Computer Image Encryption Technology Based on Chaotic Sequence Algorithm

Li Shen
School of Finance and Economics, Xuchang Vocational Technical College, Xuchang, 461000, China

***Abstracts*—With the wide application of computer images and the popularization of network transmission, the public demand for image encryption technology is becoming more and more urgent. Privacy and data security can be effectively guaranteed through image encryption, but the existing encryption technology still has problems such as high overhead and poor encryption performance. Therefore, in order to improve the processing efficiency of encryption technology, the study constructs a two-dimensional composite chaotic system based on the analysis of existing chaotic sequence algorithms. Additionally, a novel approach to picture encryption is put forth by merging the composite chaotic system following the algorithmic optimization of disruption and diffusion in the image encryption phase. The chaotic mapping performed best, according to the experimental results, when the chaotic system's parameters were between 10 and 75. At this time, the algorithm had the highest encryption speed of 632 Mbit/s and decryption speed of 583 Mbit/s, the lowest resource consumption rate of 21.4% and the lowest delay rate of 11.5%. It can be seen that the method proposed in the study shows significant advantages in terms of security and effectiveness of image encryption, and is capable of realizing high-quality encryption of computer images. The novel image encryption technique that the research proposed has a high degree of security and feasibility and can achieve high-quality encryption of computer images.**

Keywords—Chaotic sequence algorithm; image encryption; mapping effect; pixel code; security

I. Introduction

With the development of the digital era, computer image encryption (IE) technology has become an important part of the information security field [1]. In addition to safeguarding data integrity and privacy, Internet Explorer is essential in a variety of industries, including communication, the military, and the medical industry. Traditional IE methods, such as symmetric encryption and asymmetric encryption, although effective in some cases, still have limitations when facing advanced attacks [2]. In light of the foregoing context, numerous IE algorithms have been presented by domestic and international researchers to further safeguard the confidentiality and integrity of images. For example, multi-level encryption, high standard encryption, watermark encryption, machine learning encryption, etc. [3]. Although these methods have made significant progress in securing images, there are still some challenges, such as performance security and encryption effectiveness. In recent years, IE algorithms utilizing chaotic sequences have attracted much attention due to their high degree of randomness, complexity, and attack resistance [4]. There are few IE studies on this algorithm, but the algorithm always suffers from the problems of sensitive initial conditions, large performance overhead, and difficult security evaluation. Therefore, this research innovatively proposes a new two-dimensional composite chaotic system and optimizes the disruption and diffusion steps in the image encryption process, aiming to improve the security and processing efficiency of image encryption. The goal of the research is to construct a more efficient and secure image encryption method by optimizing the chaotic algorithm. The research is expected to construct a new computerized image encryption method to provide a new direction for the development of technology in this field. This study is organized into four sections: the first summarizes and analyzes the work of others; the second describes the construction of the new chaotic system and encryption algorithm (EA); the third evaluates the new algorithm's performance; and the fourth is a summary of the article.

II. Related Works

Computer IE technology plays a crucial role in today's information security field. To safeguard picture data securely and privately, researchers have been looking for more dependable and effective encryption techniques. After merging structured phase coding, Shikder et al. presented a revolutionary binary IE approach to further improve the encryption impact of existing computer images. According to experimental findings, this method of encoding data can be used to decrypt data without noise and can withstand atmospheric turbulence over short propagation lengths [5]. Zhang et al. used bit plane decomposition and image hashing to create a dynamic DNA-encoded multiple image IE technique that secures the content of multiple images while increasing network transmission speed. The algorithm features a huge key space, strong key sensitivity, strong security, and robustness, as shown by the experimental results [6]. To lessen the shortcomings of the current medical IE algorithms, such as their lack of security and tamper-resistant techniques Man et al. included a self-validating matrix before proposing a tamper-resistant EA for medical photos. According to experimental data, the technique locates at least four pixels accurately, provides good encryption, and has strong tamper-resistance [7]. A bit-level IE approach that makes use of random alteration of edge pixels was proposed by Sheng et al. in order to improve the cryptosystem's security and, therefore, the IE outcomes. According to experimental results, the approach is very successful and resistant against popular assaults such noise attacks, data loss attacks, and differential attacks [8].

The chaos theory-based CSA algorithm generates random numbers. Through extremely complicated and unexpected repetitive operations, the algorithm generates a succession of seemingly random values by taking use of the nonlinear character of chaotic systems and the strong dependence on beginning conditions. To advance the security and sensitivity of the initial parameter selection of traditional chaotic systems in IE, Balaska et al. proposed a novel IE method after combining two-dimensional Zaslavsky chaotic mapping (CM) and cryptographic algorithms. The approach is quite dependable and successful for encrypting photos of any size or type, according to experimental data [9]. To improve the randomness of the key space, Jia et al. proposed a pixel image cross-color obfuscation method after combining the cross-color field obfuscation method. The experimental results demonstrated that the approach is robust against differential, known plaintext, selective ciphertext, selected plaintext, and brute force attacks [10]. Sheng et al. used chaotic sequences with neural networks to offer a unique image chaotic encryption method that improves the security of the IE system. The experimental results demonstrated that the method showed superior security under multiple attack environments [11]. Song et al. proposed a composite chaotic system. The experimental results demonstrated the higher security and strong practicality of the system applied in IE [12].

In summary, existing image encryption techniques have made some progress in protecting data security and privacy, but there are still some limitations. For example, the robust effectiveness problem of the techniques, the performance overhead problem and applicability problem when facing large-scale image data. In addition chaotic sequence algorithms have gained attention for their high complexity and unpredictability, but the traditional methods are still deficient in initial parameter selection and key space randomization. The proposed research aims to overcome these limitations by constructing a new two-dimensional composite chaotic system and optimizing the disruption and diffusion steps in the image encryption process. Continuing to optimize the algorithm with security as the main direction, innovative improvements are made to the chaotic system and its sequence generation, as well as the disruption and diffusion algorithms during the encryption process, and finally, a new image encryption method is proposed.

III. Computerized Image Encryption Algorithm Based on Improved CSA

The study firstly enumerates the common one-dimensional CMs and combines two of the more adaptable mappings to propose a novel two-dimensional composite chaotic system. In addition, the key steps of disruption and diffusion in the IE process are algorithmically optimized, and finally, a novel encryption method is proposed.

A. *Optimization of Two-Dimensional Composite Chaotic Systems for CSA*

The application of CSA in computer IE techniques usually involves the use of pseudo-random sequences generated by chaotic systems to encrypt images. At the heart of these algorithms are CMs that have sensitive initial conditions and parameters that make the output sequence random [13]. Some common CMs are Logistic mapping, Henon mapping, etc. These equations describe the law of system state evolution over time, and the chaotic nature makes the output sequence show highly random and complex characteristics. Among them, the schematic diagram of Logistic mapping is shown in Fig. 1.

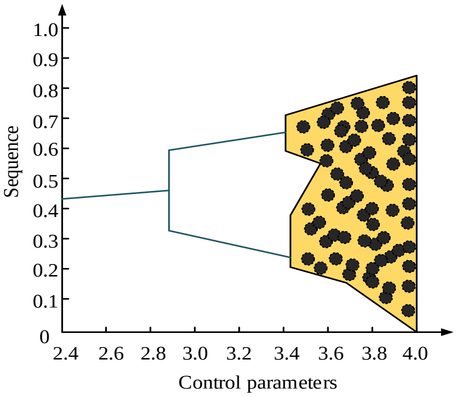


Fig. 1. Schematic diagram of logistic mapping.

In Fig. 1, the population's periodicity is represented by the vertical axis, while a parameter in the logistic mapping function is shown by the horizontal axis. When this parameter is changed, the behavior of the population bifurcates, changing from a steady state to various complex patterns between periodicity, chaos, or periodicity. When the parameter is 4, the Logistic mapping is more homogeneous at this point, and the system goes into equilibrium [14]. The formula for the Logistic mapping is shown in Eq. (1).

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

In Eq. (1), x_n denotes the value of the current iteration. r is the system parameters and n is the iterations. The Henon mapping is a two-dimensional mapping that is commonly used to generate fractal patterns and study chaotic dynamics. Its iteration formula is shown in Eq. (2).

$$\begin{cases} x_{n+1} = y_n - a x_n^2 + 1 \\ y_{n+1} = b x_n \end{cases} \tag{2}$$

In Eq. (2), x_n and y_n denote the two variable values of the Henon mapping at the n th iteration. x_{n+1} and y_{n+1} denote the two variable values of the mapping at the next iteration step, respectively. Both a and V denote the parameters of the Henon mapping. Eq. (3) displays the Arnold mapping formula.

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} mod1 \tag{3}$$

In Eq. (3), x_n and y_n denote the values of the two variables of the Arnold mapping at iteration n. $mod\ 1$ denotes that the result is taken modulo 1, i.e., only the fractional part is retained. The Chebyshev mapping is a one-dimensional mapping based on Chebyshev polynomials in various forms, but the most commonly used are first-order and second-order mappings. Its mapping bifurcation diagram is shown in Fig. 2.

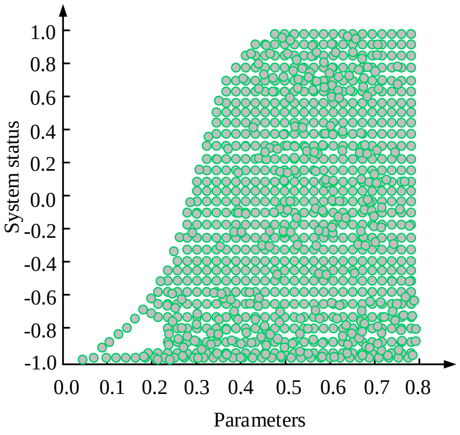


Fig. 2. Chebyshev map bifurcation diagram.

In Fig. 2, the branching points on the bifurcation map indicate the parameter values. Through the bifurcation maps, the parameter ranges of the Chebyshev mapping and the fact that the mapping exhibits chaotic properties can be determined, and in addition, it can be observed how chaos emerges from stable periodic trajectories. Thus, it can be said that the Chebyshev mapping can be used to understand and study the behavior of nonlinear dynamical systems and the relationship between chaos and periodic trajectories. The general form of his mapping is shown in Eq. (4).

$$\begin{aligned} x_{n+1} &= a - y_n^2 + x_n^2 \\ y_{n+1} &= b + 2x_n y_n \end{aligned} \tag{4}$$

In Eq. (4), x_n and y_n denote the values of the two variables of the Chebyshev mapping at iteration n. Both a and b denote the parameters of the Chebyshev mapping. The higher order mapping is shown in Eq. (5).

$$T_n(x) = -T_{n-2}(x) + 2xT_{n-1}(x) \tag{5}$$

In Eq. (5), $T_n(x)$ denotes the $T_n(x)$ th order Chebyshev polynomial and x denotes the current iteration value. The iterative process of Chebyshev mapping produces diverse trajectories and is suitable for studying the unpredictability and complexity of nonlinear systems [15]. Its adjustable parameters allow exploring the variation of the system behavior under different conditions and help to understand the sensitivity of chaotic systems. Iterative mapping, also known as iterative mapping, is a mathematical model that describes the evolution of a system's state in discrete time steps. Fig. 3 displays the Iterative mapping phase space diagram.

The complicated, non-periodic structure of the entire phase space map in Fig. 3 suggests that the system is in a chaotic state. On the other hand, the central points in the region exhibit a rather homogenous behavior, suggesting a tendency toward stability in the system's function. The general form of the mapping is shown in Eq. (6).

$$x_{n+1} = f(x_n) \tag{6}$$

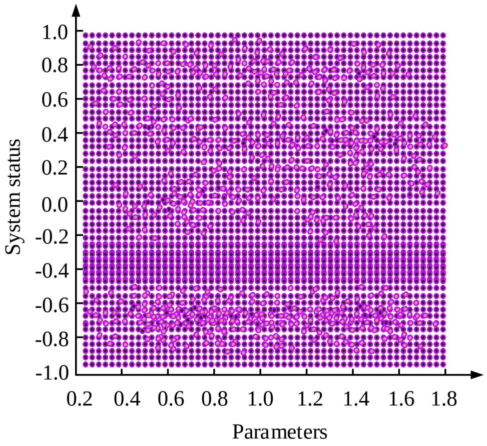


Fig. 3. Iterative mapping phase space graph.

In Eq. (6), f denotes a mapping function. The Iterative mapping describes the evolution of the system in discrete time steps rather than continuous time. Although both Chebyshev mapping and Iterative mapping show superior performance, the phase space structure of a chaotic system that is always in one dimension when mapping a sequence of images is usually limited and does not capture the complex evolution of the system well [16]. At the same time a one-dimensional system can only vary along one direction, which may not adequately represent the interactions and effects of multiple variables. Consequently, the study attempts to integrate the two, at which point Eq. (7) displays the expression of the 2D composite CM.

$$\begin{cases} x_n = \sin(\dfrac{t}{x_{n-1}}) \times \cos(k \cdot \arccos y_{n-1}) \\ y_n = \sin(\dfrac{k}{x_{n-1}}) \times \cos(a \cdot \arccos y_{n-1}) \end{cases} \tag{7}$$

In Eq. (7), t and k denote the control parameters of the two-dimensional composite CM, respectively, and n denotes the number of iterations. The new system's complexity and sequence randomness are increased by switching the control parameters of Iterative mapping and Chebyshev mapping. Additionally, the mapping function introduces mutual interference between x_{n-1} and y_{n-1}, which increases the unpredictability of CM. The qualities of both are combined in the new system, along with two control parameters that can be utilized as the EA's key. As the key increases, the IE algorithm's key space expands correspondingly.

B. An Optimized Composite Chaotic System is the Basis for the Image Encryption Technique

The unpredictability and randomness of chaotic systems introduce a new encryption means for IE. By reasonably selecting the CM model, initialization parameters and key expansion process, key sequences with a high degree of randomness can be generated. These sequences can be applied to the change of pixel values and position coordinates, thus realizing effective encryption without destroying the perceived quality of the image. The chaotic IE process is shown in Fig. 4.

In Fig. 4, first chaotic IE uses chaotic system to generate random key and encrypt the plaintext image by disruption and diffusion methods. After the ciphertext image is generated, decryption can be realized by the same key and reverse process to ensure security and reversibility. Among them, the scrambling and diffusion module is the main way to guarantee the security and effectiveness of EA. Disordering is a process to increase the complexity and randomness of encryption by changing the position or arrangement order of pixel values in IE. There may be shortcomings in some cases, such as challenges in providing sufficient randomness and uniform distribution. In order to optimize the disruption process, the study introduces a phantom square matrix for optimization, at which point the disruption process is shown in Fig. 5 [17].

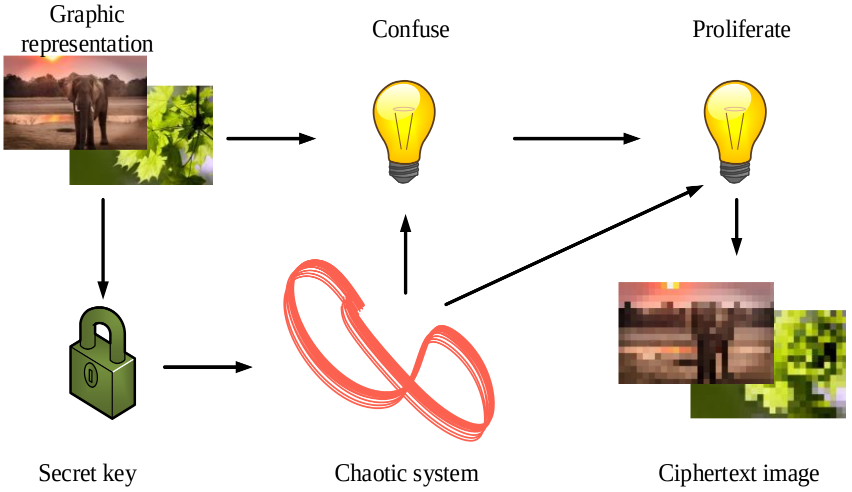
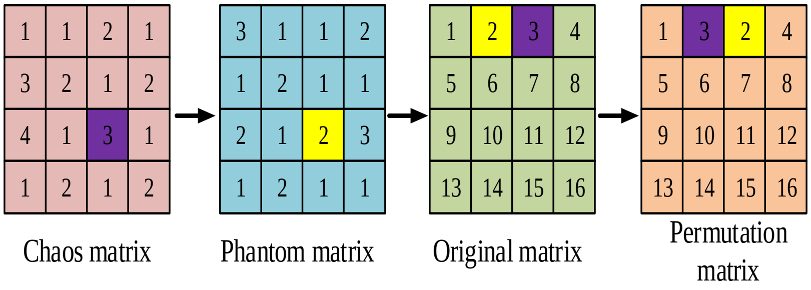


Fig. 4. Chaos image encryption process.



Chaos matrix

1	1	2	1
3	2	1	2
4	1	3	1
1	2	1	2

Phantom matrix

3	1	1	2
1	2	1	1
2	1	2	3
1	2	1	1

Original matrix

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Permutation matrix

1	3	2	4
5	6	7	8
9	10	11	12
13	14	15	16

Fig. 5. The process of scrambling the magic cube.

In Fig. 5, for any point in the initial chaos matrix, i.e., the purple region in the figure. After reading the coordinates of this region, the region with corresponding coordinates, i.e., the yellow region, is found in the phantom square matrix for replacement. Once this is done, the coordinates of the yellow box in the phantom matrix are then used to find the location of the corresponding box in the original text matrix. Finally, the values of the boxes in the chaos matrix and the phantom matrix are replaced into the original matrix to obtain a new matrix, thus completing the substitution operation. The formula of the phantom matrix is shown in Eq. (8).

$$H = floor(\sqrt{M \times N})+1 \tag{8}$$

In Eq. (8), H denotes the phantom square matrix and $M \times N$ denotes the size dimension of the picture. The formula for transforming from chaos matrix to phantom square matrix is shown in Eq. (9).

$$X_i = (floor(|X_i \times 10^8) \bmod N)+1 \tag{9}$$

In Eq. (9), X_i denotes the i th random for sequence. From this equation, the phantom matrix can be transformed into one-dimensional form, and the chaotic sequence is randomly converted into a chaotic matrix of a given size. Row permutation then reads the row information in the chaotic matrix and then replaces it with the rows in the original matrix, and repeats the operation until all the elements are replaced. Eq. (10), which represents this process' formula, is displayed.

$$B(i, y_{ij}) \leftrightarrow B(i, H1(y_{ij})) \tag{10}$$

In Eq. (10), $B(i, y_{ij})$ denotes the row element position coordinates in the chaos matrix and $B(i, H1(y_{ij}))$ denotes the row element position coordinates in the original text matrix. After completion, the reference row disarrangement is sequentially followed by column disarrangement until all the original text matrix information is replaced. Moreover, to ensure the correlation and security between the image pixel information after the disarrangement operation, the study further introduces the quadtree method to optimize the diffusion operation. First of all, pseudo-random sequence generation is carried out by the improved chaotic system for any disambiguation image, and matrix information calculation is carried out after reading the image pixel information, and the binary matrix information is transformed into a one-dimensional matrix for conversion. After completion, the pseudo-random sequence selection is performed in quadtree coding [18]. The selected pseudo-random sequence is then bit-swapped, and the above operation is repeated until all pixel values are permuted. Next, the DNA is encoded and computed using a quadtree algorithm. Lastly, the encoded DNA is sorted and decoded using the sort function, and the resulting ciphertext image is created by combining the decoded DNA. The calculation formula for the transformation of its mid-range information is shown in Eq. (11).

$$x^*_{n`} = \mathrm{mod}(floor(s_{ij} * 10^{n`}), 10) \tag{11}$$

In Eq. (11), $n`$ denotes the read bit of the dislocation matrix, s_{ij} denotes the value of the chaos matrix, and the constant denotes decimal. The calculation formula for bit-bit conversion is shown in Eq. (12).

$$p_{ij}(h) \leftrightarrow p_{ij}(10 - q_{n`}) \tag{12}$$

In Eq. (12), $p_{ij}(h)$ is the h th value in the permutation matrix and $q_{n`}$ is the $n`$th value in the quadtree encoding rule. The formula for DNA coding is shown in Eq. (13).

$$p_{ij}(h) = DNA\_encode(p, s(n`)) \tag{13}$$

In Eq. (13), p denotes the matrix to be encoded, i.e., the transformed chaos matrix of the quadtree rule. $s(n`)$ denotes the coding rule corresponding to this matrix. Combining the optimized chaotic system and the above optimized improvements of the dislocation and diffusion methods respectively, the study proposes a novel computer IE method, the encryption flow of which is shown in Fig. 6.

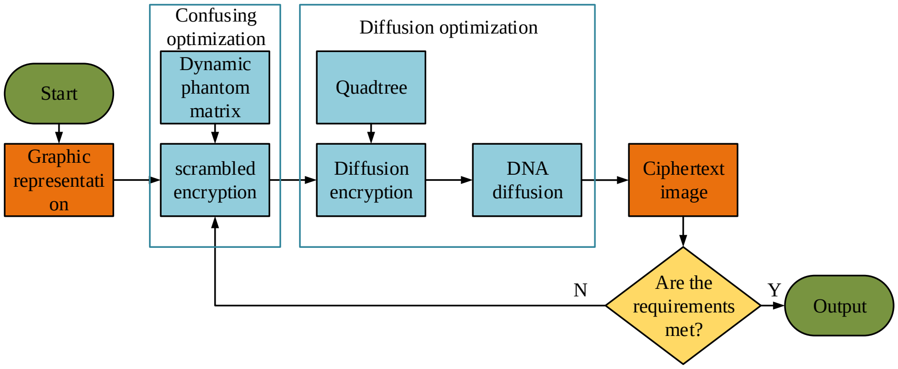


Fig. 6. New image encryption algorithm process.

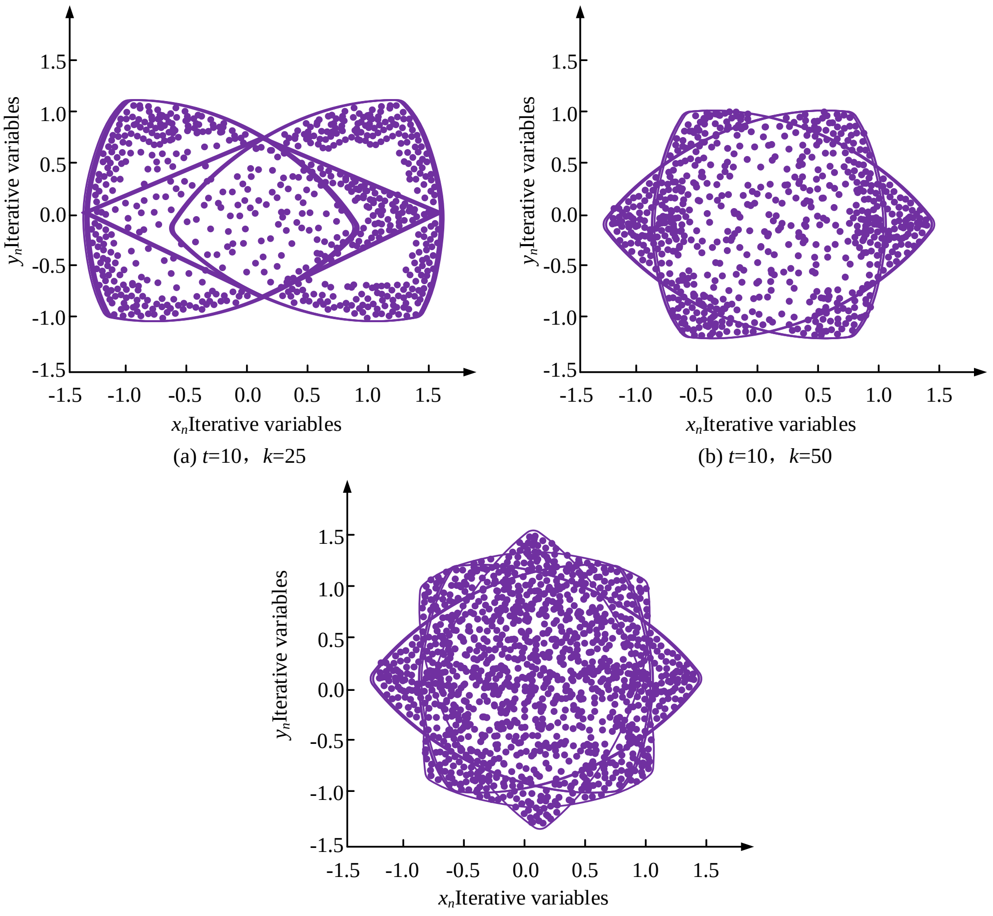
From Fig. 6, the flow of the method pair includes four modules: plaintext image input, dynamic phantom matrix optimization disruption, quadtree segmentation, DNA diffusion optimization diffusion, and ciphertext image generation. Firstly, a phantom matrix with dynamics is introduced by optimized disruption of the dynamic phantom matrix. Second, its element values or matrix size are periodically updated to increase the randomness and complexity of encryption. Subsequently, the quadtree segmentation technique is used to divide the disrupted image into a quadtree structure to achieve the purpose of more flexible processing of different parts of the image information. Then, on the basis of the quadtree, the DNA diffusion optimization diffusion algorithm is applied to enhance the nonlinear characteristics and randomness of the encryption through the diffusion based on DNA coding, so as to disperse the image information more evenly. Ultimately, the generation of ciphertext images integrates these techniques to form a multilevel and multifaceted encryption structure, which improves the security and resistance to attacks of EA.

IV. Experimental Tests

To confirm the impact of the innovative computerized IE algorithm on performance, the research constructs an appropriate testing setup. Before conducting the EA's performance test and comparison test, the ideal parameters for the new chaotic system are ascertained. Ultimately, the algorithm's safety and efficacy are confirmed by simulating the impact of a real-world implementation.

A. *Algorithm Performance Testing*

The study established an appropriate test environment to assess the new IE algorithm's performance impact. The selected operating system is Windows and the image processing library is OpenCV. The CPU is Intel i7-9300H and the GPU is RTX3060Ti. The RAM is set to 32G and Python is used for language programming. The study first attempts to validate the optimized two-dimensional composite chaotic system, and also for subsequent easy testing, the study defines the system as improving Chebyshev-Iterative (ICI). The optimal control parameters, i.e., t and k, for the 2D composite CM are first determined by means of phase space analysis. The 2D composite chaotic system with different parameters at this point is shown in Fig. 7.



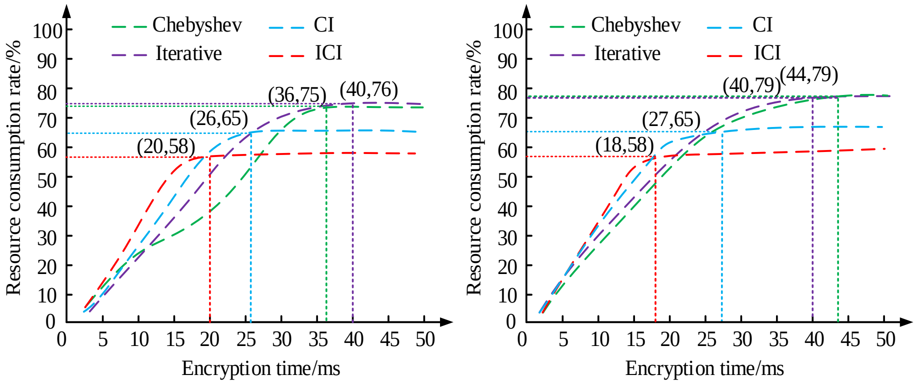
(a) t=10，k=25

(b) t=10，k=50

(c) t=10，k=75

Fig. 7. Optimal control parameter testing for two-dimensional composite chaotic mapping.

Fig. 7(a) shows the CM results at $t=10$，$k=25$, and Fig. 7(b) shows the CM results at $t=10$，$k=50$. Fig. 7(c) shows the CM results at $t=10$，$k=50$. In Fig. 7, the 2D composite CM under the control of different parameters presents different results, and when the k value is larger, the mapping result at this time is more uniform, which enables the system to achieve better mapping randomness. Compared to Fig. 7(a) and 7(b), Fig. 7(c) has the strongest traversal, therefore, it can be said that the 2D composite CM at this time is the best when $t=10$，$k=75$, and the subsequent research determined to test with this parameter value. For the novel IE algorithm proposed by the study. The research introduced the ImageNet image dataset for testing. The dataset contains millions of high-resolution color images covering more than a thousand categories. It is separated into training and test sets in an 8:2 ratio. The test results are displayed in Fig. 8. First, the data are subjected to an ablation test for EA with Chebyshev mapping alone, EA with Iterative mapping alone, EA with Chebyshev-Iterative mapping, and ICI.



(a) Training set

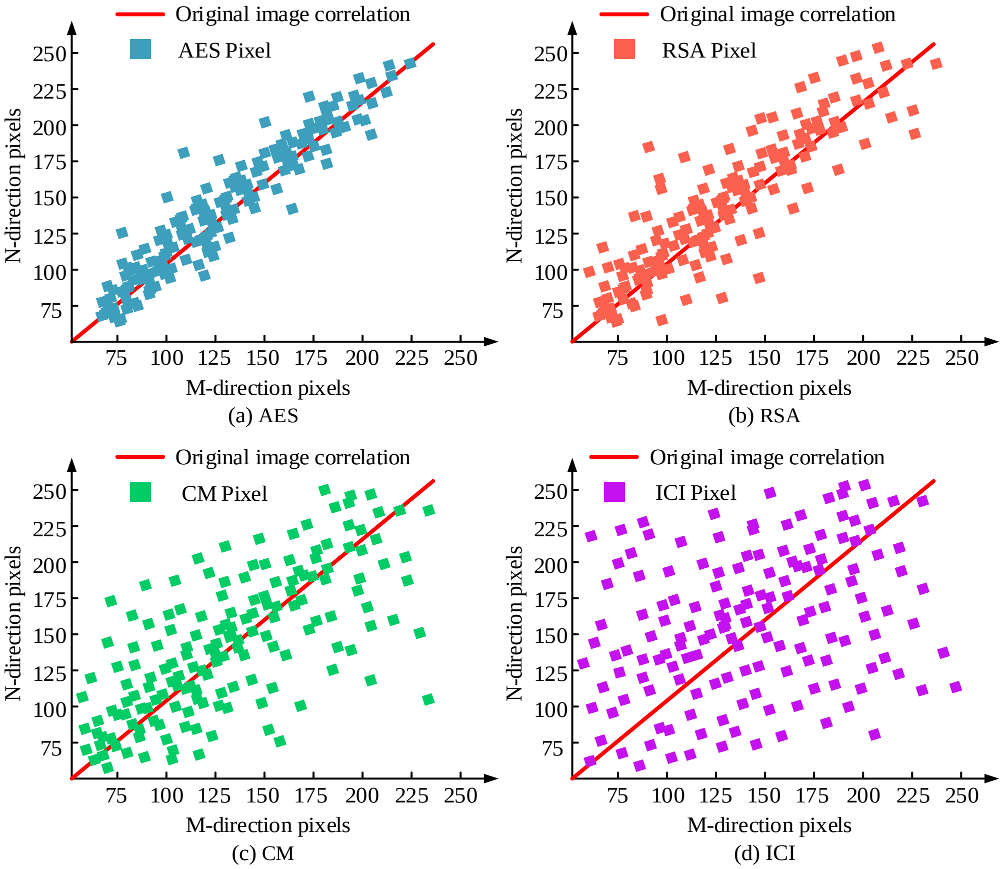
(b) Test set

Fig. 8. Results of ablation tests for different modules.

The performance test results of the four different module types under the training set are displayed in Fig. 8(a), and the results of the performance test of the four different module types under the test set are displayed in Fig. 8(b). In Fig. 8, both Chebyshev mapping alone and Iterative mapping alone have average performance results, with the highest resource consumption rate of 79% for both. On the contrary, the resource consumption rate of CI mapping is reduced to 65% after combination. The lowest resource consumption rate is 58% for ICI. The shortest mapping time is 18 milliseconds. From the above data, it is illustrated that there is a significant functional facilitation effect of each module on ICI, which makes ICI get a better mapping performance. Furthermore, the study presents the same kind of EA, such as CM, rivest-shamir-adleman (RSA), and advanced encryption standard (AES), to test with correlation as the test index. The ES algorithm is set up with a 128-bit key and standard mode; the RSA algorithm with a 2048-bit key; and the CM algorithm with a 2048-bit key. Fig. 9 displays the test findings. The outcomes are displayed in Fig. 9.

The image correlation findings under the AES, RSE, CM, and ICI algorithms are displayed in Fig. 9(a), (b), (c), and (d). In Fig. 9, the red diagonal line indicates the pixel correlation results of the original image, and the comparison reveals that the pixel correlation is the strongest under the AES algorithm with the highest concentration of pixel points. The CM and RSA algorithms come next, with the study's suggested ICI algorithm having the lowest pixel point correlation. The distribution is more uniform and random, indicating that the encrypted image presents characteristics that are difficult to be analyzed and predicted. As a result, it is evident that the researchers suggested approach performs better in IE visualization. To further quantify the test results, the study continues to introduce more algorithms of the same type, such as two fish EA (Twofish), elliptic curve cryptography (ECC), and visual cryptography (VC). In addition, the ECC algorithm uses a P-256 curve; the VC algorithm uses a predefined key-sharing matrix; and the ICI algorithm has optimal parameter configurations of chaotic system parameters 10 and 75. The encryption speed Mbit/s, decryption speed, resource consumption rate and latency rate are used as metrics for testing and the results are shown in Table I.

In Table I, a variety of algorithms all show superior IE performance, with encryption and decryption speeds above 400 Mbit/s. The slowest encryption speed is 441 Mbit/s for CM algorithm, and the slowest decryption speed is 412 Mbit/s for AES. The highest resource utilization rate is 62.4% for Twofish algorithm, and the highest latency rate is 27.4% for AES. With the highest encryption speed of 632 Mbit/s, the fastest decryption speed of 583 Mbit/s, the lowest resource consumption rate of 21.4%, and the lowest delay rate of 11.5%, a numerical comparison shows that the research-proposed ICI algorithm performs well. In summary, the ICI algorithm shows superior encryption performance among the same type of methods with high feasibility and effectiveness.



(a) AES

(b) RSA

(c) CM

(d) ICI

Fig. 9. Image correlation results under different encryption algorithms.

TABLE I. INDICATOR TEST RESULTS OF VARIOUS ALGORITHMS

Algorithm	Encryption Speed/Mbit/S	Decryption Speed/Mbit/S	Resource Consumption Rate/%	Delay Rate/%
AES	458.0	412.0	37.4	27.4
RSA	527.0	587.0	31.6	17.6
CM	441.0	428.0	45.7	13.4
Twofish	472.0	424.0	62.4	18.8
ECC	447.0	486.0	54.3	23.5
VC	528.0	479.0	27.1	14.8
ICI	632.0	583.0	21.4	11.5

B. Algorithm Simulation Testing

To validate the innovative EA's practical application, the study presents the Brodatz Texture Database image collection for various testing categories. Brodatz Texture Database contains nearly 20,000 images of various textures. Randomly selecting images from this dataset, the study introduced each of the AES, RSA and hash function algorithms for comparison, i.e., AES, RSA and secure hash algorithm 256-bit (SHA-256) for comparison. The encryption results under each method are shown in Fig. 10.

The encryption effect under the AES technique is shown in Fig. 10(a), the encryption effect under the RSA method is shown in Fig. 10(b), the encryption effect under the SHA-256 method is shown in Fig. 10(c), and the encryption effect under the ICI method is shown in Fig. 10(a). The results of the test in Table I are consistent with Fig. 10, which shows that among the four methods, the pixels of the encrypted image from RSA are much smaller than those of AES. This shows the validity of the test, in addition, intuitively, it can be found that the studied ICI encryption performance is optimal and the image security is the highest, while the pixel code in the encrypted image is more random and uniform, and does not retain traces. Therefore, it can be shown that ICI has some feasibility. In order to further understand whether the encrypted image information better meets the security requirements, the study plotted the histograms of the above methods respectively, as shown in Fig. 11.

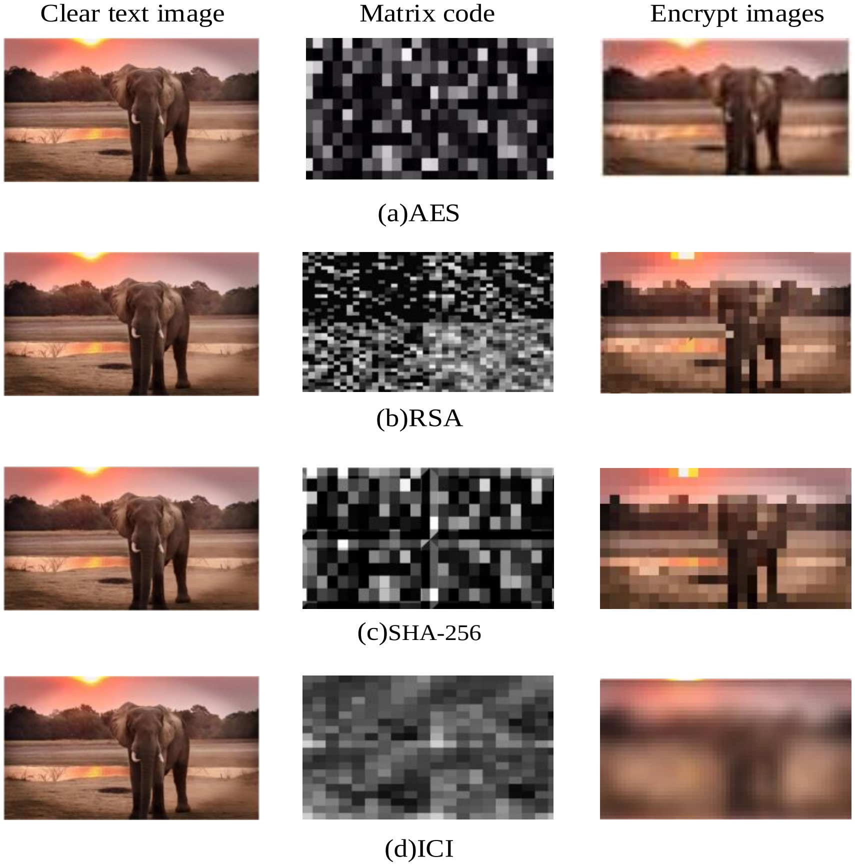
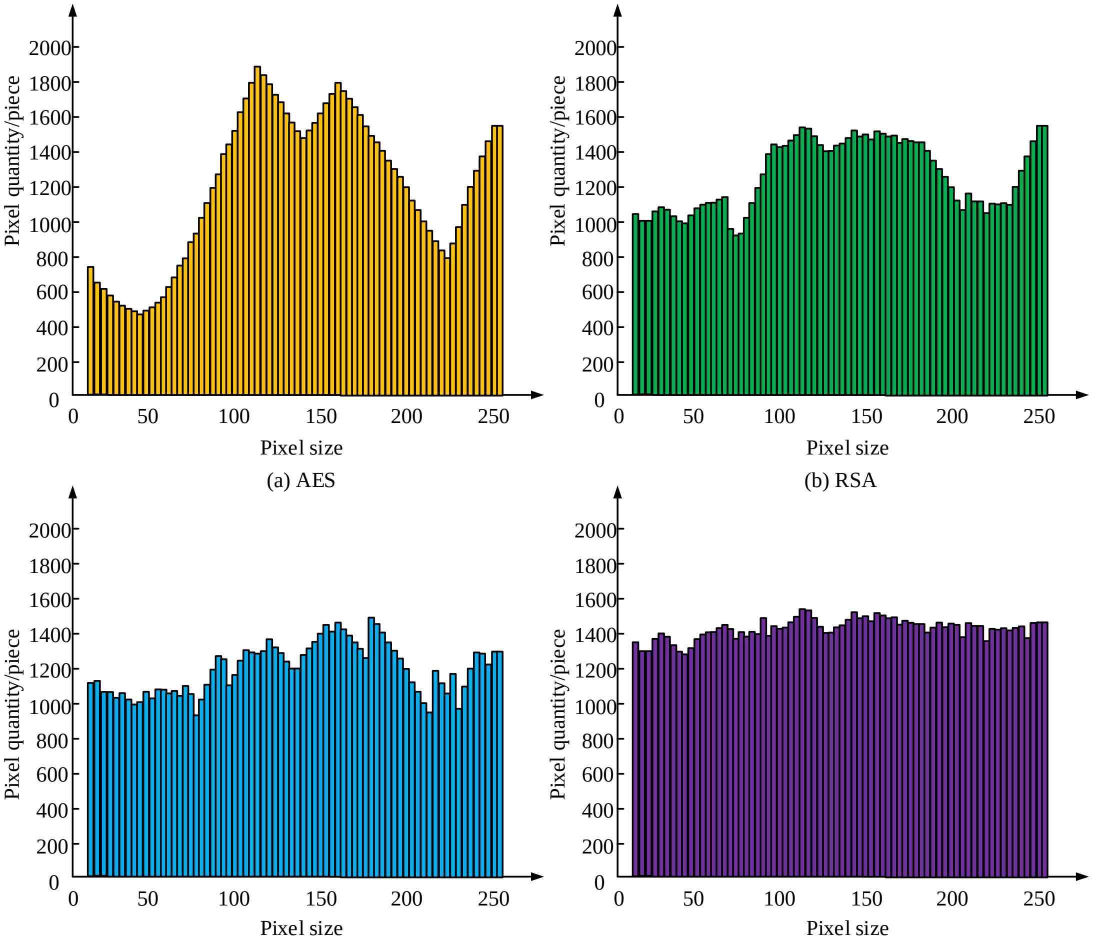


Fig. 10. Image encryption effects under different methods.



(a) AES

(b) RSA

(c) SHA-256

(d) ICI

Fig. 11. Test of image encryption histograms using four algorithms.

The encrypted image histograms for the AES, RSA, SHA-256, and ICI algorithms are displayed in Fig. 11(a), 11(b), and 11(d), respectively. Also shown are the encrypted image histograms for the algorithms. In Fig. 11, among the four algorithms, the pixel histogram of the AES algorithm is the most uneven, with multiple peaks showing, which indicates that the encrypted image is more specific and less secure. And it shows the trend of higher pixel value at the center point and lower at both ends. The pixel histograms of encrypted images of RSA algorithm, SHA-256 algorithm and ICI algorithm gradually tend to be stable, with fewer outliers, i.e. peaks, in the data. Especially the ICI algorithm, which shows the best IE effect, the encrypted image is more random and variant. And the average number of pixels of the encrypted image can be up to 1400, which is much higher than the AES algorithm. In summary, ICI has absolute advantages in computer IE, and its performance is far more reliable than the same type of encryption methods.

V. Discussion

With the rapid development of information technology, the importance of image encryption technology in safeguarding data privacy and security is becoming more and more prominent. Image encryption not only protects the privacy and integrity of data, but also plays a key role in many fields such as medical, military and communication. However, traditional image encryption methods such as symmetric encryption and asymmetric encryption show some limitations in the face of advanced attacks. Therefore, the study proposes a two-dimensional composite chaotic system based on the improved chaotic sequence algorithm and optimizes the disruption and diffusion steps in the image encryption process by combining the dynamic phantom square matrix and quadtree partitioning techniques, aiming to enhance the security and processing efficiency of image encryption. The experimental results show that when the parameters of the chaotic system are 10 and 75, the ICI algorithm achieves an encryption speed of 632 Mbit/s and a decryption speed of 583 Mbit/s, with a resource consumption rate of 21.4% and a delay rate of 11.5%. These data show that the ICI algorithm is far ahead of other algorithms such as AES, RSA, Twofish and ECC in terms of performance. The results compare favorably with the phase-coded binary image encryption method proposed by Hamadi I A et al. in terms of processing efficiency and security [19]. In addition, the ICI algorithm exhibits the lowest pixel-point correlation in the correlation test with a more uniform and random distribution that is difficult to be analyzed and predicted. And compared with the traditional dynamic coding multi-image encryption algorithm, the ICI algorithm in this paper performs more superior in dealing with statistical analysis, differential attack and exhaustive attack. In the simulation test, compared with the other three types of methods, the research proposed ICI encryption has the best performance and the highest image security, while the pixel code in the encrypted image is more random and uniform, and does not retain traces. From this result, it can be seen that compared to the research method proposed by Tiken C et al., the ICI algorithm proposed in this study significantly reduces the resource consumption rate and latency rate by optimizing the disruption and diffusion steps, so that it still maintains efficient performance when processing large-scale image data [20].

In summary, the two-dimensional composite chaotic system based on improved chaotic sequence algorithm proposed in this paper significantly improves the security and processing efficiency of image encryption by optimizing the disruption and diffusion steps. Future research can further explore how to combine other encryption algorithms and image processing techniques to further improve the performance and reliability of computerized image encryption technology. In conclusion, the research in this paper provides new theoretical and practical support for the development of image encryption technology, which has important academic value and application prospects. It is hoped that through further research and practice, we can promote the continuous progress of image encryption technology and make greater contributions to the field of information security.

VI. Conclusion

The study analyzes the existing chaotic sequence algorithms on the basis of the algorithmic optimization of disruption and diffusion in the encryption process through the combination, and finally puts forward a new type of image encryption algorithm. The experimental results show that when the optimal control parameters $t=10$, $k=75$, the two-dimensional composite chaotic mapping at this time has the best effect. Comparison with the same type of encryption algorithms reveals that the ICI algorithm has the significantly lowest pixel point correlation and a more uniform and random distribution. It has the highest encryption speed of 632 Mbit/s and decryption speed of 583 Mbit/s, the lowest resource consumption rate of 21.4%, and the lowest delay rate of 11.5%. In addition, the simulation test results show that compared with other encryption methods of the same type, ICI encryption has the optimal performance and the highest image security, while the pixel code in the encrypted image is more random and uniform, and does not retain traces. From the histogram analysis, it is found that the encrypted image of ICI encryption algorithm is more random and variable, and the average pixel number of the encrypted image is up to 1400, which is much higher than that of AES algorithm. In summary, the encryption algorithm proposed by the research is superior to the same type of algorithms in terms of pixel-point correlation, distribution uniformity, encryption speed, decryption speed, and resource consumption rate, especially in the image security and the randomness of encryption effect, which is of significant scientific value and application prospect. Future research can further explore how to combine other EA and image processing techniques to further improve the performance and reliability of computer IE technology.

References

[1] Xu X, Chen S. Single Neuronal Dynamical System in Self-Feedbacked Hopfield Networks and Its Application in Image Encryption. Entropy, 2021, 23(4):456-457.

[2] Zhang F, Zhang X, Cao M, Ma F, Li Z. Characteristic Analysis of 2D Lag-Complex Logistic Map and Its Application in Image Encryption. IEEE multimedia, 2021, 28(4):96-106.

[3] Shengtao G, Tao W, Shida W. A Novel Image Encryption Algorithm Based on Chaotic Sequences and Cross-Diffusion of Bits. IEEE Photonics Journal, 2021, 13(1):1-15.

[4] Pourasad Y, Ranjbarzadeh R, Mardani A. A new algorithm for digital image encryption based on chaos theory. Entropy, 2021, 23(3): 341-342.

[5] Shikder A, Kumar P, Nishchal N K. Image Encryption by Structured Phase Encoding and Its Effectiveness in Turbulent Medium. IEEE Photonics Technology Letters, 2023, 35(5):128-131.

[6] Zhang Q, Han J, Ye Y. Multi-image encryption algorithm based on image hash, bit-plane decomposition and dynamic DNA coding. IET image processing, 2021, 15(4):885-896.

[7] Man Z, Li J, Di X. Medical image encryption scheme based on self-verification matrix. IET Image Processing, 2021, 15(12):2787-2789.

[8] Sheng Y, Li J, Di X, Man Z, Liu Z. Bit-level image encryption algorithm based on fully-connected-like network and random modification of edge pixels. IET Image Process. 2022, 16(10):2769-2790.

[9] Balaska N, Ahmida Z, Belmeguenai A. Image encryption using a combination of Grain-128a algorithm and Zaslavsky chaotic map. IET Image Processing, 2020, 14(6):1120-1131.

[10] Jia M. Image encryption with cross colour field algorithm and improved cascade chaos systems. IET Image Processing, 2020, 14(5):973-981.

[11] Sheng Y, Li J, Di X, Man Z, Liu Z. Bit-level image encryption algorithm based on fully-connected-like network and random modification of edge pixels. IET Image Process. 2022, 16(10):2769-2790.

[12] Song X, Xu D, Li G, Xu W. Multi-image Reorganization Encryption Based on S-L-F Cascade Chaos and Bit Scrambling. J. Web Eng. 2021, 20(4):1177-1192.

[13] He Y, Zhang Y Q, He X, Xing Y W. A new image encryption algorithm based on the OF-LSTMS and chaotic sequences. Scientific reports, 2021, 11(1): 6398-6399.

[14] Logeshwari R, Rama Parvathy L. Generating logistic chaotic sequence using geometric pattern to decompose and recombine the pixel values. Multimedia tools and applications, 2020, 79(31): 22375-22388.

[15] Chen L, Yin H, Yuan L. A novel color image encryption algorithm based on a fractional-order discrete chaotic neural network and DNA sequence operations. Frontiers of Information Technology & Electronic Engineering, 2020, 21(6): 866-879.

[16] Luan G, Li A, Chen Z, Huang C. Asymmetric Optical Image Encryption with Silhouette Removal Using Interference and Equal Modulus Decomposition. IEEE Photonics Journal, 2020, 12(2):1-8.

[17] Jia M. Image encryption with cross colour field algorithm and improved cascade chaos systems. IET Image Processing, 2020, 14(5):973-981.

[18] Hebbi C, Mamatha H. Comprehensive Dataset Building and Recognition of Isolated Handwritten Kannada Characters Using Machine Learning Models. Artificial Intelligence and Applications, 2023, 1(3):179-190.

[19] Hamadi I A, Jamal R K, Mousa S K. Image encryption based on computer generated hologram and Rossler chaotic system. Optical and Quantum Electronics, 2022, 54(1): 33-34.

[20] Tiken C, Samlı R. A comprehensive review about image encryption methods. Harran Üniversitesi Mühendislik Dergisi, 2022, 7(1): 27-49.