters μ and r. And through bit rearrangement, the ergodicity and uniformity of parameters are improved.

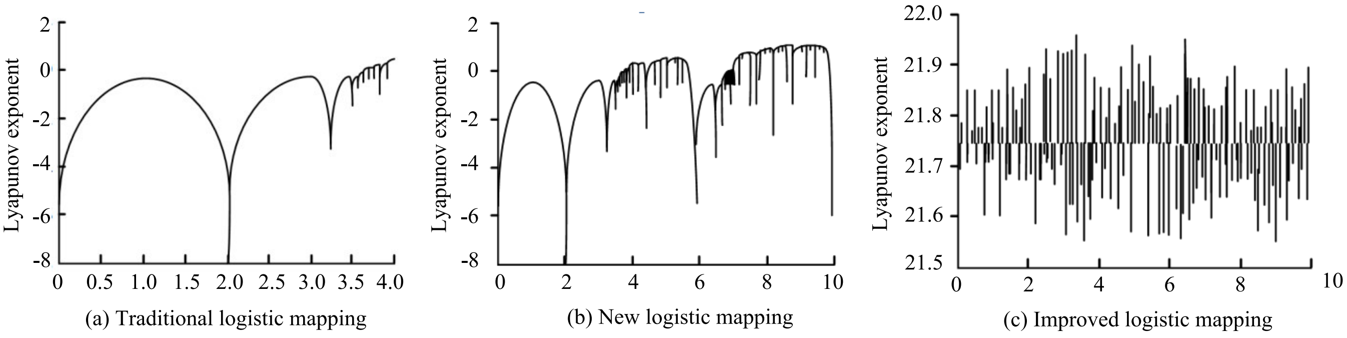
The sensitivity to initial values is vital for the properties of CSs, which can be measured by the Lyapunov exponent. If the sign of the Lyapunov exponent obtained during the calculation is positive, it indicates that the CS has strong chaos. If the sign is negative, it indicates that the CS has weak chaos. Figure 5 shows the values of the Lyapunov exponent for differentlogistic mappings. Sub-Figure (a) shows the traditionallogistic mapping with a parameter within the range of (0,4]. Sub-Figure (b) shows the new Logistic mapping obtained by taking the modulus, with a larger range of parameter values. However, the Lyapunov exponent of the new Logistic mapping has negative values. Sub-Figure (c) shows the improved method obtained by reordering the bits of the newlogistic mapping. The Lyapunov exponent of the improved Logistic mapping is greater than 21.5, which is significantly higher than that of the traditional and new logistic mappings. The results show that the improved logistic mapping has higher chaos performance.

In addition, after reordering the bits of the logistic mapping, SP800-22Rvlla was used in the experiment to test whether the chaotic sequence generated by this method had randomness. During the test, the length of the bit sequence was set to 106, and the significance level was set to 0.01. When p>0.01, it indicates that the test has passed. Tables 2 and 3 show the results of the various test items, which indicate that the bit mapping generated sequence after bit ordering can pass all subtests. However, the bit sequence generated by thelogistic mapping before bit ordering can only pass some subtests. This is because the chaotic sequence generated by logistic mapping after bit rearrangement has better randomness. Compared to the logistic mappingwithout bit rearrangement, it exhibits better chaotic performance in subtests.

Based on the bifurcation diagrams of the chaotic logistic mapping, the SP800-22Rvlla test, and the computation of the Lyapunov exponent, it can be concluded that the logistic mapping after bit ordering can effectively increase the randomness of the CS. The improved logistic mapping CS has better randomness than the original logistic mapping CS. The sequence from the improved Logistic mapping CS has higher chaos performance. Compared to the unimproved method, the improved logistic mapping method can perform both scrambling and diffusion processing simultaneously. In addition, this experiment uses modular operations to increase the range of parameters μ and r. And the improved method improves the randomness of the chaotic system, as well as the ergodicity and distribution uniformity of the parameters through bit rearrangement.

Subsequently, performance verification experiments were conducted on the plaintext-related IEwith the improved logistic mapping and hyperchaotic system. The Lena, Clock, and Pepper images in the UCS-SIPI Image Database were selected as test images for the IE. Security performance testing is a necessary step in studying the security and feasibility of the plaintext-related IE. In the experiments, statistical histogram analysis, correlation analysis, and resistance to differential attacks were analyzed. As for the correlation of adjacent pixels in the plaintext images, a high correlation is indicated by the close pixel values. In [1, 0], the correlation coefficient is greater, the correlation is stronger, and vice versa. Figure 6 shows the correlation of Lena image in various directions for both plaintext and ciphertext images. The correlation coefficients of the plaintext images tend to be 1 in each direction. However, the correlation coefficients of the ciphertext images are all below 0.05, indicating a high level of security after encryption.

Statistical histogram analysis reflects the pixel value distribution and law in the plaintext image. The statistical histogram of the plaintext image has large information, which is not conducive to information processing and results in lower security. Therefore, in the encryption of



(a) Traditional logistic mapping (b) New logistic mapping (c) Improved logistic mapping

FIGURE 5. Lyapunov exponents under three mappings.

TABLE 1. SP800-22RVLLA test results.

Test Name	P-value before improvement	Improved p-value	Test Name	P-value before improvement	Improved p-value
Single bit frequency test	0.0256	0.75342	DiCSrete Fourier Test	3.508×10-6	0.3609
In Block Frequency Test	0	0.72618	Maurer General Statistical Test	0.0756	0.8476
Poker test	6.526×10-4	0.21070	Linear complexity test	0.7198	0.1365
Maximum 1 run in block test	0.9689	0.17130	Sequence testing	0,0	0.2638,0.3798
Binary Matrix Rank Test	0.0032	0.01401	Approximate entropy test	0	0.9183
Non overlapping template matching test	0.6387	0.19580	Accumulate and Test	1,0.9997	0.9998,0.9909
Overlapping template matching test	0.5421	0.16983	-	-	-

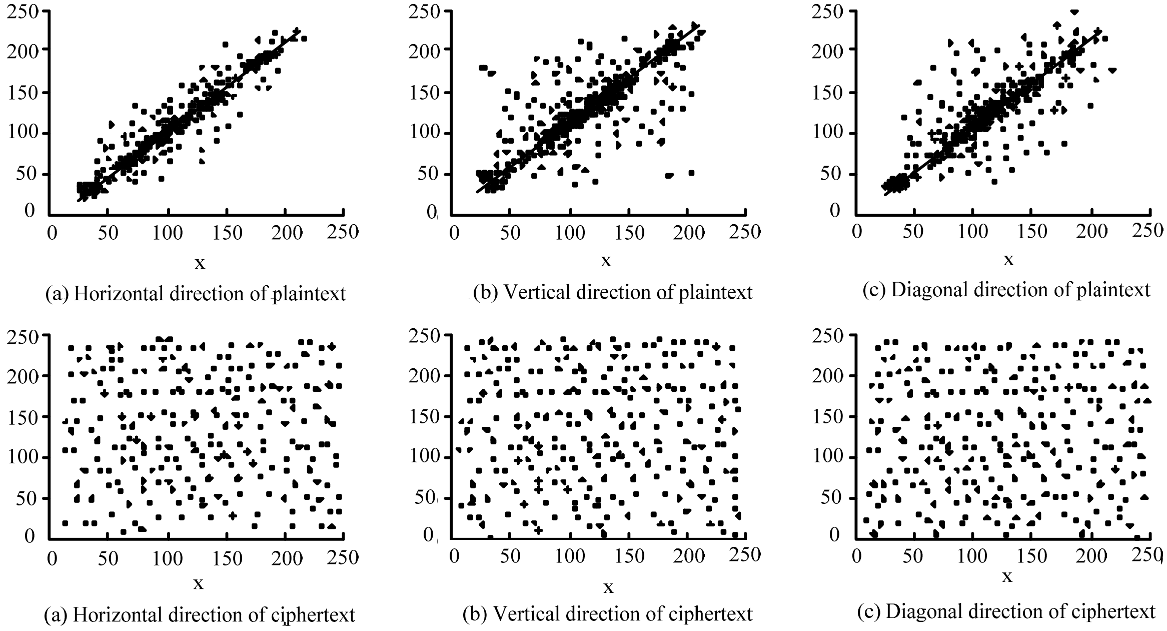
TABLE 2. Random travel test results and random travel variant test results.

Random travel test results			Random travel variant test results					
x	P-value before improvement	Improved p-value	x	P-value before improvement	Improved p-value	x	P-value before improvement	Improved p-value
-4	0	0.9062	-9	1	0.6753	1	0.4699	0.5904
-3	1.4746×10-6	0.5023	-8	1	0.8867	2	0.6694	0.3341
-2	0.8835	0.8835	-7	1	0.8242	3	0.7368	0.4362
-1	0.8723	0.8723	-6	1	0.7319	4	0.7735	0.4479
1	0.6115	0.6115	-5	1	0.6996	5	0.7974	0.4600
2	0.6080	0.6080	-4	1	0.4945	6	0.8146	0.3304
3	0.6004	0.6004	-3	1	0.2828	7	0.8276	0.2092
4	0.0650	0.0650	-2	1	0.3772	8	0.8380	0.3248
-	-	-	-1	1	0.4776	9	0.8465	0.3802

TABLE 3. Sensitivity of encryption algorithm keys.

Indicators		Lena image	Clock image	Pepper image	Theoretical value
x0	NPCR	98.6132	98.6121	98.6131	98.6133
	UACI	33.1280	33.1292	33.1274	33.1289
y0	NPCR	98.6126	98.6132	98.6133	98.6133
	UACI	33.1279	33.1291	33.1288	33.1289
z0	NPCR	98.6125	98.6118	98.6123	98.6133
	UACI	33.1282	33.1284	33.1283	33.1289
w0	NPCR	98.6115	98.6133	98.6132	98.6133
	UACI	33.1288	33.1286	33.1284	33.1289
r1	NPCR	98.6135	98.6133	98.6134	98.6133
	UACI	33.1295	33.1289	33.1302	33.1289
r2	NPCR	98.6133	98.6136	98.6127	98.6133
	UACI	33.1289	33.1290	33.1291	33.1289
r3	NPCR	98.6128	98.6133	98.6125	98.6133
	UACI	33.1283	33.1286	33.1293	33.1289

the plaintext-related image, image information should be presented as little as possible. Figure 7 shows the statistical histogram of the proposed plaintext-related IE used in this experiment. Sub-Figures (a) to (c) show the statistical histograms of the plaintext images and sub-Figures (d) to (f) show the statistical histograms of the ciphertext images for the Lena, Clock, and Pepper images. From the Figure, the statistical histogram of the plaintext images of Lena, Clock, and Pepper fluctuates greatly, indicating that they contain a lot of image information. In contrast, the statistical histogram



(a) Horizontal direction of plaintext

(b) Vertical direction of plaintext

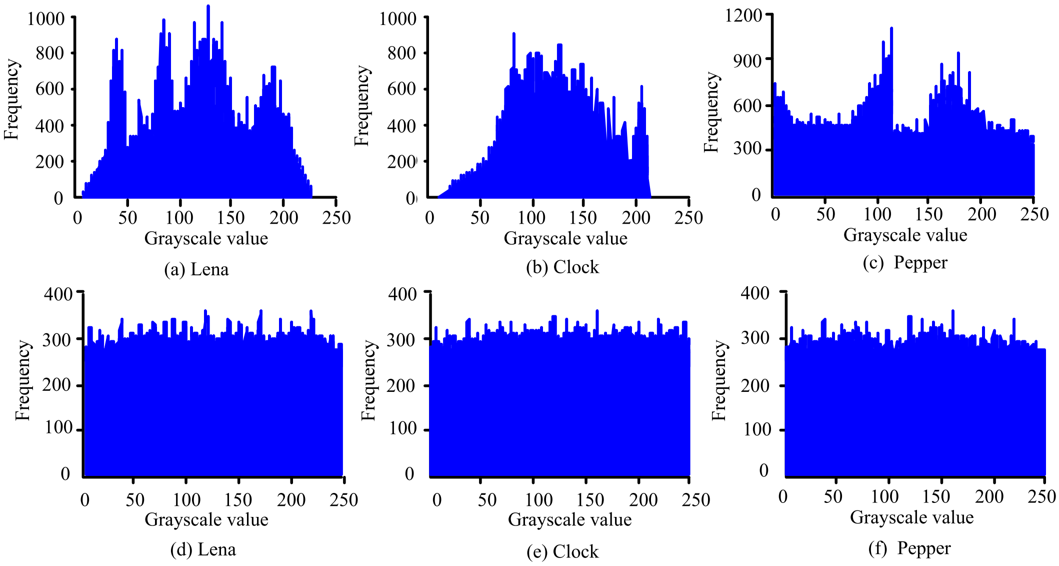
(c) Diagonal direction of plaintext

(a) Horizontal direction of ciphertext

(b) Vertical direction of ciphertext

(c) Diagonal direction of ciphertext

FIGURE 6. **Related situation of Lena image.**



(a) Lena

(b) Clock

(c) Pepper

(d) Lena

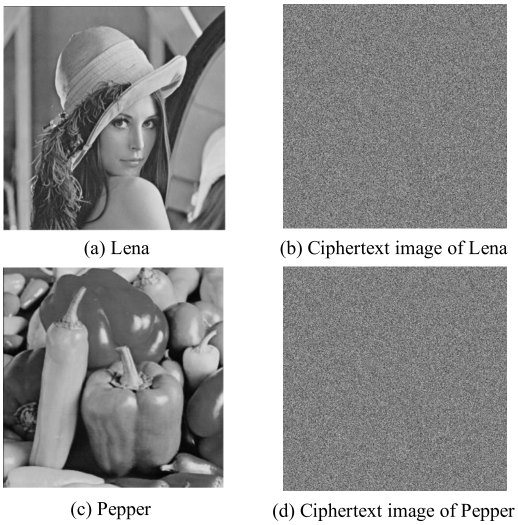
(e) Clock

(f) Pepper

FIGURE 7. **Histogram of a plaintext image and ciphertext image.**

of the ciphertext images of Lena, Clock, and Pepper is much smoother, indicating a more uniform distribution of pixels and less image information. This may be because the improved encryption method involves scrambling, diffusion processing, and bit rearrangement. It enlarges the range of parameters and improves its ergodicity, and improves the randomness and distribution uniformity of chaotic systems. The proposed plaintext-related IE algorithm based on the improved logistic mapping and hyperchaotic system has high security.

To observe the encryption effect of the improved plaintext associated image encryption algorithm more intuitively, the Lena plaintext associated image and Pepper plaintext associated image are shown as examples in Figure 8. Among them, sub-graph (a) is the Lena plaintext associated image, and sub-graph (b) is the encrypted result of the Lena plaintext associated image. Sub-image (c) shows the Pepper plaintext associated image, and sub-image (d) shows the encrypted result of the Pepper plaintext associated image. From the Figure, after being processed by the improved



(a) Lena

(b) Ciphertext image of Lena

(c) Pepper

(d) Ciphertext image of Pepper

FIGURE 8. Display of encryption results.

plaintext associated image encryption algorithm, both the Lena plaintext associated image and the Pepper plaintext associated image are displayed as noisy images. Combining the histogram, encryption result graph, and adjacent pixel correlation results mentioned above, the encrypted ciphertext image has a uniform pixel distribution, reducing its likelihood of being invaded.

In the analysis of resistant to differential attacks on images, the pixel change rate (NPCR) and the uniform average changing intensity (UACI) are often used to measure the effect of changing plaintext on ciphertext. NPCR can give the change rate of pixel Gray scale values in the image, and UACI can be used to calculate the average change amplitude. If the encryption algorithm has strong resistance to differential attacks, the sensitivity of the key and plaintext will be stronger. Table 3 shows the key sensitivity of the proposed encryption algorithm used in this experiment. The UACI and NPCR indicator values of this encryption method are close to the theoretical values, indicating its strong resistance to differential attacks. This is because the improved plaintext encryption algorithm can evenly spread plaintext information into the ciphertext image and make subtle changes to the plaintext associated image. And subtle changes can make the information in the ciphertext irrelevant to the previous plaintext information. Therefore, this subtle change effectively improves the resistance of plaintext encryption algorithms to differential attacks.

Plaintext sensitivity is the main evaluation index of the plaintext associative IE algorithm. In this study, the sensitivity of different IE methods to the Lena, Clock, and Pepper images was compared with different sizes. The results from Table 4 show that the UACI and NPCR indicator values of the proposed method in the experiment are very close to the theoretical values. Compared with the methods in references [7], [11], and [13], the indicator values of the proposed method are closer to the theoretical values, indicating that the proposed encryption method has higher sensitivity.

The analysis results of the correlation between adjacent pixels in horizontal, vertical, and diagonal directions using different methods are also compared in the experiment, as shown in Table 5. The plaintext image has high correlation in all directions, while the ciphertext image has low correlation in all directions. Compared with other methods in the literatures, the method used in this experiment has lower correlation for the ciphertext image. This indicates that the information displayed in the image is significantly reduced after being processed by the Plaintext Associative Image Encrypting Algorithm, and the security of the encryption algorithm is higher. The results suggest that the algorithm is effective in protecting image data confidentiality.

In the transmission of images, data loss and noise can occur, which increases the difficulty of decrypting plaintext associated images. This will affect the accuracy of information transmission for plaintext associated images. In the robustness analysis of improving plaintext encrypted image algorithms, it is also necessary to verify the impact of data loss and noise during transmission on the plaintext associated image decryption process. In this experiment, some ciphertext was cut and different noises were added to simulate the transmission process of plaintext related images. In Figure 9, the Lena plaintext associated image decryption diagram after simulating the transportation process is shown. The main analysis focuses on the impact of cutting 20% in sub-graph (a), salt and pepper noise in sub-graph (b), speckle noise in sub-graph (c), and Gaussian noise in sub-graph (d) on plaintext associated image transmission. The sub-graphs (e)∼(h) represent the encryption results after processing with 20% cutting, salt and pepper noise, speckle noise, and Gaussian noise, respectively. From the Figure, after data transmission simulation, Lena plaintext associated images will be affected to a certain extent. However, the correct key information can still be displayed in the end, proving that the proposed method in the experiment has noise resistance and good robustness.

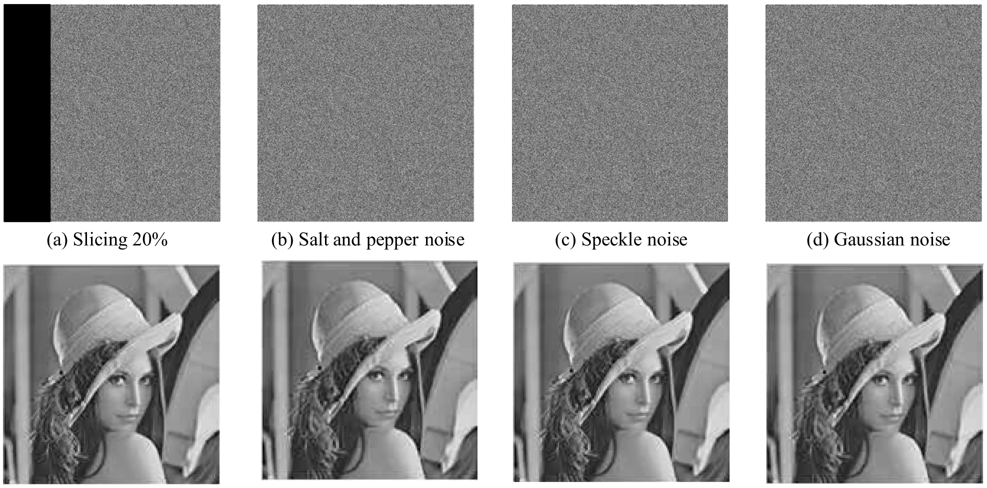
Attacks on plaintext associated images are a common means of attack in image encryption. Due to the inability of conventional plaintext associated image encryption methods to adapt to technological development, it is necessary to improve the quality of plaintext associated image encryption algorithms. Computer attackers can use the relationship analysis between theencrypted images and the plaintext associated images to decipher the image encryption algorithms, and improving the quality of the encryption algorithms can effectively prevent this situation from occurring. In the evaluation of image encryption algorithms, all white special images and all black special images can be used to evaluate the quality of encryption algorithms. The improved plaintext encryption algorithm performs both Scrambling and diffusion processing. The parameters and operational rules

TABLE 4. Test results of plaintext sensitivity of different algorithms.

Image size	NPCR(98.6133)			UACI(33.1287)		
	Lena	Clock	Pepper	Lena	Clock	Pepper
128×128	98.6072	98.6162	98.6112	33.1050	33.1144	33.0856
256×256	98.6132	98.6222	98.6171	33.1639	33.1322	33.0940
337×337	98.6110	98.6126	98.6128	33.0852	33.1249	33.0903
384×384	98.6121	98.6128	98.6131	33.1341	33.1443	33.1514
512×512	98.6130	98.6117	98.6164	33.1446	33.1147	33.1513
512×512[7]	98.6164	98.6067	98.6173	33.1266	33.1300	33.2044
512×512[11]	98.6254	98.6172	98.6166	33.1297	33.1269	33.1374
512×512[13]	98.6251	98.6078	98.6137	33.1479	33.1379	33.1312

TABLE 5. Statistical results of adjacent pixel correlation coefficient.

Image	Method	Image	Horizontal direction	Vertical direction	Diagonal direction
Lena	This paper	Plaintext	0.9659	0.9271	0.8928
		Ciphertext	0.0063	-0.0087	0.0158
	Reference[7]	Plaintext	0.9392	0.9604	0.9260
		Ciphertext	-0.0128	-0.0153	0.0198
	Reference[11]	Plaintext	0.9349	0.9357	0.9119
		Ciphertext	0.0137	0.0119	0.0401
	Reference[13]	Plaintext	0.9258	0.9224	0.9064
		Ciphertext	0.0142	0.0123	0.0412
Clock	This paper	Plaintext	0.9563	0.9179	0.8839
		Ciphertext	0.0069	0.0092	0.0173
	Reference[7]	Plaintext	0.9298	0.9508	0.9168
		Ciphertext	-0.1408	0.0168	0.0217
	Reference[11]	Plaintext	0.9255	0.9264	0.9028
		Ciphertext	-0.0151	0.0139	0.0441
	Reference[13]	Plaintext	0.9166	0.9132	0.8974
		Ciphertex	0.0156	-0.0135	0.0453
Pepper	This paper	Plaintext	0.9853	0.9457	0.9106
		Ciphertext	-0.0073	-0.0101	0.0183
	Reference[7]	Plaintext	0.9580	0.9796	0.9446
		Ciphertext	0.0147	-0.0177	0.0228
	Reference[11]	Plaintext	0.9536	0.9545	0.9301
		Ciphertext	-0.0158	0.0139	0.0463
	Reference[13]	Plaintext	0.9444	0.9408	0.9246
		Ciphertext	0.0164	-0.0147	-0.0489



(a) Slicing 20%
(b) Salt and pepper noise
(c) Speckle noise
(d) Gaussian noise
(e) Decryption result of (a)
(f) Decryption result of (b)
(g) Decryption result of (c)
(h) Decryption result of (d)

FIGURE 9. Robustness analysis of improved plaintext encrypted image algorithms.

were optimized during the Scrambling and diffusion stages, which are closely related to the plaintext. Therefore, when there are slight changes in plaintext, the improved plaintext encryption algorithm will change various operational rules. This change will result in a significant change in the quality of plaintext encryption algorithms, making it impossible to

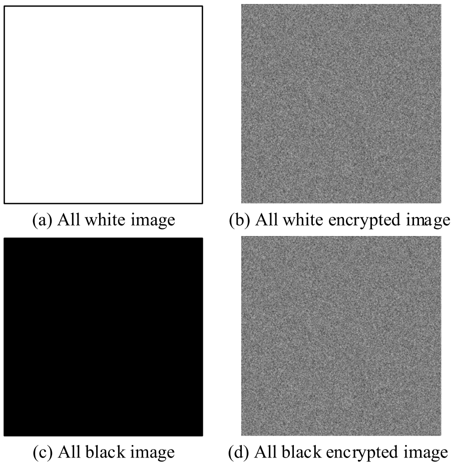

(a) All white image
(b) All white encrypted image
(c) All black image
(d) All black encrypted image

FIGURE 10. Encryption results of special images.

TABLE 6. Encryptionand decryptiontime (s).

Method	This paper	Reference[7]	Reference[11]	Reference[13]
Encryption time	1.1279	2.2786	2.8963	4.7654
Decryption time	1.2057	3.7893	2.1578	3.8107

guarantee the quality of plaintext associated image encryption algorithms. Figure 10 shows the encrypted image results of the all white special image and all black special image of the plaintext encryption algorithm in this experiment. In Figure 10, the all white special image and all black special images are both noise like images after encryption processing, and there is no significant difference between the two encrypted images. This result indicates that the improved plaintext associated image encryption algorithm can effectively resist plaintext attacks. This may be because the improved plaintext algorithm has high stability in the parameters and operational rules set during the scrambling and diffusion. Therefore, when subjected to plaintext attacks, the improved plaintext associated image encryption algorithm can maintain the stability of the plaintext, thereby ensuring the encryption quality of the plaintext encryption algorithm.

The image encryption/decryption speed is the time taken to encrypt/decrypt an image, that is, the size of the image divided by the encryption/decryption time, in bits per second. In image encryption systems, it is generally required that the encryption/decryption speed be as fast as possible. But the speed of image encryption/decryption not only depends on hardware facilities, but also on algorithm performance. The encryption and decryption times of each algorithm are shown in Table 6. Through comparative analysis, it can be seen that the algorithm has a fast encryption/decryption speed and can meet the requirements of image encryption algorithms. And the running time of this algorithm is shorter than that of other methods, which has certain advantages. This may be because the encryption algorithm proposed in the experiment includes two plaintext independent diffusion operations, one plaintext related scrambling operation, and one plaintext independent scrambling operation. Because only one scrambling operation is related to the plaintext image, the encryption speed is greatly improved, and it can effectively resist the selected or Known-plaintext attack.

The key space is a collection of all keys in an image encryption system. If the number and number of keys increase, the key space becomes larger. If the length of the key is r, then the key space is 2r. The key space size of this scheme is about 1.677×10^{64}, which is equivalent to the 213 bit Key size. When attacked by a computer, it takes approximately 10^{64} years to crack the encryption system. Therefore, the proposed scheme can effectively resist violent attacks.

Peak Signal to Noise Ratio (PSNR) is used to evaluate the quality of an image after compression compared to the original image. The higher the PSNR, the smaller the distortion after compression, and the better the effect. After calculation, it can be obtained that the peak signal-to-noise ratio of the encrypted image to the original image is very high. The PNSR of the Lena image is as high as 69.87 dB, and the lowest Clock image also reaches 55.23 dB. And the PSNR between the restored image and the original image is $+\infty$. It shows that this algorithm can extract data that is completely consistent with the original data. And it can fully restore the original image, achieving complete reversibility.

The improved plaintext associative IE algorithm has high sensitivity, security, and chaos. However, there are still some shortcomings in the experiment. The running speed of the improved encryption method has not been tested. Next,the study will consider increasing the testing indicators to improve the performance of the improved method while ensuring its computational efficiency and security. In addition, only gray plaintext associative images were studied in the experiment, and the next step will consider studying colored plaintext associative images.

V. CONCLUSION

The technology advancement has led to the expansion of the use and exchange of digital data, which places great importance on the security of these data. In text and image encryption technology, researchers use techniques such as DNA encoding to enhance their ability to resist plaintext and other attacks [29], [30] and [31]. Chaos system is an important encryption strategy in image encryption methods. Logistic mapping is a mapping method commonly used in chaotic system applications. The chaotic system based on logistic mapping has high chaotic performance and improves the security of the system [31]. Although these technologies have achieved good application results in image encryption, a single encryption method cannot guarantee high image security. Based on chaotic encryption technology, there is a problem of insecurity when scrambling images. Therefore, the experiment will combine logical mapping with hyperchaotic systems. The combined method can improve the chaotic characteristics, ergodicity, initial value sensitivity and Pseudorandomness of chaotic systems. In IE algorithms, the sensitivity of parameters, initial values, and image security are important factors to be considered for improving and optimizing encryption methods. Therefore, this study usedlogistic map and improved it, and combined it with CS for the research of Plaintext Associative IE algorithm. In the validation experiment, the improved logistic map can traverse and distribute uniformly in the space of (0,1) for all parameters, and the Lyapunov exponent of the improved map is greater than 21.5. The correlation coefficient of the encrypted image pixels after encryption processing is less than 0.05. For Lena, Clock and Pepper plaintext images, the UACI index of the improved Plaintext Associative IE method is 98.6130, 98.6117, and 98.6164 respectively, and the NPCR index is 33.1446, 33.1147, and 33.1513 respectively. Both of them are close to the theoretical values of UACI and NPCR indices, which are 98.6133 and 33.1287. In Lena, Clock, and Pepper images, the correlation coefficients of the encrypted image pixels are all less than 0.02 in different directions of the improved method. The experimental results show that the improved plaintext associated image encryption method overcomes the limitations of traditional image and text encryption techniques in terms of parameter range, slow encryption speed, and uneven chaotic sequences. The improved plaintext associative IE algorithm has high sensitivity, security, and chaos.

REFERENCES

[1] Y. Ban, Y. Ban, M. Liu, P. Wu, B. Yang, S. Liu, L. Yin, and W. Zheng, "Depth estimation method for monocular camera defocus images in microscopic scenes," *Electronics*, vol. 11, no. 13, pp. 2012–2126, 2022, doi: 10.3390/electronics11132012.

[2] X. Liu, Z. Li, X. Fu, Z. Yin, M. Liu, L. Yin, and W. Zheng, "Monitoring house vacancy dynamics in the pearl river delta region: A method based on NPP-VIIRS night-time light remote sensing images," *Land*, vol. 12, no. 4, pp. 831–851, 2023, doi: 10.3390/land12040831.

[3] S. Lu, Y. Ding, M. Liu, Z. Yin, L. Yin, and W. Zheng, "Multiscale feature extraction and fusion of image and text in VQA," *Int. J. Comput. Intell. Syst.*, vol. 16, no. 1, pp. 54–64, Apr. 2023, doi: 10.1007/s44196-023-00233-6.

[4] R. Wang, M. Y. Li, and H. J. Luo, "Exponential sine chaotification model for enhancing chaos and its hardware implementation," *Chin. Phys. B*, vol. 31, no. 8, pp. 337–346, 2022.

[5] F. Zhang, Z. Huang, L. Kou, Y. Li, M. Cao, and F. Ma, "Data encryption based on a 9D complex chaotic system with quaternion for smart grid," *Chin. Phys. B*, vol. 32, no. 1, pp. 217–226, 2023.

[6] R. Hasimoto-Beltran, M. D. Calderon-Calderon, and V. H. Olavarría-Jaramillo, "Secure real-time chaotic partial encryption of entropy-coded multimedia information for mobile devices: Smartphones," *IEEE Access*, vol. 10, pp. 15876–15890, 2022.

[7] Z. Hua, Z. Zhu, S. Yi, Z. Zhang, and H. Huang, "Cross-plane colour image encryption using a two-dimensional logistic tent modular map," *Inf. Sci.*, vol. 546, pp. 1063–1083, Feb. 2021.

[8] O. Z. Akif, S. Ali, R. S. Ali, and A. K. Farhan, "A new pseudo-random bits generator based on a 2D-chaotic system and diffusion property," *Bull. Electr. Eng. Informat.*, vol. 10, no. 3, pp. 1580–1588, Jun. 2021.

[9] B. Khokhar, S. Dahiya, and K. P. S. Parmar, "Load frequency control of a microgrid employing a 2D sine logistic map based chaotic sine cosine algorithm," *Appl. Soft Comput.*, vol. 109, Sep. 2021, Art. no. 107564.

[10] X. Wang, N. Guan, and J. Yang, "Image encryption algorithm with random scrambling based on one-dimensional logistic self-embedding chaotic map," *Chaos, Solitons Fractals*, vol. 150, Sep. 2021, Art. no. 111117.

[11] X. Li, J. Mou, Y. Cao, and S. Banerjee, "An optical image encryption algorithm based on a fractional-order laser hyperchaotic system," *Int. J. Bifurcation Chaos*, vol. 32, no. 3, Mar. 2022, Art. no. 2250035.

[12] W. Yan and Q. Ding, "A novel S-box dynamic design based on nonlinear-transform of 1D chaotic maps," *Electronics*, vol. 10, no. 11, pp. 1313–1323, 2021.

[13] J. Zheng and H. Hu, "A highly secure stream cipher based on analog-digital hybrid chaotic system," *Inf. Sci.*, vol. 587, pp. 226–246, Mar. 2022.

[14] K. Jain, A. Aji, and P. Krishnan, "Medical image encryption scheme using multiple chaotic maps," *Pattern Recognit. Lett.*, vol. 152, pp. 356–364, Dec. 2021.

[15] S. Kanamaru, Y. Shimada, K. Fujiwara, and T. Ikeguchi, "Performance evaluation of chaotic random numbers generated from responses of integer logistic maps," *Nonlinear Theory Appl.*, vol. 12, no. 3, pp. 489–499, 2021.

[16] D. Aleja, A. Inmaculada, and J. López-Gómez, "Characterizing the existence of positive periodic solutions in the weighted periodic-parabolic degenerate logistic equation," *Discrete Continuous Dyn. Syst., B*, vol. 28, no. 2, pp. 1471–1479, 2023.

[17] C. Fan, Q. Ding, and C. K. Tse, "Evaluating the randomness of chaotic binary sequences via a novel period detection algorithm," *Int. J. Bifurcation Chaos*, vol. 32, no. 5, Apr. 2022, Art. no. 2250075.

[18] J. Yu, C. Li, X. Song, S. Guo, and E. Wang, "Parallel mixed image encryption and extraction algorithm based on compressed sensing," *Entropy*, vol. 23, no. 3, pp. 278–298, 2021, doi: 10.3390/e23030278.

[19] H. Zheng and Y. Xia, "Chaotic threshold of a class of hybrid piecewise-smooth system by an impulsive effect via Melnikov-type function," *Discrete Continuous Dyn. Syst.-B*, vol. 27, no. 11, pp. 6353–6371, 2022, doi: 10.3934/dcdsb.2021319.

[20] V. Sangavi and P. Thangavel, "An exalted three dimensional image encryption model availing a novel twin attractor chaotic system," *Proc. Comput. Sci.*, vol. 204, pp. 728–735, Jan. 2022, doi: 10.1016/j.procs.2022.08.088.

[21] I. Yasser, A. T. Khalil, M. A. Mohamed, A. S. Samra, and F. Khalifa, "A robust chaos-based technique for medical image encryption," *IEEE Access*, vol. 10, pp. 244–257, 2022, doi: 10.1109/ACCESS.2021.3138718.

[22] V. R. F. Signing, T. F. Fonzin, M. Kountchou, J. Kengne, and Z. T. Njitacke, "Chaotic jerk system with hump structure for text and image encryption using DNA coding," *Circuits, Syst., Signal Process.*, vol. 40, no. 9, pp. 4370–4406, Sep. 2021, doi: 10.1007/s00034-021-01665-1.

[23] X. Liu, X. Tong, Z. Wang, and M. Zhang, "A new n-dimensional conservative chaos based on generalized Hamiltonian system and its' applications in image encryption," *Chaos, Solitons Fractals*, vol. 154, Jan. 2022, Art. no. 111693, doi: 10.1016/j.chaos.2021.111693.

[24] L. Xu and J. Zhang, "A novel four—Wing chaotic system with multiple attractors based on hyperbolic sine: Application to image encryption," *Integration*, vol. 87, no. 1, pp. 313–331, 2022, doi: 10.1142/S0218127422501917.

[25] X. An, Z. Meng, Y. Wang, and J. Sun, "Design of a single-channel chaotic secure communication system implemented by DNA strand displacement," *ACS Synth. Biol.*, vol. 11, no. 2, pp. 843–854, Feb. 2022, doi: 10.1021/acssynbio.1c00509.

[26] R. W. Ibrahim, H. Natiq, A. Alkhayyat, A. K. Farhan, N. M. G. Al-Saidi, and D. Baleanu, "Image encryption algorithm based on new fractional beta chaotic maps," *Comput. Model. Eng. Sci.*, vol. 132, no. 1, pp. 119–131, 2022, doi: 10.32604/cmes.2022.018343.

[27] J. Zhang, S. Peng, Y. Gao, Z. Zhang, and Q. Hong, "APMSA: Adversarial perturbation against model stealing attacks," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 1667–1679, 2023, doi: 10.1109/TIFS.2023.3246766.

[28] Z. Guan, J. Jing, X. Deng, M. Xu, L. Jiang, Z. Zhang, and Y. Li, "DeepMIH: Deep invertible network for multiple image hiding," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 45, no. 1, pp. 372–390, Jan. 2023, doi: 10.1109/TPAMI.2022.3141725.

[29] J. S. Khan, J. Ahmad, S. F. Abbasi, and S. K. Kayhan, ''DNA sequence based medical image encryption scheme,'' in *Proc. 10th Comput. Sci. Electron. Eng. (CEEC)*, Sep. 2018, pp. 24–29.

[30] J. S. Khan, J. Ahmad, S. S. Ahmed, H. A. Siddiqa, S. F. Abbasi, and S. K. Kayhan, ''DNA key based visual chaotic image encryption,'' *J. Intell. Fuzzy Syst.*, vol. 37, no. 2, pp. 2549–2561, Sep. 2019.

[31] S. F. Abbasi, J. Ahmad, J. S. Khan, M. A. Khan, and S. A. Sheikh, ''Visual meaningful encryption scheme using intertwinning logistic map,'' in *Proc. Sci. Inf. Conf.* Cham, Switzerland: Springer, 2019, pp. 764–773.

DANDAN HE was born in Henan, China, in 1985. She received the M.S. degree in signal and information processing from Zhengzhou University, Zhengzhou, China, in 2012.

Since 2012, she has been a Lecturer with Pingdingshan University, Henan. Her professional title is Lecturer. She has published more than ten articles. Her research interests include artificial intelligence and image processing.

RAJAMOHAN PARTHASARATHY was born in India.

He is currently a Ph.D. Supervisor with the Faculty of Engineering, Built Environment and Information Technology, SEGi University, Kota Damansara, Malaysia. His professional title is Associate Professor of computer networks and security. His research interests include cyber security, cloud computing and security, wireless communication and security, client server computing technology, web server technology, the IoT, and IR 4.0.

HONG LI was born in Chongqing, China, in 1981. She received the M.S. degree in signal and information processing from Harbin University, Harbin, China, in 2010.

Since 2012, she has been a Lecturer with Pingdingshan University, Henan. Her professional title is Lecturer. She has published more than ten articles. Her research interests include embedded system development and image processing based on deep learning.

ZEXUN GENG was born in Mengzhou, Henan, China, in 1958. He received the degree from the Department of Remote Sensing Information Engineering, PLA College of Geodesy and Mapping, in September 1996, and the Ph.D. degree in engineering, in December 1996.

He was promoted to Professor, in 2002. In September 2017, he was with the School of Information Engineering, Pingdingshan University. He was engaged in adaptive optical image processing research. He is an Expert in the evaluation of major projects for Earth observation of the Ministry of Science and Technology and an Expert in the evaluation of projects funded by the National Natural Science Foundation. He is a member of the Chinese Society of Image and Graphics.