IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 10 March 2025, accepted 6 April 2025, date of publication 15 April 2025, date of current version 5 May 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3560686

RESEARCH ARTICLE

Lightweight Image Encryption Algorithm Using 4D-NDS: Compound Dynamic Diffusion and Single-Round Efficiency

YUNLONG LIAO[1], YITING LIN[2,3], (Member, IEEE), QIUTONG LI[1], ZHENG XING[1], AND XIAOCHEN YUAN[1], (Senior Member, IEEE)

[1]Faculty of Applied Sciences, Macao Polytechnic University, Macau, China
[2]Guangdong Provincial/Zhuhai Key Laboratory of Interdisciplinary Research and Application for Data Science, Beijing Normal-Hong Kong Baptist University, Zhuhai 519087, China
[3]Department of Computer Science, Hong Kong Baptist University, Hong Kong, China

Corresponding author: Xiaochen Yuan (xcyuan@mpu.edu.mo)

This work was supported in part by the Science and Technology Development Fund of Macau under Grant 0045/2022/A, and in part by Macao Polytechnic University under Grant RP/FCA-04/2024.

ABSTRACT With the development of the Internet of Things (IoT) and communication technologies, multimedia information has become an essential part of communication. As a carrier with high information density and large transmission volume, image data is increasingly at risk of information leakage. To address the issue of digital private image leakage, this paper proposes a reliable image security protection scheme based on a non-degenerate hyperchaotic system for dynamic permutation and single-round composite diffusion. By leveraging the high dynamic properties of non-degenerate chaos, the scheme effectively addresses the insufficient sensitivity of pseudo-random sequences to initial values and enhances the sensitivity of the key to initial conditions. Additionally, the single-round composite double-diffusion system significantly improves the security and reliability of the algorithm, with the information entropy of the encrypted image reaching 7.9994. Experimental and theoretical verification demonstrate that the algorithm exhibits high sensitivity and effective robustness, capable of resisting common attacks and providing a reliable security solution for communication and the IoT.

INDEX TERMS Image encryption, dynamical analysis, chaotic system, cryptography.

I. INTRODUCTION

In today's digital age, the rapid development of the Internet of Things and cloud computing technologies has greatly promoted the progress of the information society. However, this process has also brought new challenges [1], [2]. Massive amounts of multimedia data, especially digital images, are being transmitted on the network at an unprecedented scale [3], [4]. Digital images, as one of the most straightforward means of conveying information, contain highly significant content [5], [6], including sensitive information such as personal privacy, commercial secrets and even national security [7], [8]. Therefore, it is particularly important to ensure the security of these image data. However, traditional encryption algorithms, such as the AES and the DES, are powerless when facing image data [9], [10]. Most of these algorithms are based on linear structures and are difficult to effectively deal with the high redundancy and strong correlation of image data [11], [12]. The complexity of image data makes traditional encryption methods face huge challenges in both encryption efficiency and security. This has prompted researchers to continuously explore new encryption mechanisms to find encryption methods that are more suitable for the characteristics of image data. Against this background, emerging technologies such as nonlinear encryption technology and chaotic encryption have emerged [13], [14]. Nonlinear encryption technology breaks the linear limitations of traditional encryption by

The associate editor coordinating the review of this manuscript and approving it for publication was Diana Gratiela Berbecaru.

introducing nonlinear elements, providing new ideas for image encryption [15], [16]. Chaotic encryption leverages the inherent unpredictability of chaotic systems and their extreme sensitivity to initial conditions to introduce greater security and complexity into the realm of image encryption [17], [18]. The emergence of these emerging technologies not only brings new hope to the field of image encryption, but also opens up new directions for information security research.

Over the past few years, image encryption methods leveraging chaos theory have emerged as a prominent research focus within information security, primarily attributed to their high sensitivity to initial conditions, strong ergodic properties, and the ability to generate pseudo-random sequences [19], [20]. Existing encryption methods can be mainly divided into four categories: transform domain-based algorithms [21], [22], permutation-diffusion architecture-based algorithms [23], [24], bio-inspired algorithms [25], [26], and hybrid encryption frameworks [27], [28]. Among them, chaotic systems are often used to construct permutation matrices or drive diffusion processes due to the complexity of their dynamic behavior, which significantly improves the security of encryption systems [29], [30]. In 2023, Zheng and Bao [31] proposed an image encryption algorithm via a cascade chaotic map and DNA coding for secure image transmission. The algorithm employs a 2D-Cascade-Transform-Logistic-Sine Map (2D-CTLSM) to generate chaotic sequences with improved randomness and large parameter ranges. It combines zigzag transformation with DNA encoding to enhance the diffusion and confusion processes. The scheme includes chunking dislocation and alternate row diffusion to further strengthen security. This demonstrates the robustness and reliability of the proposed encryption method. In 2024, Xue et al. [32] proposed a revolutionary compression-encryption algorithm for color medical images based on compressive sensing (CS) and DNA coding operations. This method addresses the challenges of storage efficiency and data security in medical imaging by integrating discrete wavelet transform, sparse optimization, and DNA-level encryption techniques. The algorithm enhances the randomness of the original image signal through position scrambling and reduced-stiffness operations, followed by DNA encoding, base scrambling, and XOR operations to achieve robust encryption. This approach enables efficient and secure transmission of color medical images, facilitating advancements in digital medicine and telemedicine. In 2025, İnce et al. [33] proposed a novel lightweight image encryption algorithm named Random Strip Peeling (RSP) for Internet of Things (IoT) devices, which employed a unique combination of color plane permutation and chaotic maps to achieve efficient and secure image encryption. The algorithm disrupts linearity in the confusion step using two different sequences generated by the 1D Tent Map and enhances diffusion with an XOR matrix generated by the Logistic Map. The algorithm shows robust resistance to statistical and differential attacks, making it suitable for resource-constrained IoT environments. Despite many achievements, existing chaotic encryption schemes still face the following challenges: First, the key space of one-dimensional chaotic mapping is limited and can be easily cracked by phase space reconstruction attacks; second, most two-dimensional chaotic systems have periodic windows, resulting in insufficient complexity of the generated pseudo-random sequences; third, the traditional permutation-diffusion structure does not completely eliminate the correlation between adjacent pixels and is difficult to resist statistical attacks. Recent studies [34], [35] have shown that hyperchaotic systems can produce more complex dynamic behaviors due to their multiple positive Lyapunov exponents, providing new ideas for improving the robustness of encryption systems. However, the existing hyperchaotic mapping designs mostly rely on complex nonlinear function combinations, which reduces computational efficiency and restricts their real-time applications [36], [37]. In summary, the demand for image encryption is growing, yet for IoT environments, overly simple algorithms lack practicality, while overly complex algorithms face limitations due to device performance. There is also an increasing demand for robustness in image encryption.

To tackle these issues, the paper introduces an image encryption approach that leverages non-degenerate discrete chaos and dynamic two-way permutation. The proposed method utilizes non-degenerate discrete chaos to create pseudo-random sequences, thereby fortifying the security and resilience of image encryption by implementing processes that induce confusion, dynamic rearrangement, and dynamic spreading of the data. Notably, the scheme demonstrates high sensitivity to both plaintext and ciphertext images, as evidenced by theoretical analysis and experimental validation. The main contributions are reflected in the following three aspects:

1) This study proposes a four-dimensional non-degenerate hyperchaotic system (4D-NDS). Through a unique dynamic design, the system achieves efficient generation and evolution of chaotic behavior, avoiding the degradation problem that may occur in traditional chaotic systems. This non-degenerate characteristic greatly improves the complexity and unpredictability of chaotic sequences, laying a solid foundation for subsequent encryption applications.
2) This study designs an innovative single-round composite dynamic diffusion mechanism. This highly efficient diffusion strategy achieves rapid mixing and diffusion of plaintext information through a complex dynamic process, thereby minimizing the computational burden associated with multi-round diffusion.
3) This study proposes a lightweight optimized security architecture that integrates multiple cryptographic techniques such as permutation, diffusion, obfuscation, and plaintext-associated dynamic key generation. Through the plaintext-associated dynamic key

generation mechanism, the architecture can dynamically adjust the encryption key according to the input plaintext, thereby effectively resisting common cryptographic attacks such as differential attacks and linear attacks. This lightweight optimization design is particularly suitable for resource-constrained environments, such as IoT devices and mobile terminals, and has broad application prospects.

The rest of this paper is organized as follows: Section II reviews previous related work. Section III introduces the image encryption algorithm implemented using 4D hyperchaos. Section IV discusses and analyzes the numerical experiments and security performance of the proposed scheme. Finally, Section V concludes this paper.

II. PREPARATORY WORK

A. 4D-NDS CHAOS CONSTRUCTION

To construct a new non-degenerate 4-dimensional discrete-time chaotic system (4D-NDS), as referenced in Liu et al. [38], the following steps are taken: First, obtain a transformed matrix A. Then, using a uniformly bounded anti-controller g and a control matrix B, perform inverse control on A, with the equation as follows:

$$x_n(k+1) = Ax_n(k) + Bg(\sigma x_n(k), \varepsilon) \tag{1}$$

where x_k is iteration sequence, σ and ε are parameters of the anti-controller. Pole assignment according to (1). It is possible to determine the Lyapunov exponent $LE_+ = n$, signifying that the controlled system has become an n-dimensional discrete-time hyperchaotic system.

According to this concept, the subsequent text outlines the design of a four-dimensional discrete non-degenerate chaotic system:

$$A = \begin{pmatrix} -0.1667 & 0.0333 & -0.5667 & 0.5333 \\ -0.1667 & -0.0667 & -0.4667 & 0.6333 \\ -0.3667 & -0.0667 & -0.2667 & 0.4333 \\ 0 & 0.3000 & -0.3000 & 0.1000 \end{pmatrix} \tag{2}$$

$$g(\sigma x_k, \varepsilon_k) = \begin{cases} \varepsilon_1 \dfrac{sin(2\pi x_1(k))}{1+\sigma x_1^2(k)} \\ \varepsilon_2 \dfrac{sin(2\pi x_2(k))}{1+\sigma x_2^2(k)} \\ \varepsilon_3 \dfrac{sin(2\pi x_3(k))}{1+\sigma x_3^2(k)} \\ \varepsilon_4 \dfrac{sin(2\pi x_4(k))}{1+\sigma x_4^2(k)} \end{cases} \tag{3}$$

$$B = E = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{4}$$

Ultimately, the discrete-time chaotic system developed is presented as follows:

$$\begin{pmatrix} x_1(k+1) \\ x_2(k+1) \\ x_3(k+1) \\ x_4(k+1) \end{pmatrix} = A_{4\times4} \begin{pmatrix} x_1(k) \\ x_2(k) \\ x_3(k) \\ x_4(k) \end{pmatrix} + E_{4\times4} g(\sigma x_k, \varepsilon_k) \tag{5}$$

$$\begin{cases} x_1(k+1) = A_{(1,1)}x_1(k) + A_{(1,2)}x_2(k) + A_{(1,3)}x_3(k) \\ \qquad + A_{(1,4)}x_4(k) + \varepsilon_1 \dfrac{sin(2\pi x_1(k))}{1+\sigma x_1^2(k)} \\ x_2(k+1) = A_{(2,1)}x_1(k) + A_{(2,2)}x_2(k) + A_{(2,3)}x_3(k) \\ \qquad + A_{(2,4)}x_4(k) + \varepsilon_2 \dfrac{sin(2\pi x_2(k))}{1+\sigma x_2^2(k)} \\ x_3(k+1) = A_{(3,1)}x_1(k) + A_{(3,2)}x_2(k) + A_{(3,3)}x_3(k) \\ \qquad + A_{(3,4)}x_4(k) + \varepsilon_3 \dfrac{sin(2\pi x_3(k))}{1+\sigma x_3^2(k)} \\ x_4(k+1) = A_{(4,1)}x_1(k) + A_{(4,2)}x_2(k) + A_{(4,3)}x_3(k) \\ \qquad + A_{(4,4)}x_4(k) + \varepsilon_4 \dfrac{sin(2\pi x_4(k))}{1+\sigma x_4^2(k)} \end{cases} \tag{6}$$

where $\sigma_1 = \sigma_2 = \sigma_3 = \sigma_4 = \sigma$, $\varepsilon_1 = \varepsilon_2 = \varepsilon_3 = \varepsilon_4 = \varepsilon$. The initial values $x_1(1)$, $x_2(1)$, $x_3(1)$ and $x_4(1)$ are 0.1, 0.2, 0.3 and 0.4, $\sigma = 1$, $\varepsilon = 1$. By calculating the iteration equation, a chaotic mapping is obtained as shown in FIGURE 1.

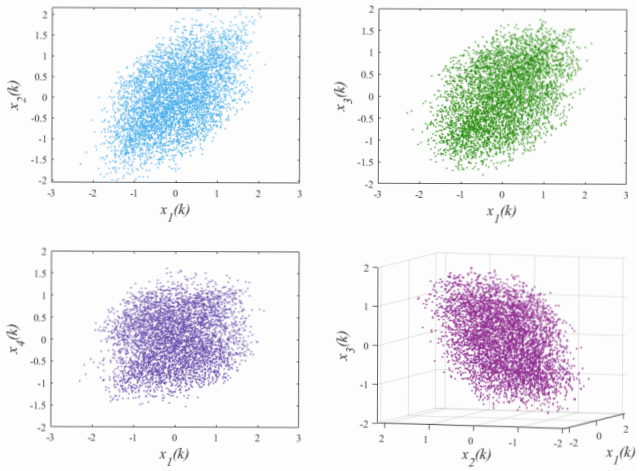

FIGURE 1. Visualization of phase diagrams of the proposed 4D-NDS chaotic maps.

B. PLAINTEXT-RELATED CHAOTIC SYSTEMS (PLCS)

The chaotic sequences generated by chaotic systems are often not directly usable in encryption programs. Meanwhile, leveraging the initial value sensitivity of chaotic systems to link the hash value of the plaintext image with the initial values of the chaotic system can effectively enhance the security of the algorithm and expand the key space. The specific operations are as follows:

$$N_i = \text{hex2dec}(\text{SHA-256}_{2i-1:2i}) \quad i = 1, 2, \ldots, 32 \tag{7}$$

where hex2dec is a conversion function that takes a 64-bit hexadecimal number, divides it into 32 groups of 2-bit hexadecimal digits, and then converts each group into a decimal form, resulting in 32 groups of decimal numbers. These 32 groups of decimal numbers are then further divided into 8 larger groups, and for each of these 8 groups, the data are processed as follows:

$$n_i = \mathrm{mod}(N_{4i-3} \oplus N_{4i-2} \oplus N_{4i-1}, N_{4i})/(H \times W) \quad i = 1, 2, \ldots, 8 \tag{8}$$

where H and W represent the height and width dimensions of the original image. From the set n, three distinct groups of parameters are selected to adjust the initial state of the non-degenerate chaotic system. Additionally, two more sets of parameters are utilized to modify the anti-control variables within the non-degenerate chaotic system. Among them, the selection of which 6 sets of parameters is random, and here the first five sets of parameters are fixed for demonstration purposes. The processing is as follows:

$$\begin{cases} x_1'(1) = x_1(1) + n_1 \\ x_2'(1) = x_2(1) + n_2 \\ x_3'(1) = x_3(1) + n_3 \\ x_4'(1) = x_4(1) + n_4 \\ \sigma' = \sigma + \mathfrak{n}_5 \\ \varepsilon' = \varepsilon + \mathfrak{n}_6 \end{cases} \tag{9}$$

After processing the initial values of the chaotic system in this manner, the pseudo-random sequences generated by the chaotic sequences will be closely related to the ciphertext. These sequences are then processed for use in the encryption process.

III. ENCRYPTION METHOD

This algorithm utilizes a combination of 4D-Non-degenerate chaotic driving for confusion, dynamic permutation, and dynamic diffusion based on plaintext-related adaptive feature points to form an encryption scheme (4D-NDTD). The encryption framework is shown in FIGURE 2 and the relevant theories and specific encryption steps will be introduced in this section.

In this paper, an image encryption scheme is introduced that operates on the principle of ''permutation - diffusion - diffusion - confusion'' The process of encryption is depicted in FIGURE 2. The detailed steps for encryption are outlined below:

A. DYNAMIC PERMUTATION

Using sequence K_{pr} and K_{pc} to perform dynamic permutation operation on plain image I, the specific process is as follows:

$$\begin{cases} K_{pr} = \mathrm{sort}\,(x_1(1:H)) \\ K_{pc} = \mathrm{sort}\,(x_1(end - W + 1 : end)) \end{cases} \tag{10}$$

$$\begin{cases} C_1(i,:) = \mathrm{circshift}\left(I_1(i,:), \left[0, K_{\mathrm{pr}}(i)\right]\right) & i = 1, 2, \ldots, H \\ C_1(:,j) = \mathrm{circshift}\left(C_1(:,j), \left[K_{\mathrm{pc}}(j), 0\right]\right) & j = 1, 2, \ldots, W \end{cases} \tag{11}$$

where C_1 is the permuted image, circshift is the shift function, sort is a sort function, *end* represents the last position in a sequence.

B. SINGLE-ROUND COMPOSITE DYNAMIC DIFFUSION MECHANISM

We propose a single-round composite dynamic diffusion scheme. This scheme consists of a dynamic bitwise diffusion and a dynamic row-column diffusion, both driven by sequences generated by a chaotic system. First, the image undergoes dynamic bitwise diffusion, which is formulated as follows:

$$\begin{cases} k_{d1} = \mathrm{mod}(\mathrm{floor}(x_2(1 : H \times W) \times 10^6), 256) \\ k_{d2} = \mathrm{mod}(\mathrm{floor}(x_2(end - H \times W + 1 : end) \times 10^5), 256) \end{cases} \tag{12}$$

$$\begin{cases} C_2(1) = C_1(1) \oplus K_{d1}(1) \oplus (sum(1) \dot{\times} K_{d2}(1)) \\ sum(1) = \sum_{i}^{H \times W} C_1(i) - C_1(1) \\ a \dot{\times} b = \mathrm{mod}(a + b, 256) \end{cases} \tag{13}$$

where floor is a downward rounding function.

Then, the subsequent positions are processed as follows:

$$\begin{cases} C_2(i) = C_1(i) \oplus (C_1(i-1) \dot{\times} K_{d1}(i) \oplus (sum(i) \dot{\times} K_{d2}(1)) \\ sum(i) = \sum_{i}^{H \times W} sum(i-1) - C_1(1) \end{cases} \tag{14}$$

where C_2 is the diffused image, K_{d1} and K_{d2} are the processed chaotic sequences.

After the dynamic bitwise diffusion is completed, the row-column dynamic diffusion operation begins. First, the chaotic sequences are processed to obtain the required D_a, D_b, D_c, and D_d.

$$\begin{cases} D_a = \begin{cases} \mathrm{mod}((x_1 \times 10^6), 256) | \,\mathrm{mod}(D_a, 2) = 1 \\ \mathrm{reshape}(D_a(1 : H \times W), H, W) \end{cases} \\ D_b = \begin{cases} \mathrm{mod}((x_2 \times 10^6), 256) \\ \mathrm{reshape}(D_b(1 : H \times W), H, W) \end{cases} \end{cases} \tag{15}$$

$$\begin{cases} D_c = \begin{cases} \mathrm{mod}((x_3 \times 10^6), 256) | \,\mathrm{mod}(D_c, 2) = 1 \\ \mathrm{reshape}(D_a(1 : H \times W), H, W) \end{cases} \\ D_d = \begin{cases} \mathrm{mod}((x_4 \times 10^6), 256) \\ \mathrm{reshape}(D_c(1 : H \times W), H, W) \end{cases} \end{cases} \tag{16}$$

where reshape is a matrix transformation function. Then, a diffusion operation is performed, as specifically shown in Formula 17 and Formula 18, as shown at the bottom of the next page.

After performing the aforementioned operations, the encrypted image C_3 is obtained.

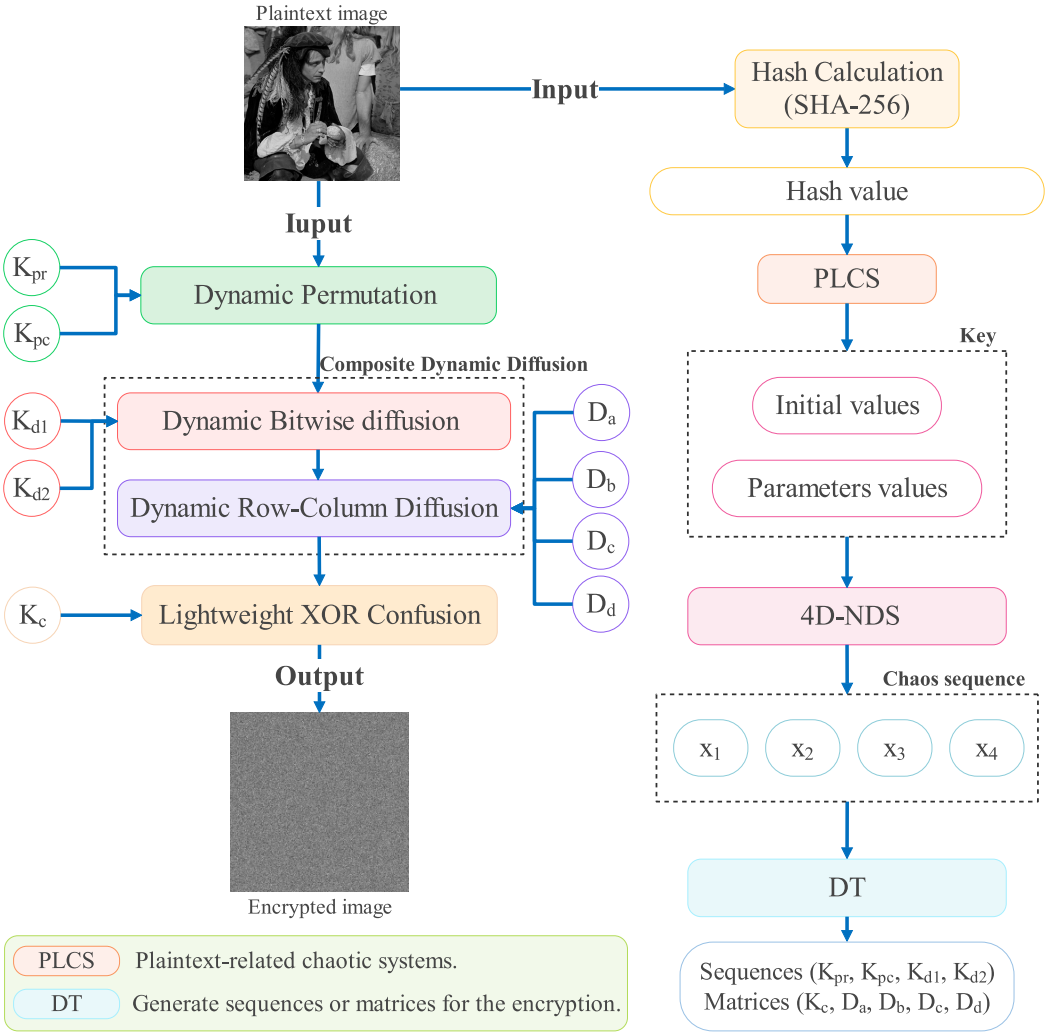

FIGURE 2. Flowchart of the proposed 4D-NDTD.

C. LIGHTWEIGHT XOR CONFUSION

Using sequence K_c to perform a confusion operation on C_2, the specific process is as follows:

$$\begin{cases} K_c = \text{reshape}\left(\left(\text{floor}\left(\text{mod}\left(x_4 \times 10^5, 256\right)\right)\right), H, W\right) \\ C(i) = C_3(i) \oplus K_c(i), \quad i = 1, 2, \ldots, H \times W \end{cases} \tag{19}$$

After executing all the operations, the encrypted image C is obtained.

IV. EXPERIMENTAL VALIDATION AND DISCUSSION

The validation of the proposed digital image encryption scheme was conducted using MATLAB 2022b. The experiment was executed on a personal computer configured with a 64-bit Windows 11 operating system, an AMD Ryzen 7-7745HX processor with integrated Radeon Graphics, and 16GB of RAM.

The proposed scheme will comprehensively evaluate the security and reliability of the algorithm through multiple

$$C_3(i,j) = \begin{cases} \text{mod}(C_2(i,j) \times D_a(i,j) + D_b(i,j), 256) & j = 1 \\ \text{mod}((C_2(i,j) + C_3(i,j-1)) \times D_a(i,j) + D_b(i,j), 256) & i = 1 \ldots H, j = 2, \ldots, W \end{cases} \tag{17}$$

$$C_3(i,j) = \begin{cases} \text{mod}(C_3(i,j) \times D_c(i,j) + D_d(i,j), 256) & i = 1 \\ \text{mod}((C_3(i,j) + C_3(i,j-1)) \times D_c(i,j) + D_d(i,j), 256) & i = 2 \ldots H, j = 1, \ldots, W \end{cases} \tag{18}$$

aspects, including encryption performance, statistical characteristics, sensitivity, and robustness.

A. ANALYSIS OF THE CHAOTIC PROPERTIES OF 4D-NDS

1) ANALYSIS OF THE LYAPUNOV EXPONENT OF 4D-NDS

The Lyapunov exponents can effectively reflect the dynamic characteristics of chaos. Generally, when a chaotic system has two positive Lyapunov exponents, it is referred to as a hyperchaotic system. Compared with ordinary chaotic systems, hyperchaotic systems exhibit stronger chaotic effects and higher sensitivity to initial conditions. The Lyapunov exponents of the chaotic system used in this study are 1.1029, 0.9655, 0.7720 and 0.4469, respectively. The results are shown in FIGURE 3, which proves that the system is a hyperchaotic system.

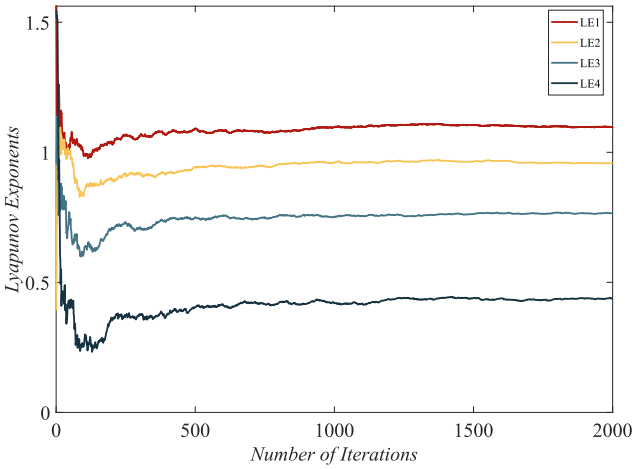

FIGURE 3. Results of the proposed 4D-NDS: Lyapunov exponents spectrum.

2) ANALYSIS OF THE BIFURCATION DIAGRAMS OF 4D-NDS

The bifurcation diagram illustrates the behavioral characteristics of a chaotic system transitioning from order to disorder as its parameters change. In this section, the fixed-point parameter method is employed for testing. By keeping parameter σ constant and varying the value of parameter ε, the system's behavior is observed. From FIGURE 4, it can be seen that as parameter ε approaches 1, the system transitions from an ordered to a disordered state, indicating the presence of chaotic characteristics at this point.

3) ANALYSIS OF THE GOTTWALD MELBOURNE 0-1 TEST OF 4D-NDS

The Gottwald-Melbourne 0-1 test is used to detect whether a time series exhibits chaotic behavior. By mapping the time series into a high-dimensional space, it determines whether the trajectory in the phase space repeats. FIGURE 5 shows the phase space trajectory of the 4D-NDS. The trajectory displays abundant chaotic characteristics, indicating that the algorithm can effectively enhance security.

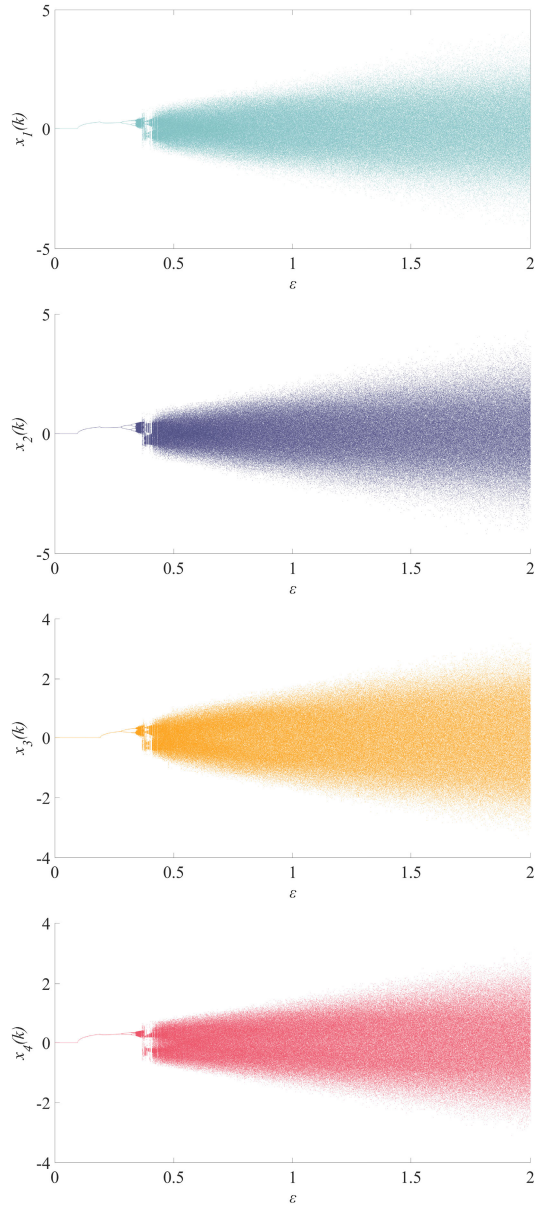

FIGURE 4. Results of the proposed 4D-NDS: Bifurcation diagram of the parameter ε. The parameter ε has chaotic behavior around 1 ($\sigma = 1$).

B. ANALYSIS OF THE PERFORMANCE RESULTS OF 4D-NDTD

The Number of Pixel Change Rate (NPCR) measures the effectiveness of an image encryption algorithm by calculating the proportion of pixels with different values between two encrypted images. The Unified Average Changing Intensity (UACI) measures the degree of pixel changes by calculating the average difference in pixel values. Together, they evaluate the encryption performance of the algorithm.

Equations relating to NPCR and UACI are as follows:

$$\begin{cases} NPCR = \dfrac{1}{H \times W} \times \sum_{i=1}^{H} \sum_{j=1}^{W} D_n(i,j) \\ UACI = \dfrac{1}{H \times W} \times \sum_{i=1}^{H} \sum_{j=1}^{W} \dfrac{|v_1(i,j) - v_2(i,j)|}{255} \end{cases} \tag{20}$$

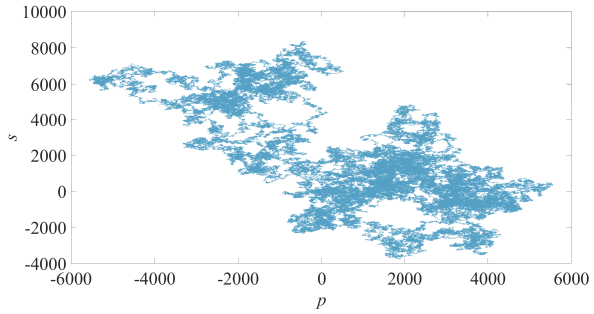

FIGURE 5. Results of the proposed 4D-NDS: The Gottwald Melbourne 0-1 test.

where D_N is the result of comparing two images at the same position, same outputs 0 and different outputs 1.

The performance of the proposed algorithm for partial image encryption and its comparison with other encryption algorithms are presented in TABLE 1 and TABLE 2. The results demonstrate that the algorithm achieves better performance and security in encryption.

TABLE 1. The comparison of NPCR with different algorithms.

Image	NPCR				
	2024 [39]	2024 [40]	2025 [41]	2024 [42]	Proposed
'baboon'	99.6166	99.6141	-	-	99.6047
'Male'	-	99.6121	99.6050	99.6039	99.6147
'Couple'	99.5880	-	99.6040	99.6197	99.9109

TABLE 2. The comparison of UACI with different algorithms.

Image	UACI				
	2024 [39]	2024 [40]	2025 [41]	2024 [42]	Proposed
'baboon'	33.4583	33.4835	-	-	33.5251
'Male'	-	33.4732	33.4746	33.4820	33.4064
'Couple'	33.4630	-	33.4206	33.4961	33.4611

C. ANALYSIS OF THE STATISTICAL PROPERTIES OF 4D-NDTD

1) HISTOGRAM

In image processing, histograms can effectively reflect the distribution of pixels in an image across different intensity values, which helps to evaluate the image's contrast, brightness, and overall quality. For encrypted images, the histogram usually shows a uniform intensity, which is an intuitive and reliable method to reflect the encryption effect of the image. The histogram of the encrypted image generated by this algorithm is shown in FIGURE 6. The analysis shows that the 4D-NDTD effectively disrupts the original pixel distribution of the image.

2) CORRELATION

In common cryptanalysis, pixel correlation analysis is a crucial component. For meaningful plaintext images, pixel correlation provides sufficient information for visual comprehension. However, it also introduces the risk of attacks.

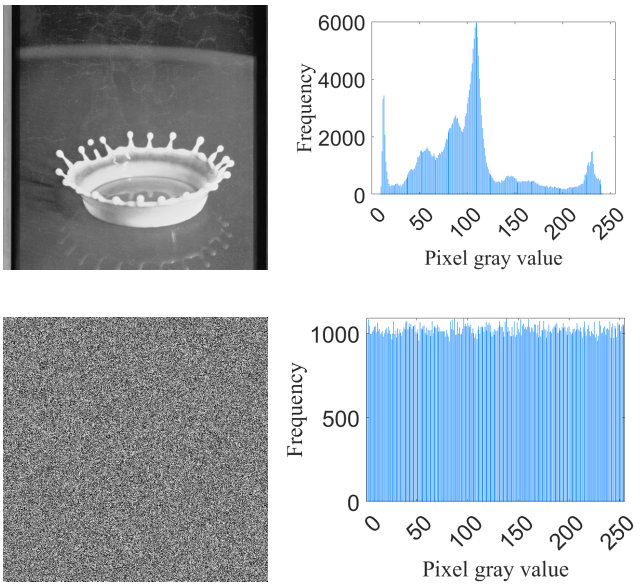

FIGURE 6. Results of the proposed 4D-NDTD: image histograms.

Therefore, the pixel correlation of encrypted images should be as low as possible, which is an essential aspect in evaluating the security of image encryption algorithms. The commonly used methods for calculating pixel correlation are as follows:

$$\begin{cases} E(x) = \dfrac{1}{N}\sum_{i=1}^{N} x_i \\ D(x) = \dfrac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \\ \mathrm{cov}(x,y) = \dfrac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \\ \gamma_{xy} = \dfrac{\mathrm{cov}(x,y)}{\sqrt{D(x)} \times \sqrt{D(y)}} \end{cases} \tag{21}$$

where x and y represent any two pixel values, $E(x)$ reflects an average of the overall pixel values, $D(x)$ embodies the value of the variance, cov(x,y) is the covariance between x and y, and γ_{xy} is the correlation coefficient.

The results of pixel correlation for the proposed algorithm are shown in FIGURE 7. Analysis reveals that the pixel correlation of the encrypted image is low in all directions, effectively resisting correlation attacks.

3) ENTROPY

Information entropy is an important measure of the randomness of image information, reflecting the uncertainty and complexity of image data. In image encryption, higher information entropy typically indicates stronger randomness and better encryption effectiveness. For common image encryption algorithms, there is typically a desired positive correlation between the magnitude of information entropy and the encryption results. Generally, the higher the

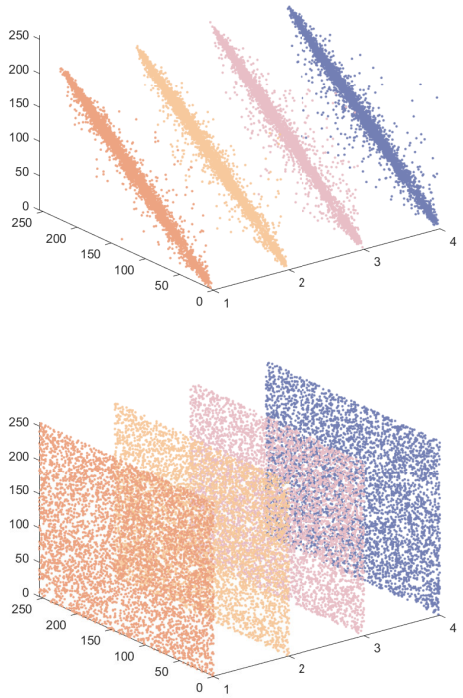

FIGURE 7. Results of the proposed 4D-NDTD: correlation characteristic: correlation of plain image and correlation of encrypted image.

information entropy, the better the encryption performance. The following equation is commonly used to calculate information entropy:

$$H(n) = -\sum_{i=0}^{H\times W-1} P(n_i)\log_2 P(n_i) \tag{22}$$

where P is the probability of calculating the gray value of a pixel. For digital images, the gray value range is limited.

The comparison of the information entropy between the proposed algorithm and other algorithms is presented in TABLE 3. The results demonstrate that our algorithm achieves sufficient security in terms of information entropy, effectively resisting related attacks.

TABLE 3. The comparison of the information entropy with different algorithms.

Images	2024 [39]	2024 [40]	2023 [43]	Proposed
'Baboon'	7.9993	**7.9994**	7.9986	7.9993
'Peppers'	-	**7.9994**	7.9992	7.9993
'Couple'	7.9993	-	7.9987	**7.9994**
'Boat'	-	7.9993	-	**7.9993**

D. ANALYSIS OF THE SENSITIVITY OF 4D-NDTD

1) KEY SENSITIVITY

Key sensitivity is used to evaluate how sensitive the sequences generated by the chaotic system are to changes in the key. By slightly adjusting the initial values of the 4D-NDS and analyzing the differences in the generated sequences, the system's sensitivity can be determined. The experimental results for key sensitivity in the 4D-NDS are shown in FIGURE 8. The results indicate that the initial value sensitivity precision of the chaotic system reaches $d = 10^{-17}$, providing robust security and ample key space for the encryption algorithm.

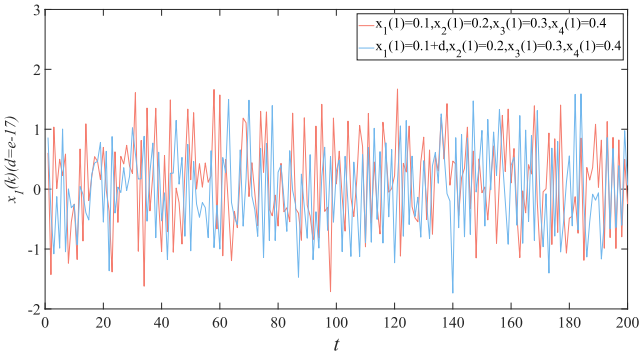

FIGURE 8. Results of the proposed 4D-NDS: demonstrating the effectiveness of chaotic sequences in timing diagrams with different initial values, highlighting the system's sensitivity to initial conditions.

2) PLAINTEXT SENSITIVITY

Plaintext sensitivity is a crucial metric for assessing an encryption algorithm's responsiveness to changes in the plaintext. In this experiment, a slight modification (with a value of 1) was made to a randomly chosen pixel in the plaintext image. The encryption algorithm was then applied to both the original and altered images, and their NPCR and UACI values were recorded. Typically, an encryption algorithm sensitive to plaintext changes should produce significantly different NPCR and UACI values under such conditions. The experimental data, as shown in FIGURE 9, indicates that the proposed algorithm is highly sensitive to plaintext changes and can effectively counteract related attacks.

E. ANALYSIS OF THE KEY SPACE OF 4D-NDTD

The proposed algorithm utilizes 4D-NDHC, with its key expressed as $x_n(1), \varepsilon_n, \sigma_n$, and the accuracy is 10^{-17}. An approximate estimate of the key space size is $10^{17\times 24} \approx 2^{1355}$. TABLE 4 illustrates that our proposed encryption scheme not only provides a substantial enhancement in the key space compared to existing methods, but also significantly improves the algorithm's robustness against a wide range of attacks.

TABLE 4. The comparison of the key space size with different algorithms.

	2024 [44]	2024 [45]	2023 [46]	Proposed
Key space/bits	425	427	159	**1355**

According to the comparison, the present algorithm has a larger key space and can provide stronger security. It is also resistant to more attacks, such as brute-force attacks.

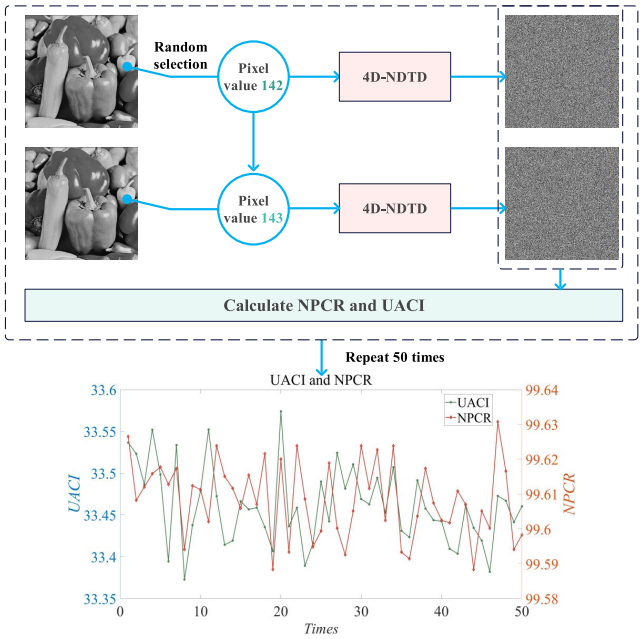

FIGURE 9. Results of the proposed 4D-NDTD: NPCR and UACI of randomly altered plain image pixels.

F. ANALYSIS OF THE ROBUSTNESS OF 4D-NDTD

1) CROPPING ATTACK

Cropping attacks, which remove parts of an image to affect the extraction of encrypted information, are a common type of attack in communication processes. In this section, we simulate the generation of cropped ciphertext and observe the results of the decrypted images. The encryption results are shown in FIGURE 10. By analyzing the decrypted images, we can still obtain the main information of the plaintext, indicating that the algorithm has a certain resistance to cropping attacks and exhibits robustness. This capability effectively enhances the reliability of the algorithm in real communication scenarios.

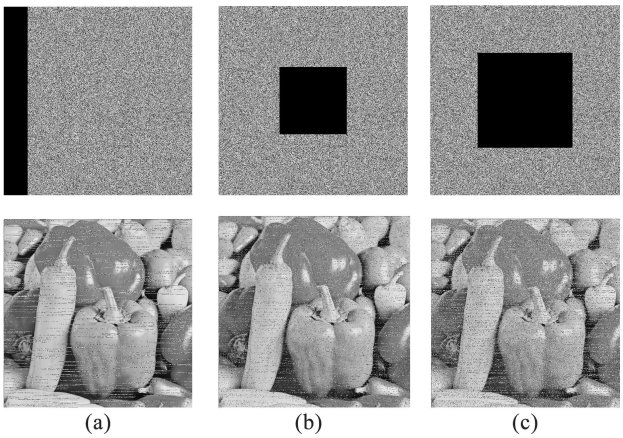

FIGURE 10. Visualization of the proposed 4D-NDTD: "Peppers" decrypted images with cropping: (a) cropping ratio of 12.5%; (b) cropping ratio of 12.5%; (c) cropping ratio of 25%.

2) SALT-AND-PEPPER NOISE

Salt-and-pepper noise can be utilized to simulate error noise in communication and evaluate the resistance of encryption algorithms to noise attacks. By introducing varying intensities of salt-and-pepper noise into encrypted images to mimic communication noise and subsequently decrypting them, the robustness of the algorithm can be assessed. The experimental results, depicted in FIGURE 11, demonstrate that the algorithm exhibits a certain level of resistance to salt-and-pepper noise, showcasing strong robustness, reliability, and security.

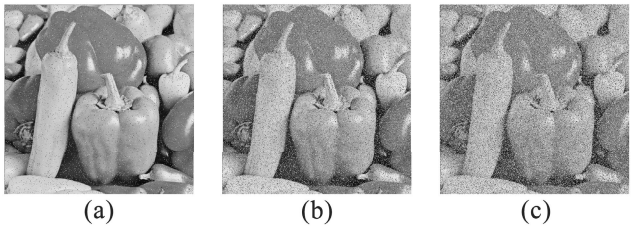

FIGURE 11. Visualization of the proposed 4D-NDTD: "Peppers" decrypted images with Salt-and-Pepper noise: (a) level of 1%; (b) level of 5%; (c) level of 10%.

V. CONCLUSION

This paper proposes a dynamic encryption scheme for secure image communication. A non-degenerate hyper-chaotic system is introduced, which possesses remarkable dynamical characteristics and can effectively address the issues of insufficient algorithm sensitivity and limited key space. The single-round combined dynamic diffusion proposed in the algorithm also significantly enhances its security. The algorithm's sensitivity, correlation, and other properties have been verified through experiments. The information entropy is generally greater than 7.9993 for images of size 512×512, demonstrating excellent encryption performance. The paper will further explore the permutation methods and robustness of the algorithm to ensure that it can make further contributions to the field of information security.

REFERENCES

[1] S. Gao, H. Ho-Ching Iu, U. Erkan, C. Şimşek, J. Mou, A. Toktas, R. Wu, and X. Tang, "Design, dynamical analysis, and hardware implementation of a novel memcapacitive hyperchaotic logistic map," *IEEE Internet Things J.*, vol. 11, no. 18, pp. 30368–30375, Sep. 2024.

[2] Z. Xing, C.-T. Lam, X. Yuan, S.-K. Im, and P. Machado, "MMQW: Multi-modal quantum watermarking scheme," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 5181–5195, 2024.

[3] L. Zhang, Y. Lin, X. Yang, T. Chen, X. Cheng, and W. Cheng, "From sample poverty to rich feature learning: A new metric learning method for few-shot classification," *IEEE Access*, vol. 12, pp. 124990–125002, 2024.

[4] Z. Xing, X. Yuan, C. Lam, and P. Machado, "NGQR: A novel generalized quantum image representation," *IEEE Trans. Emerg. Topics Comput.*, early access, Oct. 7, 2024, doi: 10.1109/TETC.2024.3471086.

[5] X. Chai, S. Song, Z. Gan, G. Long, Y. Tian, and X. He, "CSENMT: A deep image compressed sensing encryption network via multi-color space and texture feature," *Expert Syst. Appl.*, vol. 241, May 2024, Art. no. 122562.

[6] X. Wang, X. Yuan, M. Li, Y. Sun, J. Tian, H. Guo, and J. Li, "Parallel multiple watermarking using adaptive inter-block correlation," *Expert Syst. Appl.*, vol. 213, Mar. 2023, Art. no. 119011.

[7] O. Kocak, U. Erkan, A. Toktas, and S. Gao, "PSO-based image encryption scheme using modular integrated logistic exponential map," *Expert Syst. Appl.*, vol. 237, Mar. 2024, Art. no. 121452.

[8] Y. Sun, X. Yuan, T. Liu, G. Huang, Z. Lin, and J. Li, "FRRW: A feature extraction-based robust and reversible watermarking scheme utilizing Zernike moments and histogram shifting," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 35, no. 8, Sep. 2023, Art. no. 101698.

[9] L. Huang and H. Gao, "Multi-image encryption algorithm based on novel spatiotemporal chaotic system and fractal geometry," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 71, no. 8, pp. 3726–3739, Aug. 2024.

[10] C. Zhang, J. Chen, D. Chen, W. Wang, Y. Zhang, and Y. Zhou, "Exploiting substitution box for cryptanalyzing image encryption schemes with DNA coding and nonlinear dynamics," *IEEE Trans. Multimedia*, vol. 26, pp. 1114–1128, 2024.

[11] L. Dai, L. Hu, L. Chen, C. Wang, and F. Lin, "An image double encryption based on improved GAN and hyper chaotic system," *IEEE Access*, vol. 12, pp. 135779–135798, 2024.

[12] B. Long, Z. Chen, T. Liu, X. Wu, C. He, and L. Wang, "A novel medical image encryption scheme based on deep learning feature encoding and decoding," *IEEE Access*, vol. 12, pp. 38382–38398, 2024.

[13] Y. M. Khazaal, A. Douik, and M. Kherallah, "Smart pixels: Harnessing deep learning and Fibonacci decomposition for image ciphering," *IEEE Access*, vol. 12, pp. 130723–130735, 2024.

[14] H. Wen, Y. Lin, L. Yang, and R. Chen, "Cryptanalysis of an image encryption scheme using variant Hill cipher and chaos," *Expert Syst. Appl.*, vol. 250, Sep. 2024, Art. no. 123748.

[15] H. Wen, Y. Lin, and Z. Feng, "Cryptanalyzing a bit-level image encryption algorithm based on chaotic maps," *Eng. Sci. Technol., Int. J.*, vol. 51, Mar. 2024, Art. no. 101634.

[16] H. Wen and Y. Lin, "Cryptanalyzing an image cipher using multiple chaos and DNA operations," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 35, no. 7, Jul. 2023, Art. no. 101612.

[17] K. Gao, C.-C. Chang, and C.-C. Lin, "Key-free image encryption algorithm based on self-triggered Gaussian noise sampling," *IEEE Access*, vol. 12, pp. 153274–153284, 2024.

[18] J. Shao, E. Bai, X. Jiang, and Y. Wu, "Multi-view light field images compression and encryption using enhanced 3D chaotic system and pixel-bit-scrambling," *IEEE Access*, vol. 12, pp. 156471–156491, 2024.

[19] H. Wen, Y. Lin, Z. Xie, and T. Liu, "Chaos-based block permutation and dynamic sequence multiplexing for video encryption," *Sci. Rep.*, vol. 13, no. 1, p. 14721, Sep. 2023.

[20] H. Wen, S. Kang, Z. Wu, Y. Lin, and Y. Huang, "Dynamic RNA coding color image cipher based on chain feedback structure," *Mathematics*, vol. 11, no. 14, p. 3133, Jul. 2023.

[21] M. Tang, G. Du, and Y.-Y. Lin, "A novel multi-color image compression encryption algorithm based on the reconstruction coefficient matrix and DNA point mutation operation," *Expert Syst. Appl.*, vol. 270, Apr. 2025, Art. no. 126620.

[22] N. Iqbal, A. Banga, N. Innab, B. M. ElZaghmouri, A. Ikram, and H. Diab, "Utilizing the nth root of numbers for novel random data calculus and its applications in network security and image encryption," *Expert Syst. Appl.*, vol. 265, Mar. 2025, Art. no. 125992.

[23] D. Singh and S. Kumar, "Image authentication and encryption algorithm based on RSA cryptosystem and chaotic maps," *Expert Syst. Appl.*, vol. 274, May 2025, Art. no. 126883.

[24] A. Mansouri, P. Sun, C. Lv, Y. Zhu, X. Zhao, H. Ge, and C. Sun, "A secure medical image encryption algorithm for IoMT using a quadratic-sine chaotic map and pseudo-parallel confusion-diffusion mechanism," *Expert Syst. Appl.*, vol. 270, Apr. 2025, Art. no. 126521.

[25] Q. Lai and H. Hua, "Secure medical image encryption scheme for healthcare IoT using novel hyperchaotic map and DNA cubes," *Expert Syst. Appl.*, vol. 264, Mar. 2025, Art. no. 125854.

[26] F.-Q. Meng and G. Wu, "A color image encryption and decryption scheme based on extended DNA coding and fractional-order 5D hyper-chaotic system," *Expert Syst. Appl.*, vol. 254, Nov. 2024, Art. no. 124413.

[27] Z. Xie, Y. Lin, T. Liu, and H. Wen, "Face privacy protection scheme by security-enhanced encryption structure and nonlinear dynamics," *IScience*, vol. 27, no. 9, Sep. 2024, Art. no. 110768.

[28] C. Chen, F. Min, J. Cai, and H. Bao, "Memristor synapse-driven simplified Hopfield neural network: Hidden dynamics, attractor control, and circuit implementation," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 71, no. 5, pp. 2308–2319, May 2024.

[29] S. Gao, Z. Zhang, H. H.-C. Iu, S. Ding, J. Mou, U. Erkan, A. Toktas, Q. Li, C. Wang, and Y. Cao, "A parallel color image encryption algorithm based on a 2D logistic-rulkov neuron map," *IEEE Internet Things J.*, early access, Feb. 10, 2025, doi: 10.1109/JIOT.2025.3540097.

[30] S. Gao, H. H.-C. Iu, U. Erkan, C. Simsek, A. Toktas, Y. Cao, R. Wu, J. Mou, Q. Li, and C. Wang, "A 3D memristive cubic map with dual discrete memristors: Design, implementation, and application in image encryption," *IEEE Trans. Circuits Syst. Video Technol.*, early access, Feb. 26, 2025, doi: 10.1109/TCSVT.2025.3545868.

[31] J. Zheng and T. Bao, "An image encryption algorithm based on cascade chaotic map and DNA coding," *IET Image Process.*, vol. 17, no. 12, pp. 3510–3523, Oct. 2023.

[32] X. Xue, H. Jin, and C. Zhou, "Compressive sensing and DNA coding operation: Revolutionary approach to colour medical image compression-encryption algorithm," *IET Image Process.*, vol. 18, no. 14, pp. 4589–4606, Dec. 2024.

[33] K. İnce, C. İnce, and D. Hanbay, "Random strip peeling: A novel lightweight image encryption for IoT devices based on colour planes permutation," *CAAI Trans. Intell. Technol.*, vol. 2025, pp. 1–16, Jan. 2025.

[34] X. Wang, C. Zhang, W. Zeng, and Y. Luo, "Data center secure communication via DNA hyperchaotic encryption," *J. Lightw. Technol.*, vol. 42, no. 16, pp. 5564–5572, Aug. 15, 2024.

[35] Y. Luo, X. Liang, C. Zhang, W. Zeng, and K. Qiu, "Redundancy-free key distribution using multiple phase offset for secure data center," *J. Lightw. Technol.*, vol. 42, no. 2, pp. 523–531, Jan. 15, 2024.

[36] S. Gao, H. H.-C. Iu, M. Wang, D. Jiang, A. A. A. El-Latif, R. Wu, and X. Tang, "Design, hardware implementation, and application in video encryption of the 2-D memristive cubic map," *IEEE Internet Things J.*, vol. 11, no. 12, pp. 21807–21815, Jun. 2024.

[37] Q. Zhang, X. Yuan, T. Liu, C.-T. Lam, G. Huang, D. Lin, and P. Li, "Tampering localization and self-recovery using block labeling and adaptive significance," *Expert Syst. Appl.*, vol. 226, Sep. 2023, Art. no. 120228.

[38] H. Wen, Z. Liu, H. Lai, C. Zhang, L. Liu, J. Yang, Y. Lin, Y. Li, Y. Liao, L. Ma, Z. Chen, and R. Li, "Secure DNA-coding image optical communication using non-degenerate hyperchaos and dynamic secret-key," *Mathematics*, vol. 10, no. 17, p. 3180, Sep. 2022.

[39] H. Zhao, S. Wang, and Z. Fu, "A new image encryption algorithm based on cubic fractal matrix and L-LCCML system," *Chaos, Solitons Fractals*, vol. 185, Aug. 2024, Art. no. 115076.

[40] E. Winarno, W. Hadikurniawati, K. Nugroho, and V. Lusiana, "Integrating quadratic polynomial and symbolic chaotic map-based feistel network to improve image encryption performance," *IEEE Access*, vol. 12, pp. 106720–106734, 2024.

[41] L. Li, "A self-reversible image encryption algorithm utilizing a novel chaotic map," *Nonlinear Dyn.*, vol. 113, no. 7, pp. 7351–7383, Jan. 2025.

[42] J. Lu, J. Zhang, D. An, D. Hao, X. Ren, and R. Zhao, "A low-time-consumption image encryption combining 2D parametric Pascal matrix chaotic system and elementary operation," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 36, no. 8, Oct. 2024, Art. no. 102169.

[43] H. Zhang, H. Hu, and W. Ding, "VSDHS-CIEA: Color image encryption algorithm based on novel variable-structure discrete hyperchaotic system and cross-plane confusion strategy," *Inf. Sci.*, vol. 665, Apr. 2024, Art. no. 120332.

[44] T. Umar, M. Nadeem, and F. Anwer, "Chaos based image encryption scheme to secure sensitive multimedia content in cloud storage," *Expert Syst. Appl.*, vol. 257, Dec. 2024, Art. no. 125050.

[45] X. Gao, J. Mou, B. Li, S. Banerjee, and B. Sun, "Multi-image hybrid encryption algorithm based on pixel substitution and gene theory," *Fractals*, vol. 31, no. 6, Jan. 2023, Art. no. 2340111.

YUNLONG LIAO received the Bachelor of Engineering degree from the University of Electronic Science and Technology of China Zhongshan Institute, in 2022. He is currently pursuing the master's degree in big data and the Internet of Things with the Faculty of Applied Sciences, Macao Polytechnic University. His research interests include multimedia security, image processing, AI security, and cryptography.

YITING LIN (Member, IEEE) received the B.Sc. degree in computer science and technology from the University of Electronic Science and Technology of China Zhongshan Institute, in 2024. He is currently a Research Assistant with Guangdong Provincial/Zhuhai Key Laboratory of Interdisciplinary Research and Application for Data Science, Beijing Normal-Hong Kong Baptist University. He holds a teaching and research position with the University of Electronic Science and Technology of China Zhongshan Institute. He has published over 20 SCI-indexed articles and received five invention patents and more than ten computer software copyrights. As of 2024, he has authored nine highly cited papers according to the Essential Science Indicators (ESI), and one hot paper according to ESI. His research interests include cryptography, blockchain, information security, multimedia security, artificial intelligence (ML/DL), signal processing, and nonlinear dynamics.

QIUTONG LI received the B.S. degree in engineering from Nantong Institute of Technology, in 2023. She is currently pursuing the M.S. degree in big data and the Internet of Things with the Faculty of Applied Sciences, Macau Polytechnic University. Her research interests include robust watermarking technology, image processing, and deep learning.

ZHENG XING received the B.S. degree in computer science and technology from Zhengzhou University, Henan, China, in 2014, and the M.S. degree in computer technology from Chongqing University of Posts and Telecommunications, Chongqing, China, in 2017. He is currently pursuing the Ph.D. degree in computer application technology with the Faculty of Applied Sciences, Macao Polytechnic University. From 2018 to 2021, he was a Lecturer with the College of Mobile Communication, Chongqing University of Posts and Telecommunications. His research interests include quantum secure communication, quantum computing protocols, and quantum cryptography.

XIAOCHEN YUAN (Senior Member, IEEE) received the Ph.D. degree in software engineering from the University of Macau, in 2013. From 2014 to 2015, she was a Postdoctoral Fellow with the Department of Computer and Information Science, University of Macau. From 2016 to 2021, she was an Assistant Professor and an Associate Professor with the Faculty of Information Technology, Macau University of Science and Technology. She is currently an Associate Professor with the Faculty of Applied Sciences, Macao Polytechnic University. Her research interests include multimedia forensics and security, digital watermarking, AI model security, quantum watermarking, remote image processing, and deep learning techniques and applications.