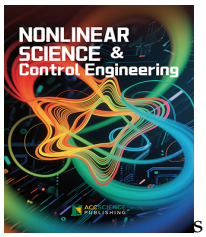
Contents lists available at AccScience Publishing
Nonlinear Science and Control Engineering (NSCE)
Vol. 1, No. 2 (2025)
https://accscience.com/journal/nsce



Lightweight image encryption via four-dimensional Hénon memristor map and fast block permutation

Yiting Lin[1,2], Yunlong Liao[3], Yunan Wei[1,2], Wenjun Zeng[4], Ugur Erkan[5], Abdurrahim Toktas[5], Yong Zhang[6], and Donglong Chen[1,2*]

[1]*Guangdong Provincial/Zhuhai Key Laboratory of Interdisciplinary Research and Application for Data Science, Beijing Normal-Hong Kong Baptist University, Zhuhai, Guangdong, China*
[2]*Department of Computer Science, Hong Kong Baptist University, Hong Kong, China*
[3]*Faculty of Applied Sciences, Macao Polytechnic University, Macao SAR, China*
[4]*The Key Lab of Optical Fiber Sensing and Communications (MOE), School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu, Sichuan, China*
[5]*Department of Artificial Intelligence and Data Engineering, Engineering Faculty, Ankara University, Ankara, Turkey*
[6]*School of Computing and Artificial Intelligence, Jiangxi University of Finance and Economics, Nanchang, Jiangxi, China*

Article History:
Received: September 25, 2025
Revised: October 14, 2025
Accepted: October 20, 2025
Published online: November 12, 2025

ABSTRACT

With the rapid proliferation of multimedia data in the big data era, digital image security has become an urgent research concern. To address the trade-off between efficiency and robustness, this paper proposes a chaos-driven image encryption scheme based on a four-dimensional Hénon memristor map (4D-HMM). First, the plaintext image is adaptively embedded into the secret key via SHA-256 perturbation, ensuring strong plaintext sensitivity. Then, pseudo-random sequences generated by the 4D-HMM are employed to drive a four-stage encryption framework consisting of fast block permutation, block rotation/flip, negative–positive transformation, and color channel permutation. Finally, lightweight bitwise diffusion and convolution-based diffusion are successively applied to achieve pixel-level scrambling and global avalanche effects. Experimental results show that the proposed scheme achieves excellent security metrics, including uniform histograms, information entropy values close to the ideal, low pixel correlation, and a large key space. Moreover, differential attack resistance is validated by the number of pixels change rate and unified average changing intensity results approaching theoretical values, while avalanche tests confirm that a single-bit change in the plaintext or key leads to significant, unpredictable variations in the ciphertext. The scheme thus provides both high efficiency and strong cryptographic security, making it suitable for real-time multimedia protection in modern communication environments.

Keywords: Multimedia security; Image encryption; Chaotic encryption; Hénon hyperchaos system

***Corresponding author**:
Donglong Chen (donglongchen@uic.edu.cn).

Citation:
Lin Y, Liao Y, Wei Y, Zeng W, Erkan U, Toktas A, Zhang Y, and Chen D. Lightweight image encryption via four-dimensional Hénon memristor map and fast block permutation. *Nonlinear Sci Cont Eng*. 2025;1(2):025390012. doi: 10.36922/NSCE025390012

1. Introduction

With the rapid development of computer communication and network technologies in recent years, various forms of digital data can now be transmitted more frequently, widely, and efficiently through public networks. While this unprecedented connectivity greatly enhances information sharing and service accessibility, it also raises serious concerns regarding data privacy, integrity, and security.[1–4] Among different types of multimedia, digital images stand out as one of the most visual and frequently transmitted carriers of sensitive information, widely used in fields such as medical diagnosis, military reconnaissance, cloud storage, and social networking. Once intercepted or tampered with, these images may cause irreparable privacy violations or economic losses. Therefore, reliable and efficient image encryption techniques are urgently needed to safeguard critical data against unauthorized access during transmission and storage.[5–7] Over the past decades, various image encryption strategies have been proposed, including biological coding,[8] and transform-domain methods such as discrete wavelet transform (DWT),[9] discrete cosine transform (DCT),[10] and Fourier transform.[11] Other approaches have focused on bit-level substitution,[12] permutation-based scrambling,[13] and hybrid frameworks.[14] Although these techniques have achieved varying degrees of success, many face inherent trade-offs between computational efficiency, encryption strength, and adaptability to modern communication environments. Among these approaches, chaos-based image encryption has attracted the greatest attention due to its inherent unpredictability, pseudo-randomness, and extreme sensitivity to initial conditions.[15–19] Chaotic systems possess the capability to generate complex, non-repetitive key streams and induce significant diffusion and confusion effects across image pixels.[20–22] These properties make chaotic dynamics particularly well-suited for cryptographic applications, enabling resistance against brute-force, statistical, and differential attacks.[23–25]

With the rapid development of digital communication technologies, particularly the Internet and mobile applications, the transmission and storage of consumer-related image data in cloud platforms have surged dramatically. This shift has further underscored the importance of encryption for safeguarding user privacy and security in distributed environments. To meet these needs, increasingly more encryption methods have been proposed.[26–28] Obaid et al.[29] propose a reliable color image encryption scheme based on a novel dual-wing hyperchaotic map, utilizing hyperchaotic dynamics, BIBO stability criteria, and bifurcation theory to achieve secure and efficient image encryption. The method adopts a confusion–diffusion architecture that combines pixel position scrambling and bitwise XOR-based pixel value alteration, capable of processing standard color images (e.g., 256×256 and 512×512). It demonstrates significant advantages in key space, information entropy (close to 8), pixel correlation (near zero), and resistance to data loss, especially showing strong robustness against brute-force, statistical, and data loss attacks. Lu et al.[30] propose a multiple-image encryption algorithm based on a new three-dimensional (3D) hyperchaotic map and Whac-A-Mole scrambling model, utilizing 3D hyperchaotic dynamics, dice rotation, and Cartesian product-based spatial diffusion to achieve secure and efficient batch image encryption. The method adopts a fusion-scrambling-diffusion architecture, capable of simultaneously encrypting multiple images of varying sizes, and demonstrates significant advantages in encryption speed (0.1156 s for 256×256 images), information entropy (7.9999), key sensitivity, and resistance to various attacks, especially showing strong robustness against statistical, differential, noise, and cropping attacks. Liu et al.[31] propose a semantically enhanced selective image encryption scheme with parallel computing, utilizing lightweight deep salient object detection (EDN-lite), LICC hyperchaotic system, and reversible data hiding to achieve secure and efficient region of interest (ROI) encryption. The method adopts a detect-encrypt-embed pipeline, capable of processing high-resolution color images, and demonstrates significant advantages in encryption efficiency (up to 54% faster than serial methods), key sensitivity, and resistance to statistical and differential attacks, especially showing strong robustness in semantic accuracy, visual quality preservation, and side information protection. Furthermore, with the rapid development of information technology, a plethora of innovative technologies have emerged in the field of image encryption, ranging from traditional approaches based on chaotic systems to novel solutions that integrate cutting-edge methods such as deep learning, artificial intelligence, reversible data hiding, and semantic perception. These technologies not only play a crucial role in protecting image privacy but also drive a paradigm shift in image security from "full-image encryption" to "intelligent selective encryption." These technologies provide efficient, secure, and low-latency privacy protection solutions for diverse scenarios such as medical imaging, military communications, and social media, significantly expanding the application boundaries and research depth of image encryption.

This paper proposes an image encryption scheme based on the four-dimensional (4D) Hénon memristor map (4D-HMM). The 4D-HMM serves as the core pseudo-random generator, tightly coupled to the plaintext by perturbing the initial key using SHA-256. The pseudo-random sequence generated by the 4D-HMM is processed and then used in a fast block permutation module and a two-stage diffusion pipeline (lightweight bitwise diffusion and convolutional diffusion). The main innovations and contributions of this paper are summarized as follows:

(i) A novel plaintext-dependent key perturbation mechanism is proposed by embedding SHA-256 hash values of the plaintext image into the initialization of the 4D-HMM. This adaptive key disturbance ensures that the generated chaotic sequences are tightly coupled with the plaintext, thereby improving sensitivity, enhancing resistance to chosen-plaintext attacks, and significantly expanding the effective key space.

(ii) An efficient, fast block permutation framework is designed, where four 4D-HMM-generated sequences control block-level permutation, block rotation/flip, negative–positive transformation, and RGB channel permutation. By combining these complementary operations, the scheme achieves strong spatial confusion, effectively disrupts the correlation between adjacent pixels, and enhances the robustness of the overall encryption process.

(iii) A dual-stage diffusion strategy is introduced, consisting of lightweight bitwise diffusion and convolution-based diffusion. The first stage

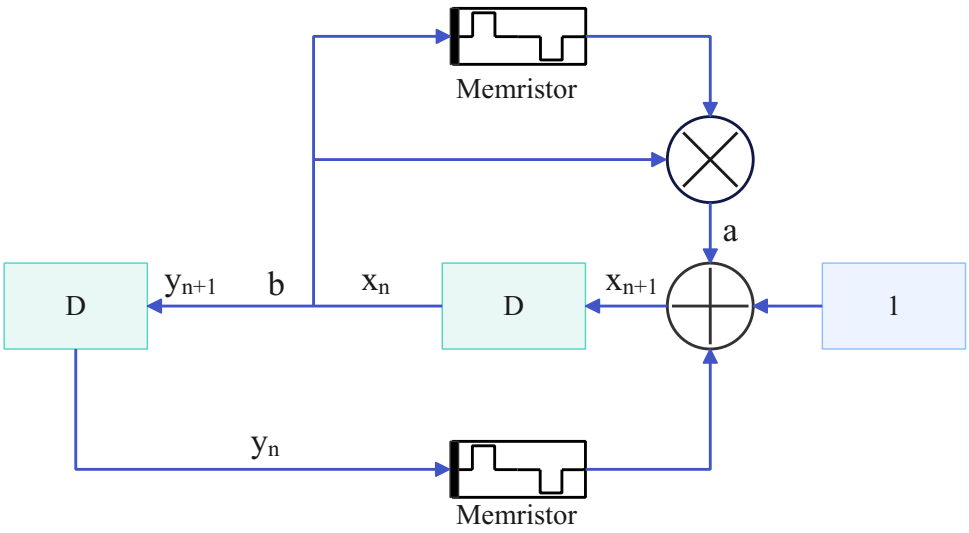


Figure 1. The structure diagram of chaotic mapping based on discrete memristor

ensures rapid local diffusion through XOR and circular shift operations, while the second stage provides global avalanche propagation by convolutional mixing of neighboring pixels. This layered design guarantees that a single-bit change in the plaintext or key leads to widespread, unpredictable changes in the ciphertext, thereby strengthening resistance to differential, statistical, and cryptanalytic attacks while maintaining computational efficiency.

Section 1 introduces the structure of this paper. Section 2 presents the 4D-HMM implementation. Section 3 introduces the proposed encryption scheme. Section 4 discusses and analyzes the numerical experiments and security performance of the proposed scheme. Finally, Section 5 concludes the paper.

2. The proposed four-dimensional Hénon memristor map associated with the plain image

Liu et al.[32] proposed a chaotic system based on two types of memristors and the Hénon map, which exhibits excellent dynamical characteristics. The chaotic system is defined as follows in Equation (1):

$$\begin{cases} x_{n+1} = 1 + (c + dsin(u_n))y_n - a(e + gcos(w_n))z_n x_n), \\ y_{n+1} = bx_n, \\ z_{n+1} = z_n + kx_n, \\ w_{n+1} = w_n + kz_n, \\ z_{n+1} = z_n + ky_n. \end{cases} \tag{1}$$

To facilitate the deployment of the chaotic system on edge devices, especially in contexts where circuit-level implementation is necessary, this paper introduces an improved design derived from the original system. Specifically, the two types of memristors previously employed were simplified to a single type, thereby reducing the variety and complexity of components. For convenience of reference, the system is referred to as the 4D-HMM map in this paper. The corresponding modified circuit structure is illustrated in Figure 1.

Based on the analysis of the circuit schematic, the corresponding chaotic map can be expressed as follows in Equation (2):

$$\begin{cases} x_{n+1} = 1 + (c + dsin(w_n))y_n - a(c + dsin(z_n)x_n^2), \\ y_{n+1} = bx_n, \\ z_{n+1} = z_n + kx_n, \\ w_{n+1} = w_n + ky_n. \end{cases} \tag{2}$$

where $(x_n,\ y_n,\ z_n,\ w_n)$ represents the system's state variables, namely the chaotic sequence generated through iteration. The parameters (a, b, c, d, k) are control parameters.

To verify the memristive property of the proposed 4D-HMM, a pinched hysteresis loop (PHL) test was conducted under sinusoidal voltage excitation. The hysteresis loop is the fundamental fingerprint of memristors, in which the current–voltage (i–v) characteristics exhibit a pinched loop crossing the origin. The internal state dynamics of the memristor emulator were modeled as Equation (3):

$$\frac{dw}{dt} = -\gamma w + \alpha v(t) + \beta\xi(t), \tag{3}$$

where w denotes the internal state variable, $v(t) = A\sin(2\pi ft)$ is the input voltage, and $\xi(t)$ is the normalized chaotic sequence generated by the 4D-HMM. The memductance was defined as Equation (4):

$$G(t) = G_{\min} + (G_{\max} - G_{\min})\left(\tfrac{1}{2} + \tfrac{1}{2}\tanh(w(t))\right), \tag{4}$$

and the current was obtained by $i(t) = G(t)\,v(t)$. In the simulation, parameters were set to $\alpha = 0.6$, $\beta = 0.02$, $\gamma = 0.15$, $G_{\min} = 0.05$, $G_{\max} = 3.0$, and the input frequency was $f = 0.05$, while the voltage amplitude was varied as $A = 0.5,\ 0.8,\ 1.0$.

The obtained i–v curves are shown in Figure 2. For all amplitudes, the hysteresis loops are clearly pinched at the origin, confirming the memristive nature of the system. As the amplitude increases, the loops expanded and became more pronounced, which agrees with the theoretical expectation that larger excitation signals induce stronger nonlinear conductance modulation. Moreover, the inclusion of chaotic perturbation $\xi(t)$ enriched the loop dynamics, avoiding degeneration into a linear resistor-like characteristic. These results demonstrate that the proposed

4D-HMM exhibits the essential fingerprint of a memristor and offers flexible controllability of its hysteresis behavior.

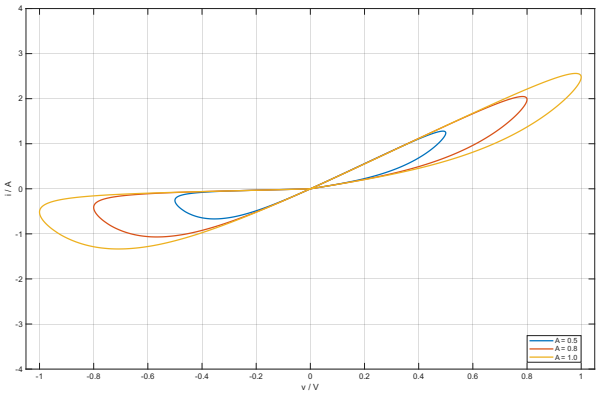


Figure 2. Pinched hysteresis loops of the proposed 4D-HMM under different excitation amplitudes

In this algorithm, the initial values x_0 to z_0 were set to 0.1, and the system parameters a, b, c, d, and k are assigned as 0.001, 1.8, 0.5, 0.4, and 0.1, respectively. Under this parameter configuration, the system exhibited a distinct, discrete chaotic behavior, and the corresponding chaotic attractor is illustrated in Figure 3. The attractor possesses a complex structure and exhibits high sensitivity to initial conditions, which significantly enhances the unpredictability and resistance to attacks of the encryption system.

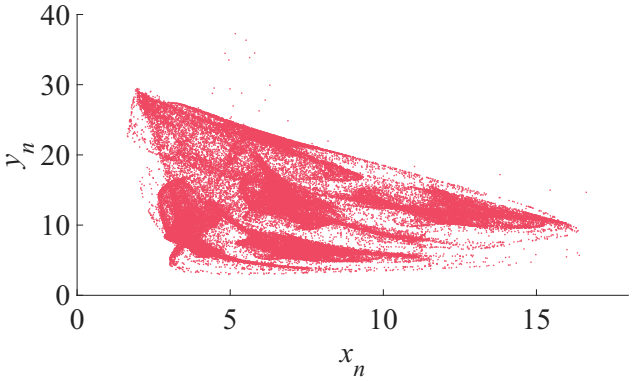


Figure 3. Visualization of proposed 4D-HMM chaotic maps: phase diagrams with different parameters

The dynamics of a chaotic system are represented by a key metric for quantifying the chaotic behavior of the system: the Lyapunov exponent. By calculating the Lyapunov exponent of the system, we arrived at 0.0390, 0.0143, -0.0001, and -0.1233, which is a hyperchaos system, and the results are displayed in Figure 4.

Fixed-point analysis and bifurcation diagrams were used to visualize the stability and instability of the system as the parameters vary. As shown in Figure 5, the bifurcation diagram clearly reveals the complexity of the system's behavior when the parameter b was varied and exhibited a clear chaotic effect as it approaches 1.7. This indicates that the system dynamics transitioned from an ordered state to a chaotic state that is highly sensitive to the initial conditions.

This study evaluated the randomness of a chaotic system using the NIST-800-22 standard, which comprehensively assesses random number generators. The results in Table 1 show that the system passes all tests, indicating that the key sequence and parameters used in encryption were sufficiently random to ensure the algorithm's security.

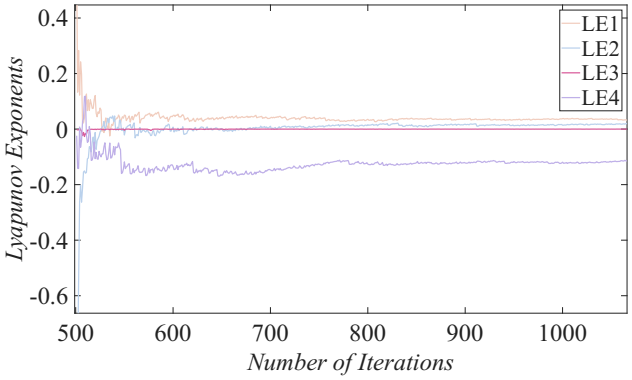


Figure 4. The proposed 4D-HMM: lyapunov exponents spectrum. The exponents tend to approach 0.0390, 0.0143, -0.0001, and -0.1233.

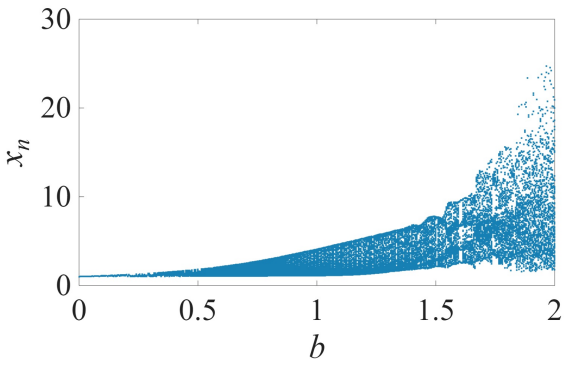


Figure 5. The proposed 4D-HMM: bifurcation diagram of x_n as a function of the parameter b. The parameter b has a chaotic behavior around 1.7

3. Proposed encryption Scheme

In this section, we present the proposed image encryption scheme. The plaintext image $P \in \mathbb{Z}_{256}^{h\times w\times 3}$ was transformed into the ciphertext image C through four major modules: (i) key perturbation and sequence generation, (ii) surrounding pixel addition, (iii) fast block permutation, (iv) lightweight bitwise diffusion, and (v) convolution-based diffusion. Each module is described in detail below with the formal mathematical expressions, where the meaning of each symbol is explicitly defined. The specific flowchart of the proposed encryption scheme is shown in Figure 6.

3.1. Key perturbation and sequence generation

To enhance plaintext sensitivity and resist chosen-plaintext attacks, the secret key was adaptively perturbed using the plaintext image P. Let the initial secret key be (x_0, y_0, z_0, w_0).

An SHA-256 hash of P was computed as Equation (5):

$$H = \mathrm{SHA256}(P), \tag{5}$$

where H is a 256-bit digest.

The first 16 bytes of H were grouped into four 32-bit integers and normalized as Equation (6):

Table 1. Results of the proposed 4D-HMM: NIST-800-22 Test

Statistical tests	*p*-value	Result
Frequency (Monobit) test	0.997823	Successful
Block-frequency test	0.129620	Successful
Cumulative-sums test	0.998821	Successful
Runs test	0.935716	Successful
Longest-run test	0.213309	Successful
Binary matrix rank test	0.554420	Successful
Discrete fourier transform test	0.115387	Successful
Non-overlapping templates test	0.991468	Successful
Overlapping templates test	0.191687	Successful
Maurer's universal statistical test	0.419021	Successful
Approximate entropy test	0.798139	Successful
Random-excursions test	0.931952	Successful
Random-excursions variant test	0.931952	Successful
Serial test	0.884308	Successful
Linear-complexity test	0.319084	Successful

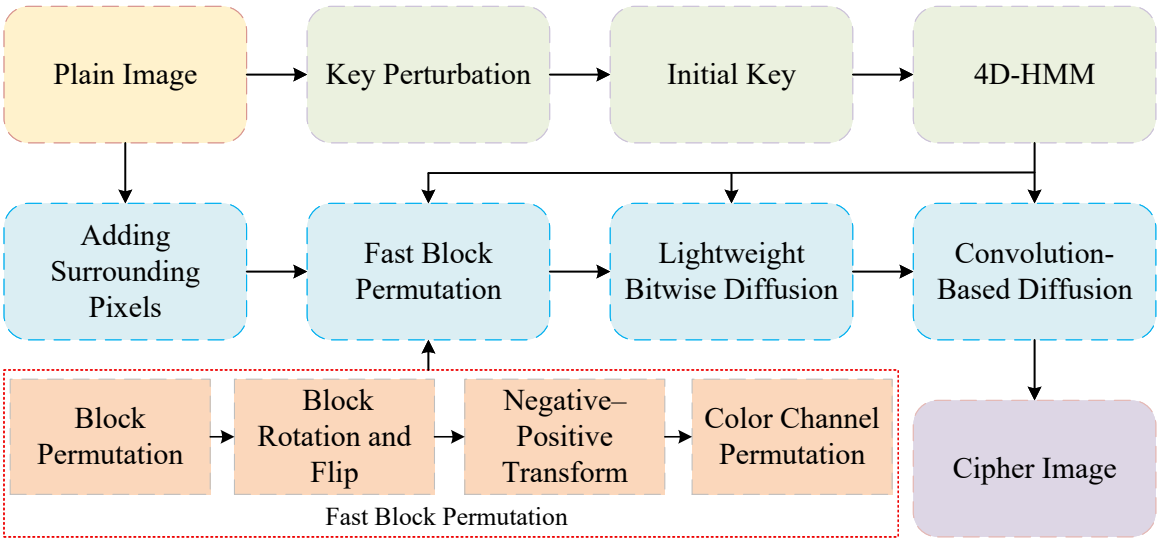


Figure 6. Flowchart of the proposed image encryption scheme

$$ld_j = \frac{1}{10^6}\sum_{i=0}^{7} \mathrm{H}(4i+j), \quad j = 1,2,3,4, \tag{6}$$

where $H_{(4i+j)}$ denotes the j-th 32-bit integer extracted from H, and $ld_j \in (0,1)$ are perturbation factors.

The perturbed initial states of the chaotic map are given by Equations (7–10):

$$x_0' = x_0 + ld_1, \tag{7}$$
$$y_0' = y_0 + ld_2, \tag{8}$$
$$z_0' = z_0 + ld_3, \tag{9}$$
$$w_0' = w_0 + ld_4, \tag{10}$$

where (x_0', y_0', z_0', w_0') are the perturbed initial conditions.

The nonlinear 4D-HMM evolved as Equation 2, where a, b, c, d, k are control parameters ensuring chaotic behavior, and (x_n, y_n, z_n, w_n) are the system states at iteration n.

After discarding $N_0 = 1,000$ transient iterations, four chaotic sequences were obtained:

$$S_1 = \{x_{N_0+1}, \ldots, x_{N_0+L}\}, \tag{11}$$
$$S_2 = \{y_{N_0+1}, \ldots, y_{N_0+L}\}, \tag{12}$$
$$S_3 = \{z_{N_0+1}, \ldots, z_{N_0+L}\}, \tag{13}$$
$$S_4 = \{w_{N_0+1}, \ldots, w_{N_0+L}\}, \tag{14}$$

where $L = h \times w$ is the total number of pixels.

3.2. Addition of surrounding pixels

Using Professor Hua's adding surrounding pixels[33] technique, random values were generated and added to the area surrounding the plaintext image. These values, after the obfuscation and diffusion operations, affected all pixels. Because these values are randomly generated and differ in each round of encryption, this crucial property enabled the cryptographic system to effectively defend

against common security attacks, such as chosen-plaintext attacks and brute-force attacks. The specific design involves adding a ring of pseudorandom numbers around the image. Assuming the plaintext image P is of size $M \times N$, a pseudorandom number generator was used to generate two random matrices NI of size $2 \times (N+2)$ and MI of size $M \times 2$. These matrices were then placed around the image.

3.3. Fast block permutation

The plaintext image P was divided into non-overlapping blocks of size $B \times B$, with $B = 8$ (The size of the block can be selected). The total number of blocks can be calculated using Equation (15):

$$N_b = \frac{h \times w}{B^2}, \tag{15}$$

where h, w denote the height and width of P, respectively.

The chaotic sequences S_1, S_2, S_3, S_4 were normalized as follows in Equations (16-19) :

$$S_1'(k) = \left\lfloor \frac{S_1(k) - \min(S_1)}{\max(S_1) - \min(S_1) + \epsilon} \cdot (N_b - 1) \right\rfloor + 1, \tag{16}$$

$$S_2'(k) = \mathrm{mod}(\mathrm{round}(S_2(k)), 6)\,, \tag{17}$$

$$S_3'(k) = \mathrm{mod}(\mathrm{round}(S_3(k)), 2)\,, \tag{18}$$

$$S_4'(k) = \mathrm{mod}(\mathrm{round}(S_4(k)), 6)\,, \tag{19}$$

where S_1' determines block permutation, S_2' controls block rotation/flip, S_3' determines the negative–positive transform, and S_4' controls channel permutation.

3.3.1. Block permutation

Let $\mathcal{B}_k$ denote the k-th image block in raster order. The permutation is controlled by S_1':

$$\mathcal{B}'_{\pi(k)} = \mathcal{B}_k, \tag{20}$$

where $\pi(k) = S_1'(k)$ specifies the destination index of block k.

3.3.2. Block rotation and flip

Each block $\mathcal{B}_k'$ is rotated or flipped according to $S_2'(k)$:

$$\mathcal{B}_k'' = \begin{cases} \mathrm{Rot}_{90}(\mathcal{B}_k'), & S_2'(k) = 1, \\ \mathrm{Rot}_{180}(\mathcal{B}_k'), & S_2'(k) = 2, \\ \mathrm{Rot}_{270}(\mathcal{B}_k'), & S_2'(k) = 3, \\ \mathrm{Flip}_H(\mathcal{B}_k'), & S_2'(k) = 4, \\ \mathrm{Flip}_V(\mathcal{B}_k'), & S_2'(k) = 5, \\ \mathcal{B}_k', & S_2'(k) = 0, \end{cases} \tag{21}$$

where Rot_θ denotes rotation by θ degrees, and $\mathrm{Flip}_H, \mathrm{Flip}_V$ denotes horizontal and vertical flips.

3.3.3. Negative–positive transform

For each pixel $p \in \mathcal{B}_k''$, the sequence $S_3'(k)$ determines

$$p' = \begin{cases} 255 - p, & S_3'(k) = 0, \\ p \oplus 1, & S_3'(k) = 1, \end{cases} \tag{22}$$

where $\oplus$ denotes bitwise XOR, and $p' \in [0, 255]$.

3.3.4. Color channel permutation

To further increase the complexity of the encryption process, the three color channels (R, G, B) of each block were permuted under the control of the sequence S_4. Each block $\mathcal{B}$, $S_4(k) \in \{0, 1, 2, 3, 4, 5\}$ determine the transformation rule. The complete set of channel permutations is defined as follows:

$$\Pi_0(R, G, B) = (R, G, B), \tag{23}$$

$$\Pi_1(R, G, B) = (R, B, G), \tag{24}$$

$$\Pi_2(R, G, B) = (G, R, B), \tag{25}$$

$$\Pi_3(R, G, B) = (B, G, R), \tag{26}$$

$$\Pi_4(R, G, B) = (B, R, G), \tag{27}$$

$$\Pi_5(R, G, B) = (G, B, R), \tag{28}$$

where (R, G, B) are the original red, green, and blue channels, and Π_j $(j = 0, 1, \ldots, 5)$ denotes the j-th permutation. Specifically, it Π_0 leaves the order unchanged, while Π_1–Π_5 correspond to all non-trivial re-orderings of the three channels. These transformations were implemented using XOR-swap operations to prevent data loss and to maintain reversibility during decryption.

3.4. Lightweight bitwise diffusion

Let I_c denote a single color channel of the permuted image, and $S \in \{0, \ldots, 255\}^{h \times w}$ be a chaotic mask reshaped to match I_c. The diffusion process is defined as Equation (29):

$$C(i,j) = \begin{cases} I(i,j) \oplus (I(h,w) \oplus S(1,1)), & (i,j) = (1,1), \\ I(i,j) \oplus (C(i-1,w) \oplus S(i,1)), & j = 1,\ i > 1, \\ I(i,j) \oplus (C(i,j-1) \oplus S(i,j)), & j > 1, \end{cases} \tag{29}$$

where $I(i,j)$ is the pixel at position (i,j) in I_c, $C(i,j)$ is the corresponding ciphertext pixel, and $S(i,j)$ is the chaotic mask element.

This scheme ensures that the diffusion of each pixel depends on its predecessor and chaotic randomness, achieving high sensitivity.

3.5. Convolution-based diffusion

To further enhance security, convolution-based diffusion is applied. Chaotic sequences S_1, S_2 generated two integer sequences:

$$K_r = \lfloor \mathrm{mod}(S_1 \cdot 10^4, 255) \rfloor, \tag{30}$$

$$K_c = \lfloor \mathrm{mod}(S_2 \cdot 10^4, 255) \rfloor, \tag{31}$$

where K_r and K_c are row and column keys.

A composite key K was formed and converted to binary as Equation (32):

$$K = \mathrm{reshape}(\mathrm{de2bi}(K_0, 8, \text{'left-msb'}), 1, []), \tag{32}$$

where K_0 is the concatenated sequence of K_r and K_c.

From K, convolution weights are derived as Equation (33):

$$A(i) = \mathrm{bi2de}(K(24 + 12(i-1) + 1 : 24 + 12i), \text{'left-msb'}), \tag{33}$$

where $i = 1, \ldots, 8$, $A(i)$ are decimal values from binary segments of K.

The forward convolution mask is expressed as Equation (34):

$$\mathrm{M} = \begin{bmatrix} W_1 & W_2 & W_3 \\ W_4 & W_5 & W_6 \\ W_7 & W_8 & 1 \end{bmatrix}, \tag{34}$$

and the inverse mask as Equation (35):

$$\mathrm{IM} = \begin{bmatrix} W_1 & W_2 & W_3 \\ W_4 & W_5 & W_6 \\ W_7 & W_8 & 0 \end{bmatrix}, \tag{35}$$

where W_i are weights derived from $A(i)$ after sorting.

For encryption, each pixel was updated as Equation (36):

$$C(i,j) = \mathrm{mod}(\Big(\sum_{u=1}^{3}\sum_{v=1}^{3} I(i-u, j-v)\cdot \mathrm{M}(u,v) + j\Big), 256), \tag{36}$$

where $I(i,j)$ is the input pixel and $C(i,j)$ is the ciphertext pixel.

For decryption, the inverse operation was applied as Equation (37):

$$I(i,j) = \mathrm{mod}(\Big(C(i,j) - \textstyle\sum_{u=1}^{3}\sum_{v=1}^{3} C(i-u, j-v)\cdot \mathrm{IM}(u,v) - j\Big), 256), \tag{37}$$

This convolutional mechanism guarantees strong diffusion, ensuring that each ciphertext pixel depends on multiple neighbors, thus providing robustness against differential attacks.

4. Experimental validation and discussion

In this algorithm, the digital image encryption algorithm was tested and confirmed through the use of MATLAB 2025a. The testing was conducted on a personal computer that featured a 64-bit Windows 11 operating system, powered by an AMD Ryzen 9-5950X-CPU with Radeon RX6950XT graphics, and had 128 GB of RAM installed. The experiments provided a comprehensive assessment of the security and reliability of the algorithms, including the algorithmic key space, statistical distribution characteristics, sensitivity, and resistance to cropping attacks.

4.1. Analysis of the statistical properties

4.1.1. Histogram

By comparing the histograms of the original and encrypted images, changes in the pixel intensity distribution can be observed. As shown in Figure 7, the uniform pixel distribution of the encrypted image implies that the result is random, thus enhancing security.

4.1.2. Correlation

Pixel correlation is an important metric for measuring the effectiveness of image encryption. It refers to whether there is a recognizable pattern or correlation between adjacent pixels in an image. The calculation formula is as follows in Equation (38):

$$\begin{cases} E(x) = \frac{1}{N}\sum_{N}^{i=1} x_i \\ D(x) = \frac{1}{N}\sum_{N}^{i=1} (x_i - E(x))^2 \\ cov(x,y) = \frac{1}{N}\sum_{N}^{i=1} (x_i - E(x))(y_i - E(y)) \\ \gamma_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\times\sqrt{D(y)}} \end{cases}, \tag{38}$$

where x and y represent any two pixel values, $E(x)$ denotes the mean of pixel values, $D(x)$ represents the variance, $cov(x,y)$ is the covariance between x and y, and γ_{xy} is the correlation coefficient. As shown in Figure 8 and Table 2,the pixel correlation becomes even after encryption, which means that encryption destroys the original correlation and improves confidentiality performance. This characteristic is crucial for ensuring the security of the encrypted image, as it prevents attackers from inferring information about the original image by analyzing pixel patterns.

4.1.3. Entropy

The disorder of image information can be reflected by the measure of information entropy. The information entropy of an encrypted image is directly proportional to its encryption strength. The formula for calculating information entropy is as follows in Equation (39):

$$H(n) = -\sum_{i=0}^{H\times W-1} P(n_i)\, log_2 P(n_i), \tag{39}$$

where $p(n_i)$ represents the occurrence frequency of the n_i gray level in the image. Comparisons were made with other algorithms using information entropy as shown in Table 3. The results showed that the encrypted images using the present algorithm were closer to the uniform distribution in terms of probability distribution, showing better encryption performance.

4.2. Analysis of the performance results of proposed encryption system

Number of pixel change rate (NPCR) measures the sensitivity of an image encryption algorithm to small variations by calculating the percentage of pixels with different pixel values between two encrypted images. Unified average changing intensity (UACI) measures the average intensity of change between two encrypted images.

The formulae relating to NPCR and UACI are as follows in Equation (40):

$$\begin{cases} NPCR = \frac{1}{H\times W}\times\sum_{i=1}^{H}\sum_{j=1}^{W} D(i,j) \\ UACI = \frac{1}{H\times W}\times\sum_{i=1}^{H}\sum_{j=1}^{W}\frac{|v_1(i,j)-v_2(i,j)|}{255} \end{cases}, \tag{40}$$

Tables 4 and 5 show the values of NPCR and UACI for this algorithm and other algorithms. Experimental results show that the proposed algorithm performed well in terms of NPCR and UACI, demonstrating strong sensitivity to differential changes and preliminarily verifying its effectiveness against differential attacks.

4.3. Analysis of run time

To evaluate the computational efficiency of the proposed scheme, the execution time of each encryption module was measured for color images of sizes $512 \times 512 \times 3$ and $256 \times 256 \times 3$. The results are summarized in Table 6. Table 7 compares the running time of the proposed encryption algorithm with the running time of other encryption algorithms. The table reports the run time of the three major modules fast block permutation, lightweight bitwise diffusion, and convolution-based diffusion along with the total encryption time. From Table 6, it can be observed that the encryption of a $512 \times 512 \times 3$ image required approximately 0.80 seconds in total, whereas a smaller $256 \times 256 \times 3$ image took only 0.51 seconds. This scaling behavior is consistent with the quadratic relationship between image size and the number of pixel-level operations. Among the three modules, convolution-based diffusion was the most time-consuming step (0.506 s for 512×512), since it involves repeated convolutional operations across neighboring pixel blocks. In contrast, the fast block permutation stage required minimal computation (0.058 s for 512×512), owing to the efficient use of chaotic sequences for controlling block shuffling and rotation. The lightweight bitwise diffusion occupied an intermediate cost, reflecting the bit-level XOR operations with chaotic sequences. The experimental results demonstrate that the proposed encryption scheme achieved a favorable balance between security and

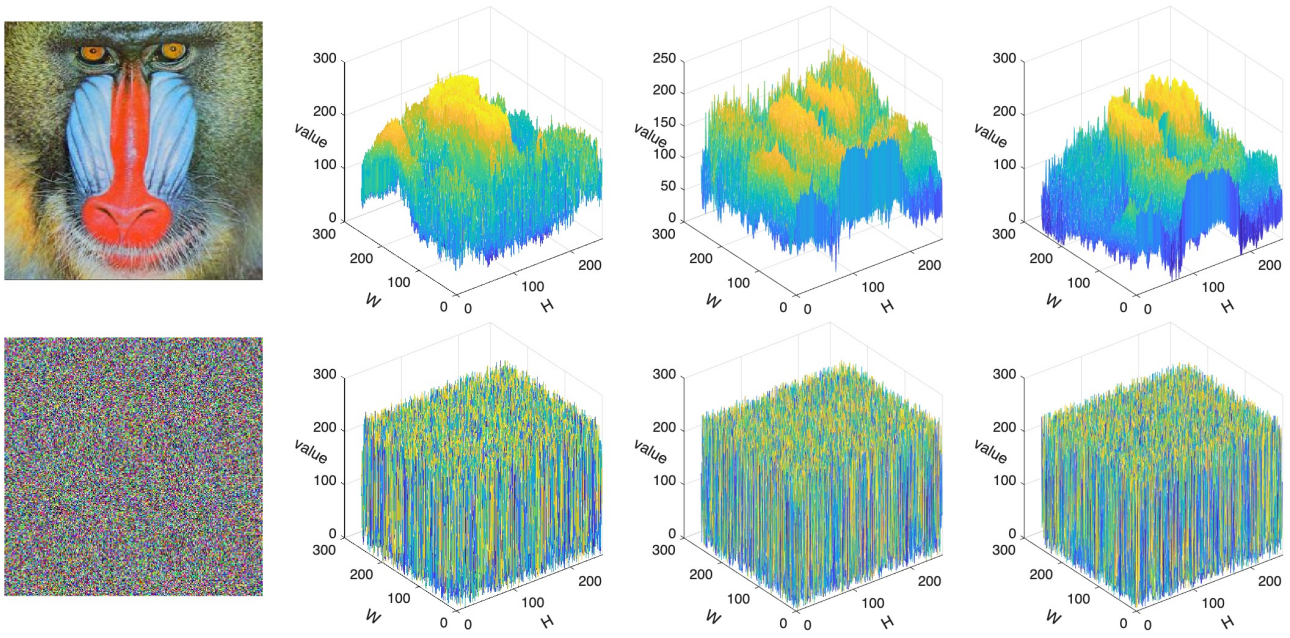
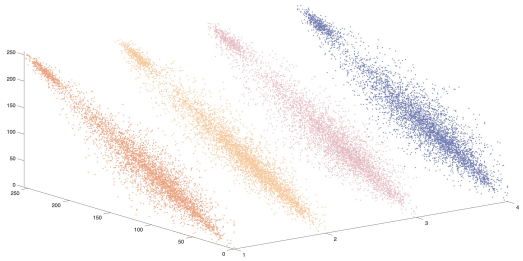
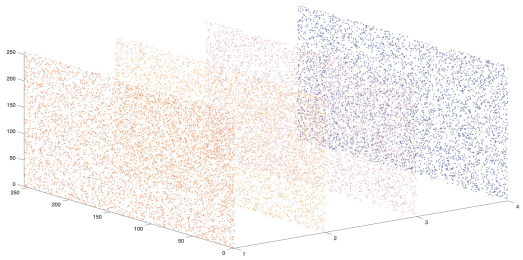


Figure 7. Results of proposed image encryption scheme: Image histograms



(a)



(b)

Figure 8. Results of the proposed image encryption scheme: correlation characteristic: (a) correlation of plain image; (b) correlation of encrypted image

efficiency. The total encryption time remains under 1 s for a standard $512 \times 512 \times 3$ color image, which is suitable for real-time or near real-time applications. Moreover, the modular structure of the encryption scheme allows the permutation and diffusion stages to be parallelized in hardware implementations, further reducing computational overhead in resource-constrained environments.

4.4. Analysis of the sensitivity

4.4.1. Key sensitivity

The high sensitivity of the key ensures robust security against exhaustive attacks. By introducing minute variations to the initial value of the chaotic system and observing whether the resulting sequence differences, the sensitivity of the system to its initial conditions can be evaluated. If the sequences exhibit significant differences, it indicates that the chaotic system is highly sensitive to initial value perturbations, thereby enhancing the security of the encryption algorithm. In the experiment, a perturbation value of $q = 10^{-14}$ was applied to modify the initial value of the system. The resulting sequences, depicted in Figure 9, demonstrate distinct outcomes even under such infinitesimal changes. These results confirm that the algorithm exhibits exceptional key sensitivity, a critical attribute for ensuring cryptographic strength.

Table 2. Results of the proposed image encryption scheme: Comparison of image components in different directions.

Component	Direction	Original image	The Proposed
R channel	Horizontal	0.9640	0.0047
	Vertical	0.9688	-0.0103
	Diagonal	0.9464	0.0216
	Anti-diagonal	0.9589	0.0019
G channel	Horizontal	0.9783	0.0067
	Vertical	0.9809	-0.0127
	Diagonal	0.9650	-0.0106
	Anti-diagonal	0.9682	0.0237
B channel	Horizontal	0.9682	0.0020
	Vertical	0.9708	0.0103
	Diagonal	0.9508	-0.0144
	Anti-diagonal	0.9525	0.0058

Table 3. Comparison of the image information entropy

Images	Original	Proposed
Couple	7.2010	7.9992
Aerial	6.9940	7.9993
Stream and bridge	5.7056	7.9994
Truck	6.0274	7.9992
Airplane	4.0045	7.9994
Tank	5.4957	7.9992
Car and APCs	6.1074	7.9992
Truck and APCs	6.5632	7.9991
Truck and APCs2	6.6953	7.9994
Tank2	5.9916	7.9993
APC	5.0534	7.9994
Average	-	7.9993
Teng et al.[34]	-	7.9980
Zhao et al.[35]	-	7.9993
Gao et al.[36]	-	7.9994

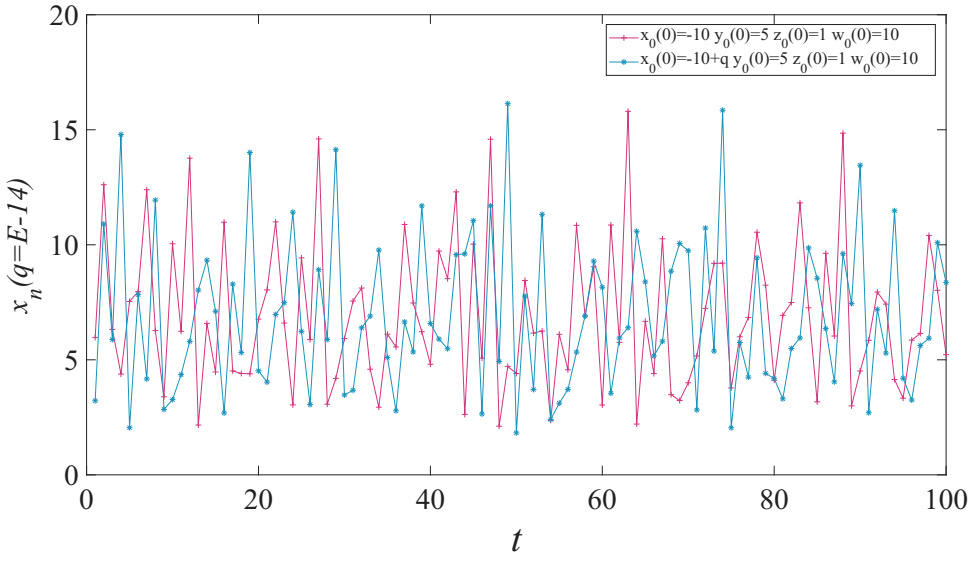


Figure 9. The proposed 4D-HMM demonstrating the effectiveness of chaotic sequences in timing diagrams with different initial values, highlighting the system's sensitivity to initial conditions

Table 4. Comparison of NPCR with different algorithms

Images	Teng et al.[34]	Wang et al. [37]	Li et al. [38]	Proposed
Couple	99.6192	99.7573	99.6151	99.6134
Aerial	99.6135	99.6791	99.6086	99.6152
Stream and bridge	99.6183	99.5894	99.6140	99.6453
Truck	99.6055	99.8033	99.6105	99.6022
Airplane	99.6144	99.7091	99.6166	99.6054
Tank	99.6150	99.5944	99.5934	99.6166
Car and APCs	99.6263	99.6358	99.5975	99.6073
Truck and APCs	99.6145	99.8321	99.6216	99.6099
Truck and APCs2	99.6211	99.7300	99.6067	99.6133
Tank2	99.6108	99.6033	99.6284	99.6154
APC	99.6201	99.7032	99.6292	99.6045
Male	99.6088	99.7182	-	99.6456
Airport	99.6112	99.7433	-	99.6245

Table 5. Comparison of UACI with different algorithms

Images	Teng et al.[34]	Wang et al.[37]	Li et al.[38]	Proposed
Couple	33.4306	33.5390	33.4759	33.4112
Aerial	33.4019	33.3498	33.4310	33.3987
Stream and bridge	33.4124	33.4532	33.5011	33.3955
Truck	33.4217	33.4351	33.5131	33.3876
Airplane	33.4329	33.4981	33.5054	33.3945
Tank	33.4451	33.5329	33.4403	33.4111
Car and APCs	33.4237	33.4977	33.4692	33.4345
Truck and APCs	33.4745	33.4899	33.4690	33.4122
Truck and APCs2	33.4619	33.5039	33.5106	33.3991
Tank2	33.4783	33.3789	33.4588	33.4067
APC	33.4524	33.5511	33.5165	33.3943
Male	33.4585	33.4893	-	33.4322
Airport	33.4605	33.5033	-	33.4195

Table 6. Comparison of time with different algorithms

Image Size	Time(s)			
	Fast block permutation	Lightweight bitwise diffusion	Convolution-based diffusion	All
$512 \times 512 \times 3$	0.058293	0.239761	0.505631	0.803685
$256 \times 256 \times 3$	0.024936	0.150661	0.332242	0.507839

Table 7. Comparison of time with different algorithms

Image Size	Time(s)					
	Zhou et al.[7]	Zhang et al.[39]	Wang et al.[40]	Meng et al.[41]	AES[7]	Proposed
512 × 512 × 3	-	-	0.9447	-	-	0.803685
256 × 256 × 3	1.44177	1.646906	-	1.24	75.0690	0.507839

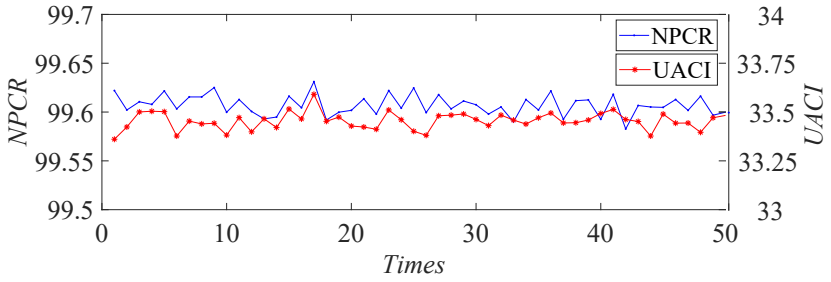


Figure 10. The proposed image encryption scheme. NPCR and UACI of randomly altered plain image pixels

4.4.2. Plain sensitivity

Plain sensitivity means that if there is a small change in the original image, the encrypted image will change accordingly. A pixel point was selected randomly from the original image, and the value was re-encrypted with a change of size 1. Figure 10 shows the NPCR and UACI after 50 separate encryptions. Experimental results indicate that the proposed algorithm exhibited high sensitivity to plain, effectively resisting known-plain attacks.

4.5. Key Space

The security of an image encryption algorithm largely depends on the size of its key space, which determines the resistance against brute-force attacks. In the proposed scheme, the secret key was composed of the perturbed initial conditions of the memristor-based Hénon 4D map, denoted as (x_0', y_0', z_0', w_0'). Each of these parameters was represented by a floating-point number in the interval $(0, 1)$ and was perturbed using the SHA-256 hash of the plaintext image, ensuring that even small variations in the input image led to significantly different key values.

Assuming that the computational precision of each initial value is 10^{-14}, each parameter can take approximately 10^{14} distinct values. Therefore, the total key space of the four-dimensional key is given by Equation (41):

$$K = 10^{14} \times 10^{14} \times 10^{14} \times 10^{14} = 10^{4\times14} = 10^{56}, \quad (41)$$

where K represents the number of possible key combinations. In terms of binary representation, this value corresponds to approximately:

$$10^{56} \approx 2^{186}. \quad (42)$$

A key space of 2^{186} is significantly larger than the minimum recommended value of 2^{100} for resisting exhaustive search attacks. Table 8 compares the key space of the proposed image encryption scheme with the key space of other image encryption schemes. Furthermore, the dynamic perturbation of initial conditions by plaintext-dependent SHA-256 hashing ensures that the key is not only vast in size but also tightly coupled with the input image, effectively preventing key reuse across different plaintexts. The proposed encryption scheme provides an extremely large and secure key space, far beyond the capabilities of brute-force attacks.

4.6. Analysis of the chosen-plaintext attack

The chosen-plaintext attack is a common method and means in cryptanalysis. Chosen-plaintext refers to the situation where attackers select specific plain inputs and observe the corresponding encryption results to infer the internal mechanisms of encryption algorithms, keys, or other sensitive information. In this experiment, encryption of all black and all white images was performed to verify whether the algorithm can withstand such attacks. Figure 12 shows the encrypted results. The algorithm performed well in both visual and statistical analyses, indicating that this type of attack has a limited impact on our algorithm.

5. Conclusion

This paper proposed a secure and efficient image encryption scheme based on the 4D-HMM. By leveraging the enhanced nonlinear dynamics of the 4D-HMM, the scheme generated high-quality pseudo-random sequences for driving multi-stage encryption operations, including block permutation, pixel-level scrambling, and dual-stage diffusion. The plaintext-dependent key perturbation mechanism ensured resistance to chosen-plaintext attacks, while the cascade of lightweight and convolutional diffusion modules provided strong avalanche effects. Experimental evaluations demonstrated that the scheme achieved excellent security performance: ciphertext histograms were uniform, entropy values were close to ideal, and pixel correlations were effectively eliminated. Furthermore, the method exhibited high resistance to statistical, differential, and brute-force attacks, supported by NPCR and UACI results near theoretical expectations. Importantly, the scheme maintained computational efficiency, making it well-suited for real-time applications in cloud computing, smart devices, and multimedia communication. In summary, the proposed 4D-HMM-based encryption framework offers a robust solution to digital image security challenges, balancing efficiency and security. Future work will explore hardware implementations leveraging memristor devices and extend the design to multi-image and video encryption scenarios in distributed environments.

Table 8. Table of key space comparisons.

Proposed	Murillo-Escobar et al.[42]	Liu et al.[43]	Mansouri et al.[44]	Shafique et al.[45]
186	128	166	154	224

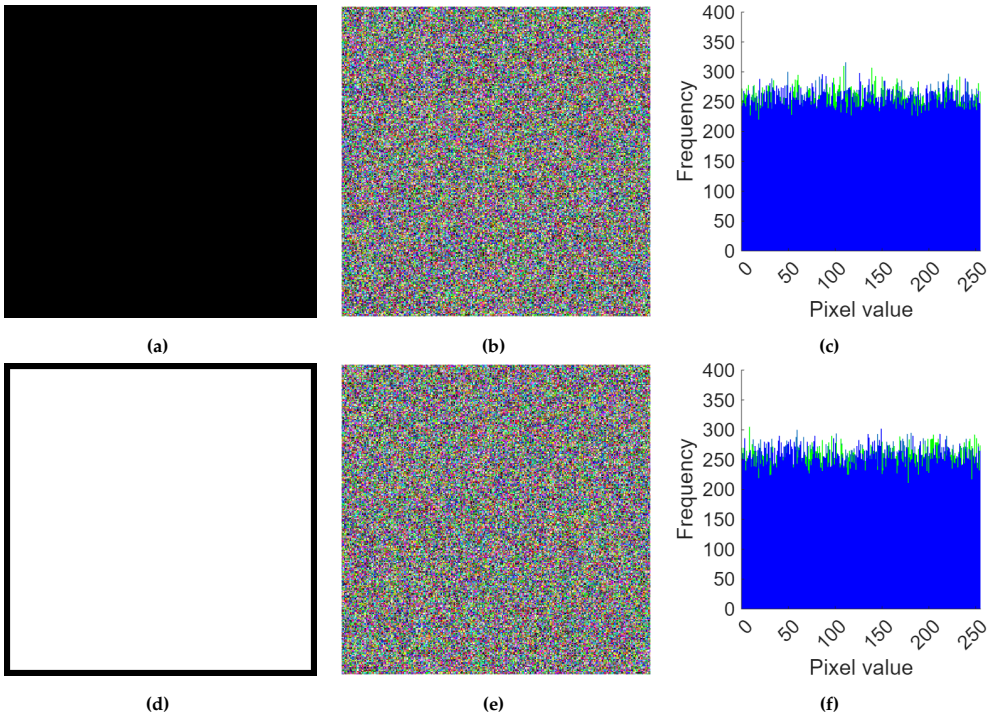


Figure 12. Result of the proposed image encryption scheme. (a)-(c) All black plain image, encrypted image, histogram of (b); (d)-(f) all white plain image, encrypted image, histogram of (e)

Acknowledgments

None.

Funding

None.

Conflict of interest

Abdurrahim Toktas is an Editorial Board Member of this journal, but was not in any way involved in the editorial and peer-review process conducted for this paper, directly or indirectly. Separately, other authors declared that they have no known competing financial interests or personal relationships that could have influenced the work reported in this paper.

Author contributions

Conceptualization: Yiting Lin, Yunlong Liao
Data curation: Yiting Lin, Yunlong Liao
Formal analysis: Yiting Lin, Yunan Wei, Ugur Erkan, Abdurrahim Toktas
Funding acquisition: Donglong Chen
Investigation: Yunan Wei, Wenjun Zeng, Yong Zhang
Methodology: Yiting Lin, Yunlong Liao
Project administration: Donglong Chen
Resources: Donglong Chen
Software: Yiting Lin, Yunlong Liao
Supervision: Donglong Chen
Validation: Yunan Wei, Wenjun Zeng, Ugur Erkan, Abdurrahim Toktas, Yong Zhang
Visualization: Yiting Lin, Wenjun Zeng, Ugur Erkan, Abdurrahim Toktas, Yong Zhang
Writing – original draft: Yiting Lin, Yunlong Liao, Yunan Wei, Ugur Erkan, Abdurrahim Toktas
Writing – review & editing: Yiting Lin, Yunlong Liao, Yunan Wei, Ugur Erkan, Abdurrahim Toktas

Availability of data

Not applicable.

AI Tools Statement

All authors confirm that no AI tools were used in the preparation of this manuscript.

References

1. Yan S, Wu X, & Jiang J. Dynamics analysis and predefined-time sliding mode synchronization of multi-scroll systems based on a single memristor model. *Chaos, Solitons, & Fractals* 2025;196.
2. Gao S, Zhang Z, Li Q, Ding S, Iu HH-C, Cao Y, Xu X, Wang C, & Mou J. Encrypt a story: A video segment encryption method based on the discrete sinusoidal memristive rulkov neuron. *IEEE Trans Dependable Secure Comput.* 2025;1–15.
3. Şimşek C, Erkan U, Toktas A, Lai Q, & Gao S. Hexadecimal permutation and 2d cumulative diffusion image encryption using hyper- chaotic sinusoidal exponential memristive system. *Nonlinear Dyn.* 2025;113(13):17177–17208.
4. Erkan U, Toktas A, Toktas F, Lin Y, & Gao S. Hybridization of benchmark functions for a high-performance 1d chaotic map and image encryption application. *Nonlinear Sci Control Eng.* 2025;0(0):025340010. [Online]. Available: https://accscience.com/journal/NSCE/articles/online first/5711

5. Chai X, Long G, Ma Y, Li C, Gan Z, & Zhang Y. Privacy protection based on hopfield cross neural network in wbans for medical images. *IEEE Trans Multimedia* 2025;1–15.
6. Chen C, Gao B, Yu Y, Zhao S, Yang Y, Chen L, & Bao H. Synchronously adjustable offset boosting and amplitude control in memristive neural network with hardware implementation. *Chaos, Solitons, Fractals* 2025;199.
7. Zhou S, Tao Z, Erkan U, Toktas A, H. H.-Iu C, Zhang Y, & Zhang H. Multidimensional chaotic signals generation using deep learning and its application in image encryption. *Eng Appl Artif Intell.* 2025;156.
8. Wen H, Kang S, Wu Z, Lin Y, & Huang Y. Dynamic rna coding color image cipher based on chain feedback structure. *Mathematics* 2023;11(14).
9. Wen H, Chen Z, Zheng J, Huang Y, Li S, Ma L, Lin Y, Liu Z, Li R, Liu L, Lin W, Yang J, Zhang C, & Yang H. Design and embedded implementation of secure image encryption scheme using dwt and 2d-lasm. *Entropy* 2022;24(10).
10. Lin Y, Xie Z, Chen T, Cheng X, & Wen H. Image privacy protection scheme based on high-quality reconstruction dct compression and nonlinear dynamics. *Expert Syst Appl.* 2024;257.
11. Wen H, Feng Z, Bai C, Lin Y, Zhang X, & Feng W. Frequency-domain image encryption based on iwt and 3d s-box. *Phys Scr.* 2024;99(5).
12. Cheng X, Cheng T, Yang X, Cheng W, & Lin Y. A face image encryption scheme based on nonlinear dynamics and rna cryptography. *Cryptography* 2025;9(3).
13. Liao Y, Lin Y, Li Q, Xing Z, & Yuan X. Lightweight image encryption algorithm using 4d-nds: Compound dynamic diffusion and single-round efficiency. *IEEE Acc.* 2025;13:74652–74662.
14. Xie Z, Xie W, Cheng X, Yuan Z, Cheng W, & Lin Y. Image privacy protection communication scheme by fibonacci interleaved dif- fusion and non-degenerate discrete chaos. *Entropy* 2025;27(8).
15. Gao S, Wu R, Iu HH-C, Erkan U, Cao Y, Li Q, Toktas A, & Mou J. Chaos-based video encryption techniques: A review. *Comput Sci Rev.* 2025;58.
16. Mou J, Tan L, Cao Y, Zhou N, & Zhang Y. Multiface image compression encryption scheme combining extraction with stp-cs for face database. *IEEE Internet Things J.* 2025;12(12):19522–19531.
17. Zhou S, Yin Y, Erkan U, Toktas A, & Zhang Y. Novel hyper-chaotic system: Implementation to audio encryption. *Chaos, Solitons, Fractals* 2025;193.
18. Rao H, Zhao Y, & Lai Q. Predicting chaotic system behavior using machine learning techniques. *ArXiv* 2024;abs/2408.05702.
19. Wan Z, Pu Y-F, & Lai Q. Memristive feedback-controlled chaotic system with diverse dynamics. *Nonlinear Sci Control Eng.* 2025;1(1). [Online]. Available: https://www.accscience.com/journal/NSCE/1/1/10.36922/NSCE025310008
20. Toktas A, Erkan U, Ustun D, & Lai Q. Multiobjective design of 2d hyperchaotic system using leader pareto grey wolf optimizer. *IEEE Trans Syst Man Cybern Syst.* 2024;54(9):5237–5247.
21. Erkan U, Toktas A, Memiş S, Lai Q, & Hu G. An image en- cryption method based on multi-space confusion using hyperchaotic 2d vincent map derived from optimization benchmark function. *Nonlinear Dyn.* 2023;111(21):20377–20405.
22. Lai Q, Zhu C, Zhao X-W, Sun X, & Hua J. A unified framework for generating 4d discrete memristive hyperchaotic maps with complex dynamics and application to encryption. *IEEE Internet Things J.* 2025;1–1.
23. Yunlong L, Yiting L, Zheng X, & Xiaochen Y. Privacy image se- crecy scheme based on chaos-driven fractal sorting matrix and fibonacci q-matrix. *Vis Comput.* 2025;41(9):6931–6941.
24. Zeng W, Zhang C, Liang X, Xia J, Lin Y, & Lin Y. Intrusion detection-embedded chaotic encryption via hybrid modulation for data center interconnects. *Opt Lett.* 2025;50(13).
25. Alexan W, Hosny K, & Gabr M. A new fast multiple color image encryption algorithm. *Clust Comput.* 2025;28(5).
26. Feng W, Zhang J, Chen Y, Qin Z, Zhang Y, Ahmad M, & Woźniak M. Exploiting robust quadratic polynomial hyperchaotic map and pixel fusion strategy for efficient image encryption. *Expert Syst Appl.* 2024;246.
27. Zhang Y. Image encryption algorithm based on butterfly module and chaos. *Math Comput Simul.* 2025;232:382–407.
28. Wen W, Yuan Z, Qi S, Zhang Y, & Fang Y. Ppm-sem: A privacy-preserving mechanism for sharing electronic patient records and medical images in telemedicine. *IEEE Trans. Multimedia* 2024;26:5795–5806.
29. Obaid MJ, Neamah AA, Shukur AA, Pham V-T, & Grassi G. A reliable color image encryption scheme based on a novel dual-wing hyperchaotic map. *Expert Syst Appl.* 2025;289.
30. jun lu, xue xia, xiaoqiang zhang, ruoyu zhao, & yushu zhang. Multiple-image encryption algorithm based on a new 3d hyperchaotic map and whac-a-mole scrambling model. *Expert Syst Appl.* 2025;290.
31. Liu B, Song W, Zheng M, Fu C, Chen J, & Wang X. Semantically enhanced selective image encryption scheme with parallel computing. *Expert Syst Appl.* 2025;279.
32. Liu X, Mou J, Zhang Y, & Cao Y. A new hyperchaotic map based on discrete memristor and meminductor: Dynamics analysis, encryption application, & dsp implementation. *IEEE Trans Ind Electron.* 2024;71(5):5094–5104.
33. Hua Z and Zhou Y. Image encryption using 2d logistic-adjusted-sine map. *Inf Sci.* 2016;339:237–253.
34. Teng L, Cao P, & Liu Y. Multi-image encryption algorithm based on novel spatiotemporal chaotic system and dynamical chaotic trajectories. *IEEE Trans Circuits Syst Video Technol.* 2025;35(2):1562–1575.
35. Zhao H, Wang S, & Fu Z. A new image encryption algorithm based on cubic fractal matrix and l-lccml system. *Chaos, Solitons, Fractals* 2024;185(8):115076.
36. Gao X, Mou J, Li B, Banerjee S, & Sun B. Multi-image hybrid encryption algorithm based on pixel subtitution and Gene theory. *Fractals* 2023;31(06):2340111.
37. Wang Y, Chen L, Yu K, & Fu T. A secure spatio-temporal chaotic pseudorandom generator for image encryption. *IEEE Trans Circuits Syst Video Technol.* 2024;34(9):8509–8521.
38. Li L. A novel chaotic map application in image encryption algorithm. *Expert Syst Appl.* 2024;252:124316.
39. Zhang X, Wen H, Feng W, Kang S, Xie Z, Zhang X, & Lin Y. Weighted color image encryption algorithm based on rna extended dynamic coding and quantum chaotic system. *Entropy* 2025;27(8).
40. Wang M, Teng L, Zhou W, Yan X, Xia Z, & Zhou S. A new 2D cross hyperchaotic Sine-modulation-Logistic map and its application in bit-level image encryption. *Expert Syst Appl.* 2024;261:125328.
41. Meng F, & Wu G. A color image encryption and decryption scheme based on extended DNA coding and fractional-order 5D hyper-chaotic system. *Expert Syst Appl.* 2024;254:124413.
42. Murillo-Escobar M, Cruz-Hernández C, Abundiz-Pérez F, López-Gutiérrez R, & Acosta Del Campo O. A rgb image encryption algorithm based on total plain image characteristics and chaos. *Signal Process.* 2015;109:119–131.
43. Liu L, Zhang Q, & Wei X. A rgb image encryption algorithm based on dna encoding and chaos map. *Comput Electr Eng.* 2012;38(5):1240–1248, special issue on Recent Advances in Security and Privacy in Distributed Communications and Image processing.
44. Mansouri A, & Wang X. A novel block-based image encryption scheme using a new sine powered chaotic map generator. *Multimed Tools Appl.* 2021;80(14):21955–21978.
45. Shafique A, & Ahmed F. Image encryption using dynamic s-box substitution in the wavelet domain. *Wirel Pers Commun.* 2020;115(3):2243–2268.