

Article

Two-Dimensional Coupling-Enhanced Cubic Hyperchaotic Map with Exponential Parameters: Construction, Analysis, and Application in Hierarchical Significance-Aware Multi-Image Encryption

Wei Feng ¹, Zixian Tang ¹, Xiangyu Zhao ², Zhentao Qin ^{1,*}, Yao Chen ¹, Bo Cai ¹, Zhengguo Zhu ¹, Kun Qian ³ and Heping Wen ^{4,*}

¹ School of Mathematics and Computer Science, Panzhuhua University, Panzhuhua 617000, China; fengwei@pzhuh.edu.cn (W.F.); tangzx2025@126.com (Z.T.); chenyaopzhuh.edu.cn (Y.C.); caibo@pzhuh.edu.cn (B.C.); zhuzhengguo@pzhuh.edu.cn (Z.Z.)

² School of Electrical and Information Engineering, Panzhuhua University, Panzhuhua 617000, China; zhaoxiangyu@pzhuh.edu.cn

³ College of Physics and Electronics, Hunan Institute of Science and Technology, Yueyang 414006, China; tsienkun@hnist.edu.cn

⁴ School of Electronic Information, University of Electronic Science and Technology of China, Zhongshan Institute, Zhongshan 528402, China

* Correspondence: qinzhentao@pzhuh.edu.cn (Z.Q.); wenheping@uestc.edu.cn (H.W.)

Abstract

As digital images proliferate across open networks, securing them against unauthorized access has become imperative. However, many recent image encryption algorithms are limited by weak chaotic dynamics and inadequate cryptographic design. To overcome these, we propose a new 2D coupling-enhanced cubic hyperchaotic map with exponential parameters (2D-CCHM-EP). By incorporating exponential terms and strengthening interdependence among state variables, the 2D-CCHM-EP exhibits strict local expansiveness, effectively suppresses periodic windows, and achieves robust hyperchaotic behavior, validated both theoretically and numerically. It outperforms several recent chaotic maps in key metrics, yielding significantly higher Lyapunov exponents and Kolmogorov–Sinai entropy, and passes all NIST SP 800-22 randomness tests. Leveraging the 2D-CCHM-EP, we further develop a hierarchical significance-aware multi-image encryption algorithm (MIEA-CPHS). The core of MIEA-CPHS is a hierarchical significance-aware encryption strategy that decomposes input images into high-, medium-, and low-significance layers, which undergo three, two, and one round of vector-level adaptive encryption operations. An SHA-384-based hash of the fused data dynamically generates a 48-bit adaptive control parameter, enhancing plaintext sensitivity and enabling integrity verification. Comprehensive security analyses confirm the exceptional performance of MIEA-CPHS: near-zero inter-pixel correlation (<0.0016), near-ideal Shannon entropy (>7.999), and superior plaintext sensitivity (NPCR $\approx 99.61\%$, UACI $\approx 33.46\%$). Remarkably, the hierarchical design and vectorized operations achieve an average encryption throughput of 87.6152 Mbps, striking an outstanding balance between high security and computational efficiency. This makes MIEA-CPHS highly suitable for modern high-throughput applications such as secure cloud storage and real-time media transmission.



Academic Editor: Ruizhi Yang

Received: 30 October 2025

Revised: 28 November 2025

Accepted: 4 December 2025

Published: 6 December 2025

Citation: Feng, W.; Tang, Z.; Zhao, X.; Qin, Z.; Chen, Y.; Cai, B.; Zhu, Z.; Qian, K.; Wen, H. Two-Dimensional Coupling-Enhanced Cubic Hyperchaotic Map with Exponential Parameters: Construction, Analysis, and Application in Hierarchical Significance-Aware Multi-Image Encryption. *Axioms* **2025**, *14*, 901. <https://doi.org/10.3390/axioms14120901>

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Keywords: hyperchaotic map; exponential parameters; dynamical analysis; multi-image encryption; hierarchical significance awareness; security analysis

MSC: 65P20; 94-08; 94A60

1. Introduction

As a primary medium of information exchange in the digital era, digital images play a pivotal role in conveying rich, complex data with visual immediacy and ease of interpretation [1,2]. This distinctive capability has spurred their extensive adoption across critical domains, from clinical diagnostics and corporate communications to military reconnaissance and surveillance [3–5]. However, their widespread use introduces critical vulnerabilities: unauthorized exposure of confidential visual content can trigger serious security incidents. Moreover, standard encryption protocols like AES are ill suited for images due to inherent characteristics, large data volumes, and strong inter-pixel correlations, which undermine both security and efficiency in practical image encryption [6–8].

In response to growing security demands, image encryption schemes rooted in chaotic dynamics have gained significant traction within the field of information security [9–11]. Owing to their distinctive nonlinear traits, particularly high sensitivity to seed values, and intrinsic randomness in long-run evolution, chaotic systems offer an ideal foundation for achieving Shannon’s principles of confusion and diffusion [12–14]. Consequently, a surge of research activity has been devoted in the past few years to developing and optimizing chaos-based methodologies for securing digital images [15–23]. Recent studies have actively explored advanced dynamical properties to enhance cryptographic strength. For instance, Fedoseev et al. [24] utilized adaptive symmetry in discrete maps to expand the key space, while Hosbas et al. [25] leveraged fractional-order dynamics to construct robust true random number generators (TRNGs) verified by rigorous NIST assessments. In the specific domain of medical imaging, Kaya and Aydin introduced a chaos-based scheme for X-ray images using a double Lorenz map, achieving high resistance to differential attacks [26].

Despite the surge in novel encryption proposals, a considerable portion of contemporary algorithms are hindered by fundamental design shortcomings, which adversely affect their security guarantees, deployment feasibility, and runtime efficiency [27–30]. Through systematic cryptanalysis, we have uncovered two recurring weaknesses that persist across recent studies [31,32].

The first critical weakness in many current designs lies in their dependence on cryptographically weak chaotic primitives. Many schemes employ chaotic maps with known vulnerabilities. For instance, some algorithms utilize classic maps or 1D maps, which suffer from narrow chaotic ranges, uneven state distributions, and limited parameter spaces [33,34]. Others adopt hyperchaotic maps whose high complexity incurs substantial computational overhead, severely compromising encryption efficiency [35–37]. Even seemingly robust maps, such as the 2D Cubic map [38] analyzed in Section 2.1, can suffer from structural flaws like state variable independence, leading to dynamical degradation under specific parameters [39,40].

However, the design of robust chaotic maps faces deeper theoretical challenges beyond simple structural complexity. The recent literature has highlighted the critical issue of parameter-driven degradation phenomena, where chaotic systems implemented in finite-precision devices collapse into short-cycle periodic orbits or fixed points under specific parameter settings [41–43]. Furthermore, studies examining the relationship between sampling frequency and chaotic behavior have shown that improper sampling of continuous systems or weak discrete iterations can compromise the statistical independence of the

generated sequences [44,45]. Similar challenges regarding signal integrity and security in non-ideal physical channels have also been addressed in recent chaotic communication systems [46]. These issues directly undermine the long-term unpredictability required for secure encryption. Therefore, constructing a map that maintains rigorous instability and uniform distribution regardless of parameter variations is not merely a performance goal but a fundamental requirement to prevent dynamical degradation.

The second critical weakness lies in flawed cryptographic architectures. Many algorithms fail to establish a strong link between the key and the plaintext, resulting in low sensitivity to plaintext changes and vulnerability to differential attacks [31,47]. Furthermore, many designs introduce key management challenges that violate Kerckhoffs' principle, such as by directly using image hash values to initialize the chaotic system, which complicates decryption and key handling [34,48]. Finally, inefficient structures, such as pixel-by-pixel processing or complex DNA computation [48], create significant computational overhead, rendering them unsuitable for high-throughput applications.

To overcome these dual challenges in both dynamics and cryptographic design, this paper first constructs a new 2D coupling-enhanced cubic hyperchaotic map with exponential parameters (2D-CCHM-EP), and then proposes a novel, high-performance, and secure multi-image encryption framework. The primary contributions are as follows:

- We construct a new hyperchaotic map called 2D-CCHM-EP. By incorporating exponential terms to accelerate trajectory divergence and strengthen state interdependence, the map achieves robust hyperchaotic behavior.
- We rigorously demonstrate that the 2D-CCHM-EP exhibits strict local expansiveness across its entire parameter space, a key theoretical finding that guarantees the effective suppression of periodic windows. Comprehensive dynamical analyses validate its superior chaotic performance and randomness compared with several recent maps.
- We develop a hierarchical significance-aware multi-image encryption algorithm based on the 2D-CCHM-EP (MIEA-CPHS). This algorithm introduces a novel strategy that decomposes images into high-, medium-, and low-significance layers, applying differentiated encryption rounds to optimally balance security and speed.
- The algorithm integrates an SHA-384-based adaptive parameter mechanism with high-performance vector-level operations. This mechanism dynamically generates a 48-bit control parameter from the fused data, ensuring extreme plaintext sensitivity ($\text{NPCR} \approx 99.61\%$, $\text{UACI} \approx 33.46\%$) and enabling data-integrity verification.
- Extensive experiments confirm that the MIEA-CPHS achieves an outstanding balance between high security and efficiency, yielding an average encryption throughput of 87.6152 Mbps, significantly outperforming recent benchmarks and making it highly suitable for modern high-throughput applications.

The remainder of this paper is organized as follows: Section 2 details the construction, theoretical analysis, and numerical validation of the proposed 2D-CCHM-EP. Section 3 presents the complete architecture and operational steps of the MIEA-CPHS encryption algorithm. Section 4 provides a comprehensive evaluation of the algorithm's security performance and computational efficiency. Finally, Section 5 concludes the paper and discusses potential avenues for future research.

2. Construction and Dynamical Analysis of 2D-CCHM-EP

This section primarily presents the construction of the 2D-CCHM-EP, its dynamical analysis, and an evaluation of its suitability for image encryption. We first detail its mathematical formulation, followed by a theoretical investigation of its dynamical properties, including fixed points, stability, and local expansiveness. The theoretical findings are then validated through a series of numerical experiments. Furthermore, the randomness of the

sequences generated by the system is assessed using the NIST Statistical Test Suite, confirming its effectiveness and superiority as a chaotic source for cryptographic applications.

2.1. Construction of 2D-CCHM-EP

In contrast to continuous chaotic systems, discrete chaotic maps exhibit notable superiority in the speed of generating chaotic sequences—a critical advantage for engineering applications such as high-efficiency image encryption. Consequently, the adoption of diverse chaotic maps in cryptographic schemes has been steadily increasing. However, many recently proposed maps still suffer from either insufficient chaotic performance or unnecessarily complex structures.

For instance, Hua et al. proposed the 2D Cubic map in 2021 [38]. As shown in the first row of Table 1, its structure is extremely simple and computationally efficient. However, it exhibits two critical dynamical flaws: (i) the state variable y_t is independent of x_{t-1} , leading to weak interdependence between dimensions; and (ii) for certain parameter values (e.g., $b = 2$ or 10), both y_t and x_t collapse into non-chaotic, periodic, or even fixed-point dynamics.

Table 1. Definitions of our 2D-CCHM-EP and four recent 2D chaotic maps.

Name	Definition	Control Parameters
2D Cubic map [38]	$\begin{cases} x_t = (ax_{t-1} + cy_{t-1}^3) \bmod 1, \\ y_t = by_{t-1} \bmod 1. \end{cases}$	a, b, c
Our 2D-CCHM-EP	$\begin{cases} x_t = (e^\theta x_{t-1} + y_{t-1}^3 / \pi) \bmod 1, \\ y_t = (e^\gamma y_{t-1} + x_{t-1} / \pi) \bmod 1. \end{cases}$	θ, γ
2D-SCMCI [35]	$\begin{cases} x_t = r \sin(\pi((y_{t-1} + h)k \sin(a\pi/x_{t-1}))), \\ y_t = r \sin(\pi((kx_t + h) \sin(a\pi/x_{t-1}))). \end{cases}$	r, h, k, a
2D-LCCCM [36]	$\begin{cases} x_t = \cos(\pi^2(4\mu x_{t-1}(1 - x_{t-1}) + py_{t-1}(1 - y_{t-1}^2)) + \pi/2), \\ y_t = \cos(\pi^2(4\mu y_{t-1}(1 - y_{t-1}) + px_{t-1}(1 - x_{t-1}^2)) + \pi/2). \end{cases}$	p, μ
2D-FOCM [37]	$\begin{cases} x_t = x_{t-1} + \frac{h^v}{\Gamma(1+v)} \cos\left(\frac{2\pi x_{t-1}}{2\mu x_{t-1}^4 - 1} - y_{t-1}\right), \\ y_t = y_{t-1} + \frac{h^v}{\Gamma(1+v)} \cos(\mu\pi x_t + y_{t-1}). \end{cases}$	h, v, μ

To address these intrinsic limitations, we propose a robust hyperchaotic map named 2D-CCHM-EP, defined as

$$\begin{cases} x_t = (e^\theta x_{t-1} + y_{t-1}^3 / \pi) \bmod 1, \\ y_t = (e^\gamma y_{t-1} + x_{t-1} / \pi) \bmod 1, \end{cases} \quad (1)$$

where (x_{t-1}, y_{t-1}) and (x_t, y_t) denote the input and output states at the t -th iteration, respectively, and (θ, γ) are the control parameters. As analytically derived in Section 2.2.2, when $\theta, \gamma \in [1, 13]$, the system exhibits strictly expanding local dynamics (with Jacobian eigenvalues always exceeding 2.167), guaranteeing persistent hyperchaotic behavior across the entire parameter range. This interval is chosen to balance numerical stability (avoiding overflow from excessively large exponentials) and cryptographic applicability.

The design of 2D-CCHM-EP incorporates three mathematically engineered improvements, each addressing a specific dynamical deficiency in the original 2D Cubic map:

- Exponential Repulsion Mechanism:** The linear coefficients in the original map are replaced by exponential modulators e^θ and e^γ . As verified later in Equation (4), these terms ensure that the eigenvalues of the Jacobian at the origin are $\lambda_1 = e^\theta$ and $\lambda_2 = e^\gamma$. For $\theta, \gamma \geq 1$, we have $|\lambda_i| \geq e^1 \approx 2.718 > 1$. This theoretically guarantees that the fixed point acts as a strong unstable repeller regardless of parameter fluctuations, solving the weak divergence issue found in some polynomial-based maps such as the original 2D Cubic map.

2. **Full State Coupling:** A linear coupling term x_{t-1}/π is introduced into the equation for y_t . In the original 2D Cubic map, the decoupling of y_t from x_{t-1} results in a sparse Jacobian matrix, making the system vulnerable to parameter-driven degradation and reducing the statistical independence between dimensions. Our modification ensures a fully dense Jacobian (Equation (3)), enforcing bidirectional state dependence to mitigate these degradation phenomena.
3. **Scaling for Strict Local Expansiveness ($1/\pi$):** The coefficient $1/\pi$ is not an arbitrary choice but a theoretically derived bound. As demonstrated in Section 2.2.2, this specific scaling ensures that even in the worst-case scenario ($\theta = \gamma = 1, y \rightarrow 1$), the smaller eigenvalue remains strictly above unity ($\lambda_{\min} \approx 2.167 > 1$). Without this scaling, the system could violate the strict expansion condition, leading to periodic windows.

With these theoretically grounded enhancements, 2D-CCHM-EP achieves robust, parameter-insensitive hyperchaos. In the following sections, we provide a rigorous dynamical analysis and comprehensive performance evaluation to validate its suitability for secure image encryption.

2.2. Dynamical Analysis

Before presenting numerical validations, we conduct a theoretical analysis of the dynamical properties of 2D-CCHM-EP. This establishes the mathematical foundation for the hyperchaotic behavior observed in subsequent experiments and directly justifies the design choices outlined in Section 2.1.

2.2.1. Fixed Points and Stability Analysis

A fixed point $X^* = (x^*, y^*)$ of a map satisfies $F(X^*) = X^*$. For 2D-CCHM-EP (Equation (1)), the fixed points must satisfy

$$\begin{cases} x^* = (e^\theta x^* + (y^*)^3/\pi) \bmod 1, \\ y^* = (e^\gamma y^* + x^*/\pi) \bmod 1. \end{cases} \quad (2)$$

This implies the existence of integers k_1, k_2 such that

$$\begin{cases} (e^\theta - 1)x^* + (y^*)^3/\pi = k_1, \\ x^*/\pi + (e^\gamma - 1)y^* = k_2. \end{cases}$$

Clearly, $(x^*, y^*) = (0, 0)$ is a fixed point when $k_1 = k_2 = 0$.

For local stability analysis, the mod 1 operation can be omitted, as it only affects global topology, not local linearization. The Jacobian matrix at any point (x, y) is

$$J(x, y) = \begin{pmatrix} e^\theta & 3y^2/\pi \\ 1/\pi & e^\gamma \end{pmatrix}. \quad (3)$$

Evaluated at the origin:

$$J(0, 0) = \begin{pmatrix} e^\theta & 0 \\ 1/\pi & e^\gamma \end{pmatrix}, \quad (4)$$

which is lower triangular. Its eigenvalues are the diagonal entries: $\lambda_1 = e^\theta, \lambda_2 = e^\gamma$.

Given $\theta, \gamma \in [1, 13]$, we have $|\lambda_i| \geq e^1 \approx 2.718 > 1$. Unlike certain polynomial-based maps such as the 2D Cubic map, whose eigenvalues may approach or fall below 1 for certain parameters, the exponential structure here enforces a rapid, guaranteed rate of separation. Thus, the origin is a robust unstable repeller, ensuring that all nearby trajectories diverge exponentially. This result rigorously validates the necessity of the exponential repulsion

mechanism introduced in Section 2.1, as it eliminates the risk of trajectory collapse inherent in maps with weak fixed-point repulsion.

2.2.2. Jacobian Matrix and Local Expansiveness Analysis

A system is hyperchaotic if it possesses at least two positive Lyapunov exponents (LEs) [49]. While LEs are defined as long-term averages along trajectories, a sufficient condition for hyperchaos in smooth or piecewise-smooth systems is the presence of strict local expansiveness: that is, all eigenvalues of the Jacobian matrix $J(x, y)$ satisfy $|\lambda| > 1$ for all (x, y) in the interior of the phase space. This condition ensures that infinitesimal perturbations grow exponentially at every point, precluding the existence of stable periodic orbits.

Although the mod 1 operation renders the map discontinuous at the boundaries of $[0, 1]^2$, the Jacobian matrix remains valid for analyzing local dynamics in the interior $(0, 1)^2$, where almost all trajectories evolve due to the strong repulsion from fixed points (see Section 2.2.1). Moreover, since the map is piecewise smooth and the expansion condition holds strictly throughout the open domain, no attracting periodic orbits can emerge—a fact corroborated by extensive numerical simulations (see Section 2.3).

From Equation (3), the characteristic equation is

$$\lambda^2 - (e^\theta + e^\gamma)\lambda + (e^\theta e^\gamma - 3y^2/\pi^2) = 0.$$

The discriminant is

$$\Delta = (e^\theta - e^\gamma)^2 + \frac{12y^2}{\pi^2} \geq 0,$$

proving that both eigenvalues are real for all (x, y) . They are given by

$$\lambda_{1,2} = \frac{(e^\theta + e^\gamma) \pm \sqrt{(e^\theta - e^\gamma)^2 + 12y^2/\pi^2}}{2}.$$

We now determine the lower bound of the smaller eigenvalue λ_2 . It is minimized when θ and γ are smallest and y is largest. In the worst-case scenario ($\theta = \gamma = 1, y \rightarrow 1$):

$$\lambda_2 = \frac{2e - \sqrt{12/\pi^2}}{2} = e - \frac{\sqrt{3}}{\pi} \approx 2.718 - 0.551 = 2.167 > 1.$$

This result explicitly justifies the choice of the scaling factor $1/\pi$. We can demonstrate its necessity by analyzing the counterfactual scenario where this scaling is removed (i.e., the coefficient is set to 1). In that case, the discriminant term $12y^2/\pi^2$ would increase to $12y^2$. Consequently, in the worst-case limit ($\theta = \gamma = 1, y \rightarrow 1$), the smaller eigenvalue would drop to $\lambda_2 = e - \sqrt{3} \approx 2.718 - 1.732 = 0.986 < 1$. This violates the strict expansion condition, thereby removing the theoretical guarantee against periodic windows and permitting the emergence of stable orbits. Hence, the factor $1/\pi$ is a mathematically derived stability bound required to ensure $\lambda_{\min} > 1$ globally.

Since $\lambda_1 \geq \lambda_2 > 2.167 > 1$ everywhere in the interior of the phase space, the system exhibits strictly expanding local dynamics throughout its domain. Consequently, the time-averaged logarithmic growth rates (LEs) satisfy $LE_1 > 0$ and $LE_2 > 0$. This establishes that 2D-CCHM-EP exhibits robust hyperchaos across its entire parameter range and is free from periodic windows, a significant improvement over certain existing maps such as the 2D Cubic map.

Thus, the structure of 2D-CCHM-EP is not an ad hoc combination of existing components, but a theoretically constrained design that enforces global hyperchaoticity through analytically derived parameter bounds.

2.3. Numerical Verification of Dynamical Behaviors

To complement the theoretical findings in Section 2.2, this subsection presents a series of numerical experiments designed to validate the dynamical properties of the 2D-CCHM-EP.

2.3.1. Trajectory Analysis

To visually verify our theoretical analysis, we present a comprehensive set of trajectory plots in Figure 1. The first plot (left) displays the 2D phase portrait of the system with fixed parameters ($\theta = 6, \gamma = 6$). As predicted by the analysis of the unstable repeller in Section 2.2.1, the trajectory rapidly diverges from the origin and exhibits a dense, space-filling behavior that uniformly covers the entire $[0, 1)^2$ phase space. This visual evidence confirms the system's strong ergodicity.

Furthermore, the second and third plots illustrate the 3D trajectory evolutions as the control parameters γ and θ vary, respectively, across their entire defined range of $[1, 13]$. In both 3D plots, the states (x_t, y_t) remain uniformly distributed across the phase space regardless of the parameter values. The complete absence of any gaps, “periodic windows,” or collapsed structures in these plots provides powerful numerical corroboration for the theoretical proof in Section 2.2.2, which concluded that the 2D-CCHM-EP exhibits strictly expanding local dynamics and is persistently hyperchaotic throughout its entire parameter domain.

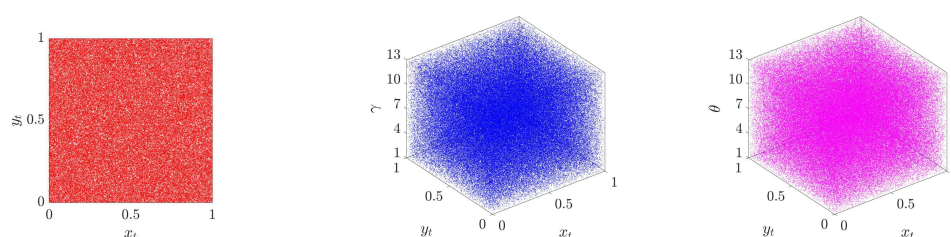


Figure 1. Trajectory analysis of 2D-CCHM-EP: The first plot (left) displays the phase portrait (y_t vs. x_t) with fixed parameters ($\theta = 6, \gamma = 6$). The second plot (middle) shows the 3D trajectory evolution as γ varies over $[1, 13]$ (with $\theta = 6$). The third plot (right) shows the corresponding evolution as θ varies over $[1, 13]$ (with $\gamma = 6$).

2.3.2. Bifurcation Diagram

Bifurcation diagrams offer an intuitive and effective means to verify the chaotic behavior of chaotic maps by exhibiting the distribution characteristics of state values as the control parameters vary [1]. For encryption applications, it is desirable that ciphertext pixels are uniformly distributed. Correspondingly, in the bifurcation diagram of the employed chaotic map, state values should also be uniformly distributed within the entire value domain, without the occurrence of blank areas or clustering of state values, often referred to as “periodic windows”.

Figure 2 showcases six bifurcation diagrams we plotted to visually assess the dynamical behavior of 2D-CCHM-EP across its full parameter range $(\theta, \gamma) \in [1, 13]$. Specifically, the first row presents bifurcation diagrams concerning the state value x_t . The first two plots are 2D diagrams showing x_t vs. θ (with $\gamma = 6$ fixed) and x_t vs. γ (with $\theta = 6$ fixed), respectively. The third plot is a 3D diagram illustrating the distribution of x_t over the entire (θ, γ) plane. The second row mirrors this structure for the state value y_t , displaying two 2D bifurcation diagrams (y_t vs. θ and y_t vs. γ) and one 3D diagram (y_t vs. (θ, γ)). It is evident from all six diagrams that both state values, x_t and y_t , exhibit extremely uniform distributions across the entire state space $[0, 1)$ for all tested parameter values within the defined range $[1, 13]$. Crucially, there is a complete absence of any periodic windows or degenerate behaviors in these diagrams. This provides strong numerical evidence corroborating

our theoretical conclusion in Section 2.2.2 that the 2D-CCHM-EP system exhibits strictly expanding local dynamics and is persistently hyperchaotic throughout its parameter space.

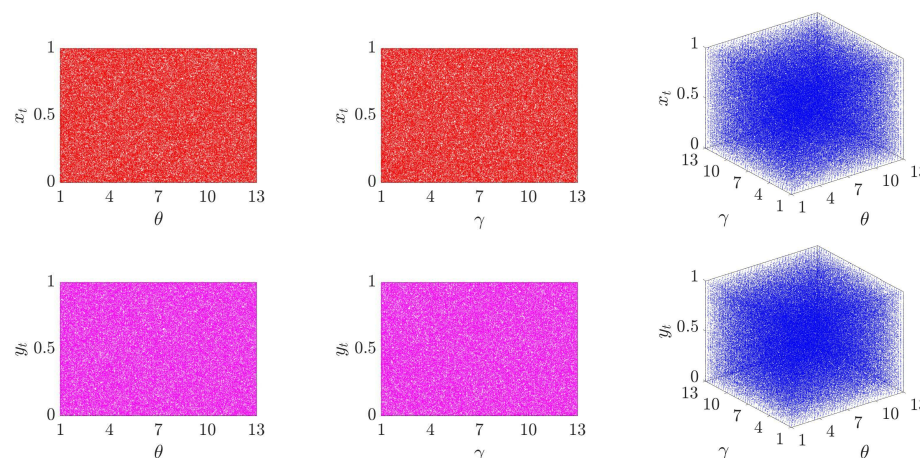


Figure 2. Six bifurcation diagrams of 2D-CCHM-EP: The first row presents two 2D diagrams and one 3D diagram of 2D-CCHM-EP for the state value x_t , and the subsequent row displays three diagrams concerning the state value y_t .

2.3.3. Lyapunov Exponents

The Lyapunov exponent (LE) serves as a pivotal metric for evaluating chaotic performance. A system is considered chaotic if it possesses at least one positive LE, and hyperchaotic if two or more LEs are positive [9]. For a 2D discrete map $\psi(x, y)$ such as 2D-CCHM-EP, the two LEs are defined as

$$LE_v = \lim_{s \rightarrow \infty} \frac{1}{s} \sum_{k=1}^s \ln |\lambda_v(J(x_k, y_k))|, \quad (5)$$

where LE_v denotes either LE_1 or LE_2 , and $\lambda_v(J(x_k, y_k))$ is the v -th eigenvalue of the Jacobian matrix evaluated at the trajectory point (x_k, y_k) .

To ensure the statistical reliability and robustness of the LE estimates, all numerical experiments were conducted using double-precision floating-point arithmetic (IEEE 754 standard). For each parameter configuration, the system was iterated for $N = 10000$ steps, with the first $N_{\text{trans}} = 2000$ iterations discarded as transients to eliminate dependence on initial conditions. The LEs were then computed from the remaining 8000 points.

As illustrated in Figure 3, both LEs of 2D-CCHM-EP remain strictly positive across the entire parameter range $(\theta, \gamma) \in [1, 13]$. While persistent hyperchaos over such a wide interval is uncommon for mod 1 maps—which are typically plagued by periodic windows—this behavior is theoretically guaranteed for 2D-CCHM-EP. As rigorously derived in Section 2.2.2, the map’s design (notably the $1/\pi$ scaling) ensures that all local Jacobian eigenvalues satisfy $|\lambda| > 2.167$ throughout the phase space. Consequently, the LEs are bounded below by $\ln(2.167) \approx 0.773 > 0$, which explains the complete absence of non-chaotic regions. Moreover, as θ and γ increase, both LEs grow rapidly, endowing the system with tunable divergence rates. These properties—broad hyperchaoticity, parameter insensitivity, and strong local expansiveness—make 2D-CCHM-EP an ideal candidate for high-security image encryption.

To highlight the chaotic performance improvement achieved through our enhancement designs, we compared the LEs of 2D-CCHM-EP with those of four recent chaotic maps, including the 2D Cubic map [35–38]. Table 2 and Figure 4 present our experimental setup and findings. Clearly, the LE_1 values of our 2D-CCHM-EP are significantly higher than those of the other four maps. Furthermore, the LE_2 values rapidly increase when the control

parameter exceeds 3, with its average value also being significantly higher. Consequently, it can be concluded that our enhancement designs are effective.

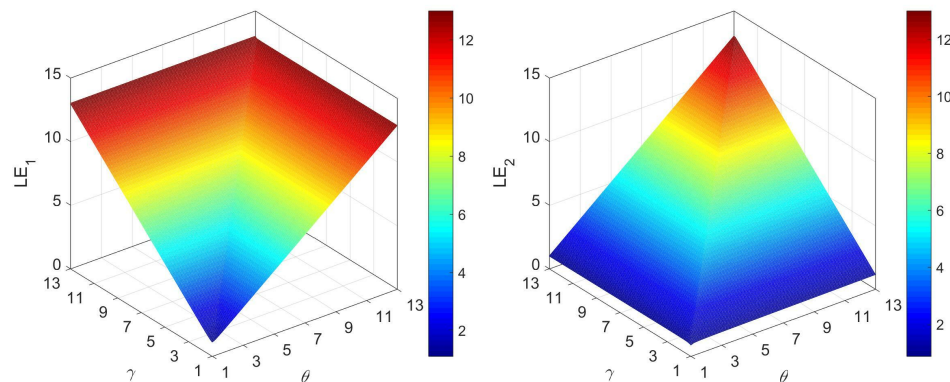


Figure 3. Two LEs of 2D-CCHM-EP: The left subplot corresponds to LE_1 , while the right subplot corresponds to LE_2 .

Table 2. Setup and findings of our LE comparative experiments.

Name	Invariable	Variable	LE_1	LE_2
2D-CCHM-EP	$\gamma = 13$	θ	12.9726	7.0274
2D Cubic map [38]	$b = 13, c = 1$	a	1.7660	2.5649
2D-SCMCI [35]	$k = 1, h = 2, r = 1$	a	4.9351	−0.2636
2D-LCCCM [36]	$p = 8.78$	μ	6.7709	2.7685
2D-FOCM [37]	$h = 0.5, v = 0.789$	μ	1.6439	0.0458

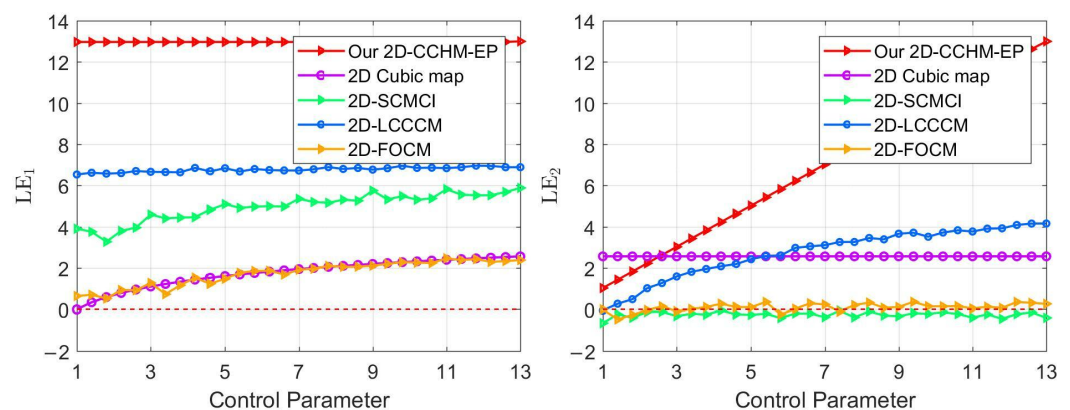


Figure 4. LE values of 2D-CCHM-EP and other four maps: The left subfigure corresponds to LE_1 , while the right subfigure corresponds to LE_2 .

2.3.4. Kolmogorov–Sinai Entropy

Kolmogorov–Sinai entropy quantifies the rate at which a dynamical system generates information, reflecting the degree of unpredictability in its evolution. It measures the average amount of new information produced per unit time as trajectories diverge, not the information needed for prediction [50]. A higher KSE indicates faster loss of predictability, signifying stronger chaos or more complex dynamics.

For measure-preserving chaotic systems, Pesin’s Identity establishes a fundamental relationship between KSE (h_{KS}) and the positive LEs: $h_{KS} = \sum_{LE_i > 0} LE_i$. This identity provides a valuable means to cross-validate numerical estimations of both quantities. The theoretical definition of KSE (or more precisely, the metric entropy K_1 , which equals h_{KS} under certain conditions) is based on the Shannon entropy rate of trajectory sequences

over a phase space partition. It involves partitioning the space into boxes of size ϵ and considering sequences of length d with delay τ :

$$K_1 = - \lim_{\tau \rightarrow 0} \lim_{\epsilon \rightarrow 0} \lim_{d \rightarrow \infty} \frac{1}{d\tau} \sum_{i_0, \dots, i_{d-1}} P(i_0, \dots, i_{d-1}) \ln P(i_0, \dots, i_{d-1}), \quad (6)$$

where $P(i_0, \dots, i_{d-1})$ is the joint probability for a trajectory sequence visiting boxes $i_0, \dots, i_{d-1}$. Directly computing K_1 from Equation (6) is numerically challenging. Therefore, we employed the widely used Grassberger–Procaccia algorithm to estimate the correlation entropy K_2 (denoted KE in our results, see Table 3 and Figure 5) [50]. This method analyzes the scaling of the correlation sum $C(\epsilon, d)$ with ϵ and d . It is well established that K_2 provides a rigorous lower bound for K_1 ($K_2 \leq K_1 \approx h_{KS}$). Despite being a lower bound, K_2 is a standard and practical measure for quantifying and comparing the complexity and unpredictability inherent in chaotic systems.

We conducted numerical experiments to evaluate the unpredictability and complexity of 2D-CCHM-EP and four other recent maps (See Table 3 and Figure 5). As revealed, all five maps exhibit positive KE values, confirming they are all in unpredictable, chaotic states. Notably, our 2D-CCHM-EP demonstrates superior performance: its KE_y values surpass all other maps across the entire tested parameter range, while its KE_x values are optimal within the parameter range $\theta \in [3, 10]$. The average KE values for 2D-CCHM-EP are significantly greater than those of the comparison maps. This indicates that 2D-CCHM-EP possesses enhanced unpredictability and complexity.

Table 3. Setup and findings of our KE comparative experiments.

Name	Invariable	Variable	KE_x	KE_y
2D-CCHM-EP	$\gamma = 6$	θ	2.3503	2.4310
2D Cubic map [38]	$b = 6, c = 1$	a	1.9094	1.9557
2D-SCMCI [35]	$k = 1, h = 2, r = 1$	a	2.1325	1.8067
2D-LCCCM [36]	$p = 8.78$	μ	2.1116	2.1129
2D-FOCM [37]	$h = 0.5, v = 0.789$	μ	0.3282	0.3214

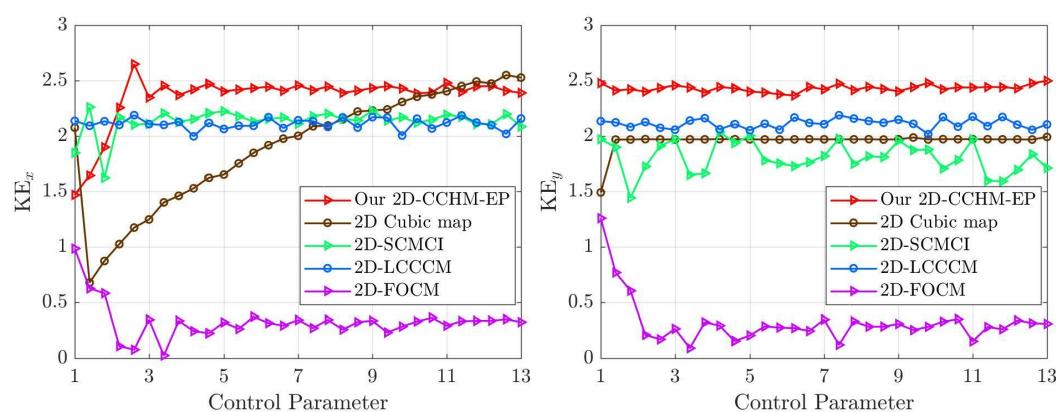


Figure 5. KE values of 2D-CCHM-EP and other four chaotic maps: The left subfigure corresponds to KE_x , while the right subfigure corresponds to KE_y .

Furthermore, comparing these results with the LEs presented earlier (Table 2 in Section 2.3.3), we observe a strong consistency. The sum of the estimated entropy components ($KE_x + KE_y$) from Table 3 closely correlates in trend with the sum of the positive LEs ($LE_1 + LE_2$) from Table 2. This alignment is consistent with Pesin’s Identity and serves as further validation for both our LE calculations and the robust hyperchaotic nature, including the strict local expansiveness established in Section 2.2.2, of the proposed 2D-CCHM-EP.

2.4. Randomness Test

While the preceding analyses have theoretically proven (Section 2.2) and numerically verified (Section 2.3) the robust hyperchaotic nature and complex dynamics of the 2D-CCHM-EP, its suitability for cryptographic applications ultimately hinges on the statistical randomness of the sequences it generates. To rigorously evaluate this aspect, we employed the NIST SP800-22 test suite, a comprehensive battery of statistical tests published by the National Institute of Standards and Technology (NIST) designed to detect non-randomness in binary sequences [51]. According to NIST standards, a binary sequence of sufficient length (e.g., 10^6 bits) is considered to possess acceptable randomness if the p -values obtained from all relevant statistical tests exceed a predefined significance level, typically $\alpha = 0.01$ [51,52].

We conducted a thorough testing procedure involving 20 rounds. In each round, a distinct set of initial values (x_0, y_0) and control parameters (θ, γ) (randomly chosen within their valid ranges) was used to iterate the 2D-CCHM-EP. For each parameter set, the output sequences $\{x_t\}$ and $\{y_t\}$ were transformed into two binary sequences of length 10^6 bits each. This resulted in a total of 40 binary sequences generated under diverse conditions. Subsequently, each sequence was subjected to the full NIST SP800-22 test suite.

The summarized results of these tests are presented in Table 4. As clearly indicated, for all 15 test items, the average p -values for both the x_t -derived and y_t -derived sequences are significantly greater than the threshold of 0.01. Furthermore, the pass ratio for every test across all 20 rounds (40 sequences) was 100%. These results strongly demonstrate that the sequences generated by 2D-CCHM-EP exhibit excellent statistical properties consistent with true randomness.

Table 4. Our random test findings for 2D-CCHM-EP.

Test Item	p -Value		Pass Ratio	Result (R = Random)
	x_t	y_t		
Freq. Bit	0.684742	0.504134	20/20	R
Freq. Block	0.976444	0.186752	20/20	R
Run	0.280215	0.968449	20/20	R
Longest Run	0.273609	0.759439	20/20	R
Bin. Mat. Rank	0.638293	0.822162	20/20	R
DFT	0.699927	0.956091	20/20	R
Non-Overlapping Temp.	0.176719	0.661149	20/20	R
Overlapping Temp.	0.892654	0.574118	20/20	R
Univ. Stat.	0.942278	0.737329	20/20	R
Linear Complexity	0.445562	0.212496	20/20	R
Serial 1	0.729394	0.655986	20/20	R
Serial 2	0.610851	0.622832	20/20	R
Appr. Entropy	0.880750	0.693010	20/20	R
Cumu. Sums Forward	0.728022	0.424428	20/20	R
Cumu. Sums Reverse	0.926945	0.724265	20/20	R
Random Excur. ($x = -1$)	0.830732	0.175877	20/20	R
Random Excur. ($x = +1$)	0.542486	0.542967	20/20	R
Random Excur. Var. ($x = -1$)	0.933815	0.630282	20/20	R
Random Excur. Var. ($x = +1$)	0.454816	0.582257	20/20	R

The comprehensive analyses in this section confirm the desirable properties of the proposed 2D-CCHM-EP. The theoretical analysis (Section 2.2) established its strictly expanding hyperchaotic nature, free from periodic windows. The numerical verifications (Section 2.3) demonstrated its superior LE and KE values compared with existing maps, alongside excellent trajectory and bifurcation characteristics. Finally, the NIST tests (Section 2.4) confirmed the high statistical randomness of its output sequences. Collectively, these findings validate the 2D-CCHM-EP as a robust and high-performance chaotic source, ideally suited for designing the image encryption algorithm proposed in the subsequent section.

3. Proposed MIEA-CPHS

Building upon the robust hyperchaotic properties of the 2D-CCHM-EP established in Section 2, we now introduce a novel multi-image encryption algorithm, termed MIEA-CPHS. The architecture of MIEA-CPHS is specifically designed to resolve the fundamental trade-off between security and efficiency in high-throughput applications. Unlike uniform encryption schemes that treat all data equally, MIEA-CPHS adopts a hierarchical significance-aware strategy grounded in the nonuniform distribution of visual information in digital images.

As illustrated in Figure 6, MIEA-CPHS integrates six stages: *Generation of Hyperchaotic Sequence*, *Hierarchical Significance-Aware Bit-Plane Fusion*, *Generation of Adaptive Control Parameter*, *Generation of Keystreams*, *Adaptive Dual-Mode Vector-Level Hybrid Diffusion*, and *2D Permutation with Adaptive Hybrid Substitution*.

Crucially, the encryption process is hierarchical significance-aware: high-significance components undergo three rounds of diffusion–substitution, medium-significance components two rounds, and low-significance components one round—ensuring enhanced security for perceptually critical information while maintaining computational efficiency.

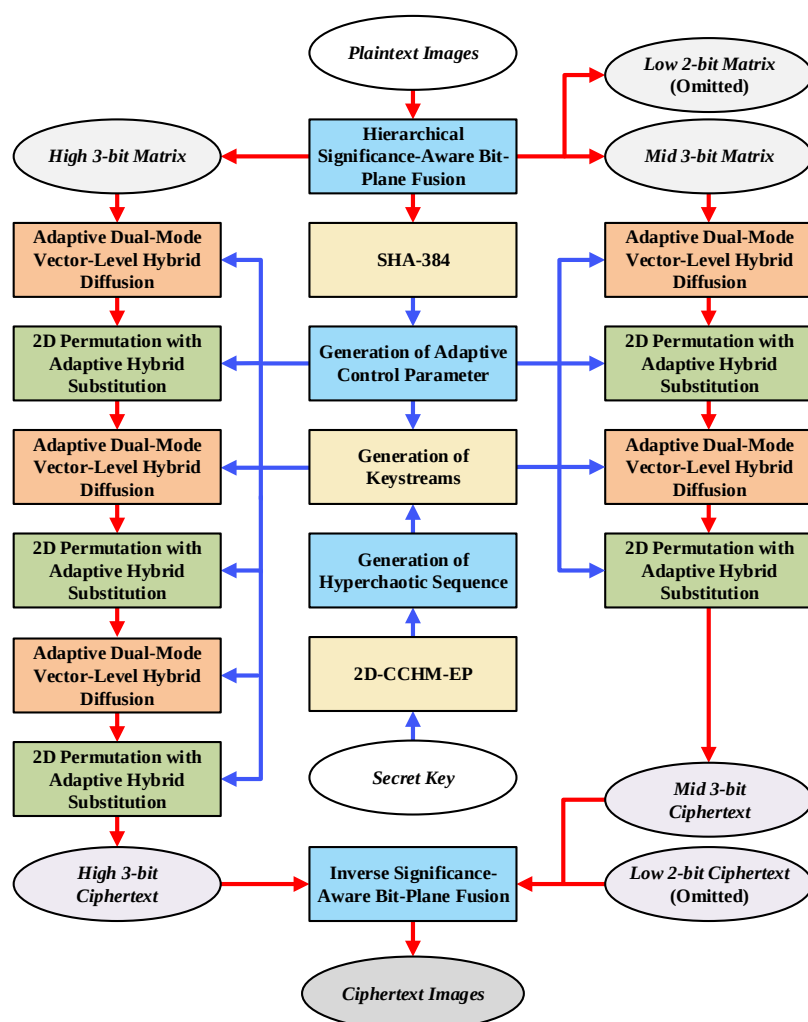


Figure 6. Encryption process of MIEA-CPHS.

3.1. Generation of Hyperchaotic Sequence

Given n input images $\{I^{(i)}\}_{i=1}^n$ with a common spatial resolution $M \times N$ and channel counts c_i ($c_i = 1$ for grayscale images and $c_i = 3$ for color images), we construct a 3D image tensor

$$\mathbf{X} \in \mathbb{Z}^{M \times N \times D}, \quad D = \sum_{i=1}^n c_i, \quad (7)$$

by sequentially stacking all image channels along the third dimension. The structural metadata is encoded as

$$\mathcal{M} = (M, N, \mathbf{c}), \quad \mathbf{c} = [c_1, c_2, \dots, c_n]^\top, \quad (8)$$

which enables exact, lossless reconstruction of the original image set from $\mathbf{X}$. The mapping $\{I^{(i)}\} \mapsto (\mathbf{X}, \mathcal{M})$ is bijective.

The secret key of MIEA-CPHS is defined as

$$\mathcal{K} = [\theta^{(1)}, \gamma^{(1)}, x_0^{(1)}, y_0^{(1)}, \theta^{(2)}, \gamma^{(2)}, x_0^{(2)}, y_0^{(2)}, \alpha], \quad (9)$$

where the first four and the next four components serve as the initial parameters for two independent instances of the 2D-CCHM-EP, respectively, and $\alpha \in \mathbb{N}$ is a transient length used to discard initial samples for enhanced security.

From $\mathcal{K}$, the proposed MIEA-CPHS generates a hyperchaotic sequence $\mathbf{S}_{\text{cut}}$ for subsequent encryption stages as follows:

- **Step 1 (Length Determination):** For the 3D image tensor $\mathbf{X}$ of size $M \times N \times D$, we compute the effective fused dimensions as $F_M = M/4$ and $F_N = ND/4$. The total number of required hyperchaotic samples is

$$L = 3F_M F_N + \alpha + 1024, \quad (10)$$

where the additional 1024 samples are reserved to enhance plaintext sensitivity in later encryption stages.

- **Step 2 (Raw Sequence Generation):** Using the first eight components of $\mathcal{K}$ as initial parameters, we alternately iterate the two instances of the 2D-CCHM-EP and concatenate their state outputs in the order $[x^{(1)}, y^{(1)}, x^{(2)}, y^{(2)}]$ at each iteration. This yields a raw hyperchaotic sequence $\mathbf{S}_{\text{org}} \in [0, 1)^L$.
- **Step 3 (Key-Controlled Transient Removal):** The first α samples of $\mathbf{S}_{\text{org}}$ are discarded, where α is the last component of $\mathcal{K}$, yielding the truncated sequence

$$\mathbf{S}_{\text{cut}} = \{s_t\}_{t=\alpha+1}^L. \quad (11)$$

- **Step 4 (Sequence Extraction):** From $\mathbf{S}_{\text{cut}}$, the first $M + N + D$ samples are extracted to form the hyperchaotic sequence

$$\mathbf{S}^{(1)} = \{s_t\}_{t=\alpha+1}^{\alpha+M+N+D}, \quad (12)$$

which is used in the subsequent hierarchical significance-aware bit-plane fusion stage. The full sequence $\mathbf{S}_{\text{cut}}$ is reserved for the keystream generation in Section 3.4.

3.2. Hierarchical Significance-Aware Bit-Plane Fusion

Building upon the hyperchaotic sequence $\mathbf{S}^{(1)}$ generated in Section 3.1, MIEA-CPHS performs a two-stage preprocessing step that jointly achieves 3D spatial confusion and

hierarchical bit-plane fusion. This stage prepares the data for subsequent encryption operations by aligning the representation with perceptual significance.

First, a key-controlled 3D permutation is applied to the input tensor $\mathbf{X} \in \mathbb{Z}^{M \times N \times D}$ using the first $M + N + D$ samples of $\mathbf{S}^{(1)}$, yielding a scrambled tensor $\mathbf{X}_{\text{sc}}$. The tensor is then reshaped and decomposed into three bit-plane groups according to visual importance: high-significance (bits 8–6), mid-significance (bits 5–3), and low-significance (bits 2–1). Each group is fused across 16 depth slices into a compact matrix through base-weighted accumulation, resulting in three matrices $\mathbf{F}_{\text{H3M}}$, $\mathbf{F}_{\text{M3M}}$, and $\mathbf{F}_{\text{L2M}}$ of size $F_M \times F_N$.

This hierarchical fusion preserves lossless reconstructability while enabling differentiated cryptographic protection according to perceptual significance. As illustrated in Figure 6, the high-significance component $\mathbf{F}_{\text{H3M}}$ undergoes three rounds of encryption, the mid-significance component $\mathbf{F}_{\text{M3M}}$ receives two rounds, and the low-significance component $\mathbf{F}_{\text{L2M}}$ is encrypted only once.

This distinct round allocation is not arbitrary but is dictated by the information entropy and spatial correlation inherent to each layer:

- **High-Significance Layer (Three Rounds):** This layer (bits 8–6) encapsulates over 94% of the total visual energy and possesses extremely strong spatial correlations. A single encryption round is mathematically insufficient to thoroughly disrupt these patterns. Therefore, three rounds are strictly necessary to guarantee the security of the most critical visual data against statistical attacks.
- **Mid-Significance Layer (Two Rounds):** Containing intermediate textural details, this layer represents a transition zone. Two rounds serve as an optimal equilibrium point, providing a safety margin superior to a single round without the computational cost of the full three-round process.
- **Low-Significance Layer (One Round):** These bits (2–1) statistically resemble random noise with negligible correlation. Applying multiple rounds here yields diminishing returns in security while tripling the computational overhead. Thus, a single round is sufficient to maximize throughput without compromising overall visual security.

This tiered strategy optimizes the balance between security and efficiency. The entire process is deterministic, invertible, and fully key-dependent, thereby satisfying Shannon's principle of confusion. The complete procedure is summarized in Algorithm 1.

Algorithm 1 Hierarchical Significance-Aware Bit-Plane Fusion in MIEA-CPHS.

Input: The 3D image tensor $\mathbf{X}$ of size $M \times N \times D$ and the hyperchaotic sequence $\mathbf{S}^{(1)}$ of length $M + N + D$.

- 1: Compute permutation indices π_1, π_2, π_3 via sorting: $\pi_1 \leftarrow \text{sort}(\mathbf{S}_{1:M}^{(1)})$, $\pi_2 \leftarrow \text{sort}(\mathbf{S}_{M+1:M+N}^{(1)})$, $\pi_3 \leftarrow \text{sort}(\mathbf{S}_{M+N+1:M+N+D}^{(1)})$.
- 2: Perform 3D spatial scrambling: $\mathbf{X}_{\text{sc}} \leftarrow \mathbf{X}(\pi_1, \pi_2, \pi_3)$.
- 3: Reshape $\mathbf{X}_{\text{sc}}$ into a 3D block array: $\mathbf{X}_{\text{blk}} \leftarrow \text{reshape}(\mathbf{X}_{\text{sc}}, F_M, F_N, 16)$.
- 4: Extract high-significance layer (bits 8–6): $\mathbf{H} \leftarrow \lfloor \mathbf{X}_{\text{blk}} / 32 \rfloor$.
- 5: Extract mid-significance layer (bits 5–3): $\mathbf{M} \leftarrow \lfloor \text{mod}(\mathbf{X}_{\text{blk}}, 32) / 4 \rfloor$.
- 6: Extract low-significance layer (bits 2–1): $\mathbf{L} \leftarrow \text{mod}(\mathbf{X}_{\text{blk}}, 4)$.
- 7: Initialize fused matrices: $\mathbf{F}_{\text{H3M}} \leftarrow \mathbf{0}$, $\mathbf{F}_{\text{M3M}} \leftarrow \mathbf{0}$, $\mathbf{F}_{\text{L2M}} \leftarrow \mathbf{0}$.
- 8: **for** $i = 1$ to 16 **do**
- 9: $\mathbf{F}_{\text{H3M}} \leftarrow \mathbf{F}_{\text{H3M}} \times 8 + \mathbf{H}(:, :, i)$;
- 10: $\mathbf{F}_{\text{M3M}} \leftarrow \mathbf{F}_{\text{M3M}} \times 8 + \mathbf{M}(:, :, i)$;
- 11: $\mathbf{F}_{\text{L2M}} \leftarrow \mathbf{F}_{\text{L2M}} \times 4 + \mathbf{L}(:, :, i)$;
- 12: **end for**

Output: Three fused matrices $\mathbf{F}_{\text{H3M}}$, $\mathbf{F}_{\text{M3M}}$, and $\mathbf{F}_{\text{L2M}}$ of size $F_M \times F_N$.

3.3. Generation of Adaptive Control Parameter

To enhance plaintext sensitivity and support secure decryption with integrity verification, MIEA-CPHS derives a 48-bit adaptive control parameter κ from the three fused matrices $\mathbf{F}_{H3M}$, $\mathbf{F}_{M3M}$, and $\mathbf{F}_{L2M}$. Critically, the SHA-384 hash digest $\mathbf{h}$ used to compute κ is transmitted alongside the ciphertext, enabling the receiver to reconstruct κ before decryption and later verify the correctness of the recovered data. The generation proceeds as follows:

- **Step 1 (Multi-Tier XOR Fusion):** Perform element-wise XOR across the three significance-aware matrices:

$$\mathbf{X}_{\oplus} = \mathbf{F}_{H3M} \oplus \mathbf{F}_{M3M} \oplus \mathbf{F}_{L2M}. \quad (13)$$

- **Step 2 (Cryptographic Hashing):** Compute the SHA-384 hash digest of $\mathbf{X}_{\oplus}$, resulting in a 48-byte vector:

$$\mathbf{h} = (h_1, h_2, \dots, h_{48}), \quad h_i \in \{0, 1, \dots, 255\}. \quad (14)$$

This digest $\mathbf{h}$ is transmitted to the receiver for parameter reconstruction and integrity checking.

- **Step 3 (Block-Wise Product Computation):** Partition $\mathbf{h}$ into eight consecutive 6-byte blocks. For the i -th block ($i = 1, \dots, 8$), compute the product of its bytes:

$$p_i = \prod_{j=1}^6 h_{6(i-1)+j}. \quad (15)$$

- **Step 4 (Modular Accumulation):** Accumulate all block products modulo 2^{48} to obtain the final 48-bit adaptive control parameter:

$$\kappa = \left(\sum_{i=1}^8 p_i \right) \bmod 2^{48}. \quad (16)$$

The parameter κ governs multiple stages of the subsequent encryption process, including keystream generation, adaptive dual-mode vector-level hybrid diffusion, and 2D permutation with adaptive hybrid substitution. At the receiver side, κ is reconstructed from the received hash digest $\mathbf{h}$ prior to decryption. After decryption, the receiver recomputes the hash from the recovered fused matrices and compares it with $\mathbf{h}$ to verify both data integrity and decryption correctness.

3.4. Generation of Keystreams

To enable significance-aware encryption, MIEA-CPHS generates six distinct keystreams tailored to the high-, medium-, and low-significance layers. These keystreams drive the encryption operations in subsequent stages and are dynamically controlled by the adaptive parameter κ . The generation proceeds as follows:

- **Step 1 (Hash-Controlled Sequence Trimming):** Let $\kappa \in [0, 2^{48} - 1]$ be the adaptive control parameter from Section 3.3. Compute a hash-derived discard offset:

$$h_{\text{dis}} = (\kappa \bmod 1024) + 1. \quad (17)$$

The pre-generated hyperchaotic sequence $\mathbf{S}_{\text{cut}}$ (from Section 3.1) is then trimmed to retain the segment

$$\mathbf{S}_{\text{trim}} = \mathbf{S}_{\text{cut}}(h_{\text{dis}} + 1 : h_{\text{dis}} + 3F_M F_N), \quad (18)$$

where $F_M = M/4$ and $F_N = ND/4$ are the fused dimensions defined in Section 3.2.

- **Step 2 (Permutation Keystreams for High-Significance Layer):** Denote $L_{\text{perm}} = F_M + F_N$ and $L_{\text{aux}} = M + N + D$. The first permutation keystream for the high-significance layer is extracted as

$$\pi_{H3}^{(1)} = \mathbf{S}_{\text{trim}}(L_{\text{aux}} + 1 : L_{\text{aux}} + L_{\text{perm}}). \quad (19)$$

The second and third permutation keystreams are derived via modular multiplication:

$$\pi_{H3}^{(2)} = \{3s \bmod 1 \mid s \in \pi_{H3}^{(1)}\}, \quad \pi_{H3}^{(3)} = \{5s \bmod 1 \mid s \in \pi_{H3}^{(1)}\}. \quad (20)$$

These three keystreams control the three rounds of 2D permutation within the “2D Permutation with Adaptive Hybrid Substitution” stage: $\pi_{H3}^{(1)}$ drives the first round, $\pi_{H3}^{(2)}$ the second, and $\pi_{H3}^{(3)}$ the third, ensuring dynamic and non-repeating spatial shuffling.

- **Step 3 (Permutation Keystreams for Medium-Significance Layer):** The medium-significance layer employs two permutation keystreams:

$$\pi_{M3}^{(1)} = \mathbf{S}_{\text{trim}}(L_{\text{aux}} + L_{\text{perm}} + 1 : L_{\text{aux}} + 2L_{\text{perm}}), \quad (21)$$

$$\pi_{M3}^{(2)} = \{3s \bmod 1 \mid s \in \pi_{M3}^{(1)}\}. \quad (22)$$

These control the first and second rounds of 2D permutation for the medium-significance fused matrix, respectively.

- **Step 4 (Permutation Keystream for Low-Significance Layer):** The low-significance layer uses a single permutation keystream:

$$\pi_{L2} = \mathbf{S}_{\text{trim}}(L_{\text{aux}} + 2L_{\text{perm}} + 1 : L_{\text{aux}} + 3L_{\text{perm}}), \quad (23)$$

which drives the sole round of 2D permutation for this layer.

- **Step 5 (Substitution Keystreams for High-Significance Layer):** The first block of $F_M F_N$ samples from $\mathbf{S}_{\text{trim}}$ is scaled under modulus 2^{48} :

$$\sigma_{H3}^{(1)} = \left\lfloor \mathbf{S}_{\text{trim}}(1 : F_M F_N) \cdot 2^{48} \right\rfloor, \quad (24)$$

with auxiliary matrices generated via modular multiplication:

$$\sigma_{H3}^{(2)} = (3\sigma_{H3}^{(1)}) \bmod 2^{48}, \quad \sigma_{H3}^{(3)} = (5\sigma_{H3}^{(1)}) \bmod 2^{48}. \quad (25)$$

Each is reshaped into an $F_M \times F_N$ matrix and applied in a distinct round of hybrid diffusion and hybrid substitution: $\sigma_{H3}^{(1)}$ in round 1, $\sigma_{H3}^{(2)}$ in round 2, and $\sigma_{H3}^{(3)}$ in round 3.

- **Step 6 (Substitution Keystreams for Medium-Significance Layer):** The second block yields

$$\sigma_{M3}^{(1)} = \left\lfloor \mathbf{S}_{\text{trim}}(F_M F_N + 1 : 2F_M F_N) \cdot 2^{48} \right\rfloor, \quad (26)$$

$$\sigma_{M3}^{(2)} = (3\sigma_{M3}^{(1)}) \bmod 2^{48}. \quad (27)$$

These matrices are used in the first and second rounds of hybrid diffusion and hybrid substitution for the medium-significance layer, respectively.

- **Step 7 (Substitution Keystream for Low-Significance Layer):** The third block is scaled under modulus 2^{32} :

$$\sigma_{L2} = \left\lfloor \mathbf{S}_{\text{trim}}(2F_M F_N + 1 : 3F_M F_N) \cdot 2^{32} \right\rfloor, \quad (28)$$

and reshaped into an $F_M \times F_N$ matrix that drives the single round of hybrid diffusion and hybrid substitution for the low-significance component.

3.5. Adaptive Dual-Mode Vector-Level Hybrid Diffusion

To achieve robust diffusion that is both content-adaptive and key-dependent, MIEA-CPHS introduces an encryption step called adaptive dual-mode vector-level hybrid diffusion. This stage operates independently on each significance layer (high, medium, and low) and is coupled with the substitution keystreams generated in Section 3.4. The diffusion process is structured in multiple rounds, three for the high-significance layer, two for the medium, and one for the low, each round alternating with an encryption step called 2D permutation with adaptive hybrid substitution (as detailed in Section 3.6).

The necessity of the vector-level architecture stems from the computational demands of the multi-round strategy described in Section 3.2. Traditional pixel-by-pixel diffusion involves computationally expensive nested loops that create significant latency, especially when reiterated multiple times. By designing the diffusion to operate on entire row or column vectors (as detailed in Algorithm 2), we leverage CPU vectorization and efficient memory access patterns. This architectural optimization acts as a necessary enabler, allowing MIEA-CPHS to execute multiple rounds of high-intensity encryption on critical layers while maintaining a high throughput.

Algorithm 2 Adaptive Dual-Mode Vector-Level Hybrid Diffusion in MIEA-CPHS.

Input: An input matrix $\mathbf{P}$ of size $F_M \times F_N$, an adaptive control value $\tilde{\kappa}$, and the first element $\tilde{\sigma}$ of the corresponding substitution keystream.

Output: The diffused output matrix $\mathbf{C}$ of size $F_M \times F_N$.

```

1: Compute the mode selector:  $f \leftarrow (\tilde{\kappa} + \tilde{\sigma}) \bmod 2$ .
2: if  $f = 1$  then
3:   Compute column split index:  $i_c \leftarrow \left\lfloor \frac{F_N}{2} \right\rfloor + \left\lfloor \tilde{\kappa} \bmod \left\lfloor \frac{F_N}{4} \right\rfloor \right\rfloor$ .
4:   Initialize first column:  $\mathbf{C}(:, 1) \leftarrow (\mathbf{P}(:, 1) + \tilde{\kappa}) \bmod 2^b$ .
5:   for  $j = 2$  to  $i_c$  do
6:      $\mathbf{C}(:, j) \leftarrow (\mathbf{P}(:, j) + \mathbf{C}(:, j-1)) \bmod 2^b$ .
7:   end for
8:   for  $j = i_c + 1$  to  $F_N$  do
9:      $\mathbf{C}(:, j) \leftarrow \mathbf{P}(:, j) \oplus \mathbf{C}(:, j-1)$ .
10:  end for
11: else
12:   Compute row split index:  $i_r \leftarrow \left\lfloor \frac{F_M}{2} \right\rfloor + \left\lfloor \tilde{\kappa} \bmod \left\lfloor \frac{F_M}{4} \right\rfloor \right\rfloor$ .
13:   Initialize first row:  $\mathbf{C}(1, :) \leftarrow (\mathbf{P}(1, :) + \tilde{\kappa}) \bmod 2^b$ .
14:   for  $i = 2$  to  $i_r$  do
15:      $\mathbf{C}(i, :) \leftarrow (\mathbf{P}(i, :) + \mathbf{C}(i-1, :)) \bmod 2^b$ .
16:   end for
17:   for  $i = i_r + 1$  to  $F_M$  do
18:      $\mathbf{C}(i, :) \leftarrow \mathbf{P}(i, :) \oplus \mathbf{C}(i-1, :)$ .
19:   end for
20: end if
```

The core of this diffusion step lies in the dual-mode diffusion, which dynamically selects between row-wise and column-wise propagation based on the adaptive control parameter κ derived from the plaintext hash digest and the current round of substitution keystream. This design ensures that even minor changes in either the plaintext or the

secret key result in drastically different diffusion trajectories, thereby achieving a strong avalanche effect and robust resistance against differential and chosen-plaintext attacks.

Notably, the two control inputs $(\tilde{\kappa}, \tilde{\sigma})$ to each diffusion round (see Algorithm 2) differ across rounds, causing the diffusion direction to vary dynamically between row-wise and column-wise modes. For the high-significance layer, the last two control inputs for each round are, respectively, as follows:

- Round 1: $\tilde{\kappa} = \kappa, \tilde{\sigma} = \sigma_{H3}^{(1)}(1, 1),$
- Round 2: $\tilde{\kappa} = \kappa + 1, \tilde{\sigma} = \sigma_{H3}^{(2)}(1, 1),$
- Round 3: $\tilde{\kappa} = \kappa + 2, \tilde{\sigma} = \sigma_{H3}^{(3)}(1, 1).$

Similarly, the medium layer uses two rounds with $\tilde{\kappa} = \kappa, \kappa + 1$ and $\tilde{\sigma} = \sigma_{M3}^{(1)}(1, 1), \sigma_{M3}^{(2)}(1, 1),$ respectively. The low layer performs a single diffusion with $\tilde{\kappa} = \kappa$ and $\tilde{\sigma} = \sigma_{L2}(1, 1).$

The precise operations of a single diffusion round are formalized in Algorithm 2, which takes the current fused matrix, the round-specific $\tilde{\kappa}$, and the first element $\tilde{\sigma}$ of the corresponding substitution matrix as inputs. By design, the algorithm's mode selection and split-point computation are driven by these two values, enabling lightweight yet highly sensitive diffusion behavior tailored to each layer's security requirements. Notably, the modular arithmetic in the diffusion operations is performed modulo 2^b , where the bit-width b is layer-adaptive: $b = 48$ for both the high- and medium-significance layers, and $b = 32$ for the low-significance layer.

3.6. 2D Permutation with Adaptive Hybrid Substitution

Complementing the diffusion mechanism in Section 3.5, MIEA-CPHS employs a tightly integrated permutation–substitution step named 2D permutation with adaptive hybrid substitution. This operation is applied to each significance layer after every diffusion round, forming an alternating sequence of diffusion, permutation, and substitution, thereby enhancing security while maintaining high encryption efficiency.

Specifically, for the high-significance layer, three rounds of this operation are executed; for the mid-significance layer, two rounds; and for the low-significance layer, one round. Each invocation consumes four inputs: an input diffused pixel matrix, a permutation keystream $\tilde{\pi}$, a substitution matrix $\tilde{\sigma}$, and an adaptive control parameter $\tilde{\kappa}$. The precise procedure is formalized in Algorithm 3, which operates in three sequential phases:

1. **2D Permutation:** The input matrix is shuffled row-wise and column-wise using sorted indices derived from the permutation vector $\tilde{\pi}$.
2. **Segmented Modular Addition:** The permuted matrix undergoes a three-segment horizontal (column-wise) modular addition, where segment boundaries are dynamically determined by $\tilde{\kappa}$.
3. **Adaptive Dual-Mode Substitution:** Depending on $\tilde{\kappa}$, the result is either combined with $\tilde{\sigma}$ via modular addition or bitwise XOR, enabling a dual-mode, key-driven substitution mechanism.

Critically, the modulus used in all modular operations is layer-specific: 2^{48} for the high- and medium-significance layers, and 2^{32} for the low-significance layer. Round-specific inputs are used as follows:

- For the high-significance layer, the r -th permutation and substitution round ($r = 1, 2, 3$) uses permutation keystream $\pi_{H3}^{(r)}$, substitution matrix $\sigma_{H3}^{(r)}$, and control parameter $\kappa + r$.
- For the medium-significance layer, the r -th round ($r = 1, 2$) uses $\pi_{M3}^{(r)}, \sigma_{M3}^{(r)}$, and $\kappa + r$.
- For the low-significance layer, a single round is performed using π_{L2}, σ_{L2} , and $\kappa + 1$.

Algorithm 3 2D Permutation with Adaptive Dual-Mode Substitution in MIEA-CPHS.

Input: An input matrix $\mathbf{P}$ of size $F_M \times F_N$, a permutation keystream $\tilde{\pi}$ of length $F_M + F_N$, a substitution matrix $\tilde{\sigma}$ of size $F_M \times F_N$, and the adaptive control parameter $\tilde{\kappa}$.

Output: The substituted and permuted output matrix $\mathbf{C}$ of size $F_M \times F_N$.

```

1: Compute row sorting indices:  $\pi_r \leftarrow \text{sort}(\tilde{\pi}(1 : F_M))$ .
2: Compute column sorting indices:  $\pi_c \leftarrow \text{sort}(\tilde{\pi}(F_M + 1 : F_M + F_N))$ .
3: Apply 2D permutation:  $\mathbf{C} \leftarrow \mathbf{P}(\pi_r, \pi_c)$ .
4: if  $F_N < 3$  then
5:    $\mathbf{C} \leftarrow (\mathbf{C} + 3\tilde{\kappa}) \bmod 2^b$ 
6: else
7:    $q \leftarrow \max(1, \lfloor F_N/4 \rfloor)$ 
8:    $o_1 \leftarrow \lfloor \tilde{\kappa} \bmod q \rfloor$ ,  $o_2 \leftarrow \lfloor (7\tilde{\kappa}) \bmod q \rfloor$ 
9:    $j_1 \leftarrow \min(\max(1, \lfloor F_N/4 \rfloor + o_1), F_N - 2)$ 
10:   $j_2 \leftarrow \min(\max(j_1 + 1, j_1 + o_2), F_N - 1)$ 
11:   $\mathbf{C}(:, 1 : j_1) \leftarrow (\mathbf{C}(:, 1 : j_1) + 2\tilde{\kappa}) \bmod 2^b$ 
12:   $\mathbf{C}(:, j_1 + 1 : j_2) \leftarrow (\mathbf{C}(:, j_1 + 1 : j_2) + 3\tilde{\kappa}) \bmod 2^b$ 
13:   $\mathbf{C}(:, j_2 + 1 : F_N) \leftarrow (\mathbf{C}(:, j_2 + 1 : F_N) + 4\tilde{\kappa}) \bmod 2^b$ 
14: end if
15: if  $\tilde{\kappa} \bmod 3 = 2$  then
16:    $\mathbf{C} \leftarrow \mathbf{C} \oplus \tilde{\sigma}$ 
17: else
18:    $\mathbf{C} \leftarrow (\mathbf{C} + \tilde{\sigma}) \bmod 2^b$ 
19: end if

```

3.7. Brief Overview of the Decryption Process

The decryption process of MIEA-CPHS is the exact inverse of the encryption procedure, executed in reverse order using the same secret key K . Notably, the 48-bit adaptive control parameter κ , which governs keystream generation, diffusion, permutation, and substitution, is not derived from the (unknown) plaintext but is reconstructed by the receiver from the SHA-384 hash digest $\mathbf{h}$ that is transmitted alongside the ciphertext. Specifically, upon receiving $\mathbf{h}$, the receiver computes κ via the same four-step procedure as in encryption. This allows all round-dependent parameters (e.g., $\tilde{\pi}$, $\tilde{\sigma}$, $\tilde{\kappa}$) to be correctly instantiated before decryption begins.

Each significance layer is then decrypted with the corresponding number of inverse rounds (three for high-, two for medium-, one for low-significance), followed by inverse hierarchical bit-plane fusion and tensor reshaping using the metadata $\mathcal{M} = (M, N, \mathbf{c})$ to recover the original images losslessly. After decryption, the receiver recomputes the hash from the recovered fused matrices and compares it with the received $\mathbf{h}$ to verify both data integrity and decryption correctness. Since all encryption operations are bijective and fully determined by the secret key K and the adaptive parameter κ , and since κ can be exactly reconstructed from the received hash digest $\mathbf{h}$, the original plaintext is uniquely recoverable. Consequently, the decryption process is the exact inverse of encryption; its detailed description is omitted for brevity.

4. Experiments and Analyses

This section presents a comprehensive validation of the proposed MIEA-CPHS, evaluating its performance on two key dimensions: cryptographic security and practical efficiency. Security is assessed by the algorithm's resilience against a suite of standard crypt-analytic attacks, while efficiency is quantified primarily by its encryption throughput. To ensure comparability and reproducibility, all experiments were conducted in a standardized environment: MATLAB R2017a on a computer equipped with an Intel E3-1231 processor (3.40 GHz) and 8 GB of RAM. Test images were drawn from the standard USC-SIPI image

database. Furthermore, to guarantee an unbiased evaluation, secret keys were randomly generated for each independent security test.

4.1. Visual Analysis

Visual security requires that encrypted images reveal no discernible trace of the original content, appearing as pure noise to the human eye. To evaluate this property, our MIEA-CPHS was tested on five images with diverse resolutions and textures (Figure 7). As observed, all output ciphertexts exhibit visual randomness and contain no meaningful patterns. Moreover, decryption using the correct key perfectly reconstructs the original inputs, confirming that the MIEA-CPHS is both lossless and fully invertible.

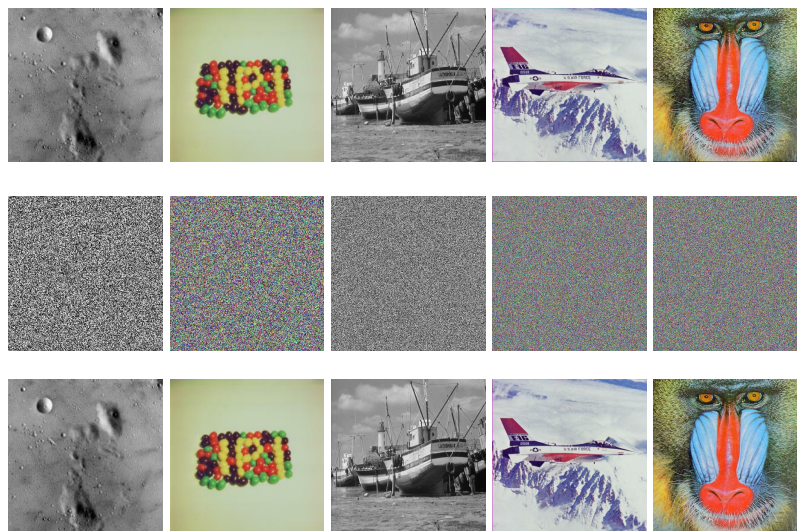


Figure 7. Visual analysis on MIEA-CPHS: The first row shows five input images (5.1.09, 4.1.07, boat.512, 4.2.05, and 4.2.03); the second row displays their encrypted counterparts; and the third row presents the corresponding decrypted images.

4.2. Key Space

The security of an encryption algorithm against brute-force attacks hinges on the cardinality of its key space. A sufficiently large key space renders exhaustive key search computationally infeasible, thereby preventing successful brute-force attacks [47]. In contemporary cryptographic practice, a key space of at least 2^{128} is widely regarded as the minimum requirement for robust classical security. Furthermore, in the post-quantum era, this requirement is strengthened: to preserve a 128-bit security level against quantum-accelerated attacks, such as those based on Grover's algorithm, a symmetric key space of size 2^{256} is now considered necessary [53].

As described in Section 3.1, the secret key $\mathcal{K}$ of MIEA-CPHS comprises nine components: the control parameters $(\theta^{(1)}, \gamma^{(1)}, \theta^{(2)}, \gamma^{(2)})$ and initial values $(x_0^{(1)}, y_0^{(1)}, x_0^{(2)}, y_0^{(2)})$ for two independent instances of the 2D-CCHM-EP, and an integer transient length α . The control parameters are drawn from the closed interval $[1, 13]$, while the initial values lie in the open interval $(0, 1)$. In the MIEA-CPHS, these eight real-valued components are implemented with a uniform numerical precision of 10^{-14} . Under this precision, each control parameter admits approximately 1.2×10^{15} distinct values, while each initial value supports 10^{14} possible values. The integer parameter α is selected from the practical range $[200, 1200]$, yielding approximately 10^3 possible values. Consequently, the total key space size $|\mathcal{K}|$ is given by

$$\begin{aligned}
|\mathcal{K}| &= \left(1.2 \times 10^{15} \cdot 1.2 \times 10^{15} \cdot 10^{14} \cdot 10^{14}\right)^2 \cdot 10^3 \\
&= \left(1.44 \times 10^{58}\right)^2 \cdot 10^3 \\
&= 2.0736 \times 10^{119} \approx 2^{397}.
\end{aligned} \tag{29}$$

Since $|\mathcal{K}| \approx 2^{397} \gg 2^{256}$, the key space of MIEA-CPHS exceeds the post-quantum security threshold, rendering brute-force attacks infeasible even under quantum adversaries.

4.3. Key Sensitivity

A fundamental property of any secure cryptosystem is extreme sensitivity to its secret key. This requires that even a minimal alteration in the key must cascade to produce a completely different and uncorrelated ciphertext [54,55]. This behavior is the primary defense against differential attacks that attempt to deduce the key by comparing ciphertexts generated from closely related keys.

To evaluate the key sensitivity of MIEA-CPHS, we performed a controlled experiment whose results are presented in Figure 8. We began by defining a base secret key $\mathcal{K}^{(b)}$ with randomly chosen values from the valid key space:

$$\mathcal{K}^{(b)} = \begin{cases} \theta^{(1)} = 11.237885160869109, \\ \gamma^{(1)} = 5.614888174719484, \\ x_0^{(1)} = 0.112705677161724, \\ y_0^{(1)} = 0.346717246178014, \\ \theta^{(2)} = 2.842757828942319, \\ \gamma^{(2)} = 7.668183447408417, \\ x_0^{(2)} = 0.471700071387344, \\ y_0^{(2)} = 0.520149028090077, \\ \alpha = 531. \end{cases}$$

This key was used to encrypt the standard test image 5.1.11, yielding a reference ciphertext C . Next, we generated nine perturbed keys $\mathcal{K}_1$ through $\mathcal{K}_9$, each differing from $\mathcal{K}^{(b)}$ in only one component, modified by the minimal representable amount (i.e., 10^{-14} for floating-point parameters or $+1$ for the integer α). Using these slightly altered keys, we re-encrypted the same image to obtain nine new ciphertexts C_1 to C_9 , enabling a direct assessment of how minute key changes affect the encrypted output.

As shown in Figure 8b,(c1–c9), the base ciphertext C and nine example modified ciphertexts (C_1 to C_9) are all visually indistinguishable from random noise, completely obscuring the plaintext content. More importantly, Figure 8(d1–d9) shows the difference images. These difference images are also entirely random and unstructured, visually confirming that a minimal change in any single key component results in a completely different and unpredictable output ciphertext. This demonstrates that MIEA-CPHS possesses exceptionally high key sensitivity, rendering brute-force and key-differential attacks computationally infeasible.

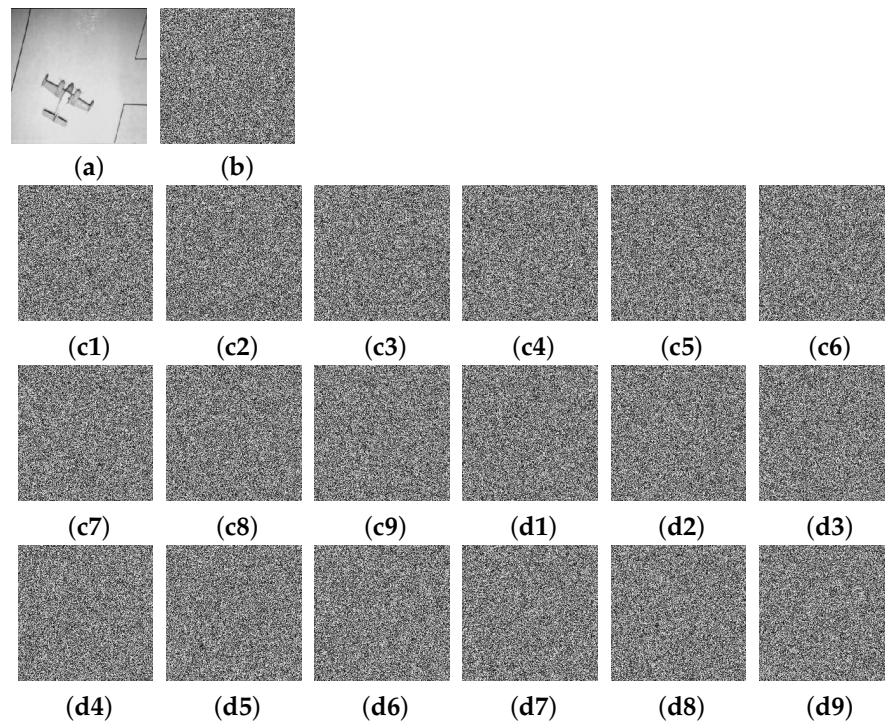


Figure 8. Key sensitivity analysis of MIEA-CPHS. (a) Original test image 5.1.11; (b) Ciphertext generated using the base key $\mathcal{K}^{(b)}$. Panels (c1–c9) show ciphertexts produced by perturbing a single component of $\mathcal{K}^{(b)}$ by the minimal representable amount: 10^{-14} for all floating-point key components $(\theta^{(1)}, \gamma^{(1)}, x_0^{(1)}, y_0^{(1)}, \theta^{(2)}, \gamma^{(2)}, x_0^{(2)}, y_0^{(2)})$ and +1 for the integer key component α . The corresponding difference images in (d1–d9) are computed as $\text{mod}(C - C_i, 256)$ for $i = 1, \dots, 9$, and appear as random noise.

4.4. Pixel Distribution

The capacity of an image cryptosystem to produce a highly uniform pixel distribution is a key indicator of its resistance to statistical cryptanalysis [47]. In Figure 9, the distribution plots of the original images exhibit distinct peaks and valleys, reflecting their content-dependent statistical characteristics. In contrast, the ciphertexts generated by MIEA-CPHS display nearly flat distributions, effectively concealing the original statistical structure and thereby thwarting distribution-based attacks.

Furthermore, we also employed the chi-square test to critically examine whether the pixel values in MIEA-CPHS's ciphertexts follow a uniform distribution. The test statistic is given by

$$Q = \sum_{v=0}^{255} \frac{(N_v - N_{\text{exp}})^2}{N_{\text{exp}}} \quad (30)$$

where N_v denotes the count of pixels with intensity v , and $N_{\text{exp}} = R \times C / 256$ is the expected count for each intensity level in an ideal uniform distribution, with R and C denoting the image height and width. Under a 0.05 significance level, the critical value is 293.2478 [56]. The results in Table 5 show that all computed Q values are substantially lower than this threshold, confirming that the output pixels are statistically uniform. Such uniformity significantly reduces the likelihood of successful statistical attacks based on pixel frequency analysis.

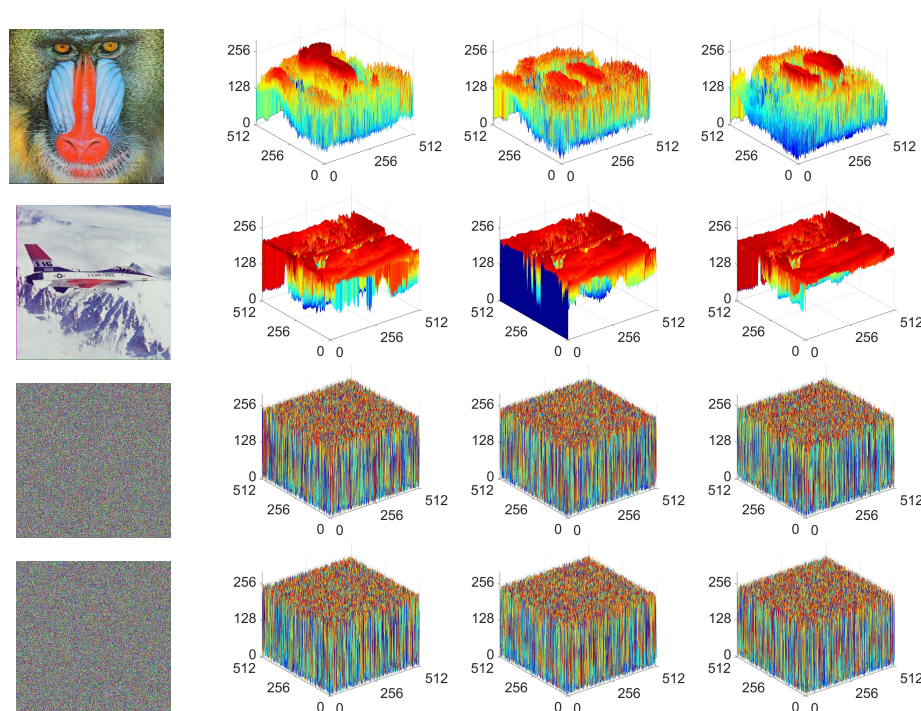


Figure 9. Three-dimensional pixel distribution plots for the simultaneous encryption of two test images by MIEA-CPHS: The first and second rows display the original images 4.2.03 and 4.2.05, respectively, each accompanied by three 3D distribution plots corresponding to their red (R), green (G), and blue (B) color planes. The third and fourth rows present the corresponding ciphertexts and their pixel distributions.

Table 5. Obtained Chi-square test scores on MIEA-CPHS (passed if <293.2478).

Size	Image	χ^2 Value	Passed or Not
256 × 256	5.1.12	228.0547	Yes
	5.1.13	256.9844	Yes
	5.1.14	247.1563	Yes
512 × 512	7.1.03	238.6699	Yes
	7.1.04	245.9668	Yes
	7.1.05	261.4297	Yes
1024 × 1024	5.3.01	267.5874	Yes
	5.3.02	229.7222	Yes
	7.2.01	210.9365	Yes

4.5. Shannon Entropy

The randomness of pixel values in a ciphertext image is commonly quantified using Shannon entropy, which serves as a key indicator of an encryption scheme's ability to conceal statistical information [57]. For the digital images with 256 intensity levels, this metric is computed as [58]

$$\mathcal{H} = - \sum_{v=0}^{255} \Pr(v) \cdot \log_2 \Pr(v), \quad (31)$$

where $\Pr(v)$ indicates the frequency of intensity level v . An ideal random image has an entropy of 8, indicating maximal uncertainty. We encrypted eight test images using MIEA-CPHS and evaluated the resulting entropy values (see Table 6). The results reveal that the ciphertext entropies are consistently above 7.999 and closely approach the theoretical maximum, while the plaintext values are substantially lower. This confirms that MIEA-CPHS produces highly randomized outputs, significantly enhancing security against entropy-based analysis.

Table 6. Shannon entropy analysis of eight images before and after encryption using MIEA-CPHS.

Size	Image	Plaintext	Ciphertext
512 × 512	5.2.08	7.2010	7.9994
	7.1.01	6.0274	7.9993
	7.1.04	6.1074	7.9993
	7.1.07	5.9916	7.9994
	7.1.10	5.9088	7.9994
1024 × 1024	5.3.01	7.5237	7.9999
	5.3.02	6.8303	7.9999
	7.2.01	5.6415	7.9998
	Avg.	6.4040	7.9996

4.6. Pixel Correlation

Natural images inherently exhibit strong inter-pixel statistical redundancies, which constitute a critical vulnerability exploitable by correlation-based cryptanalytic attacks [40]. Consequently, a secure image cryptosystem must thoroughly suppress these spatial dependencies to ensure robustness against such threats. We assessed this capability of MIEA-CPHS using the test images 4.2.05 and 4.2.07, analyzing their pixel correlations before and after encryption. Figure 10 reveals that the original images exhibit strong directional correlations, whereas the encrypted outputs display uniformly scattered, structure-free distributions across all tested orientations. These results indicate that our MIEA-CPHS effectively randomizes pixel relationships independent of the input content, fulfilling a key requirement for secure image encryption.

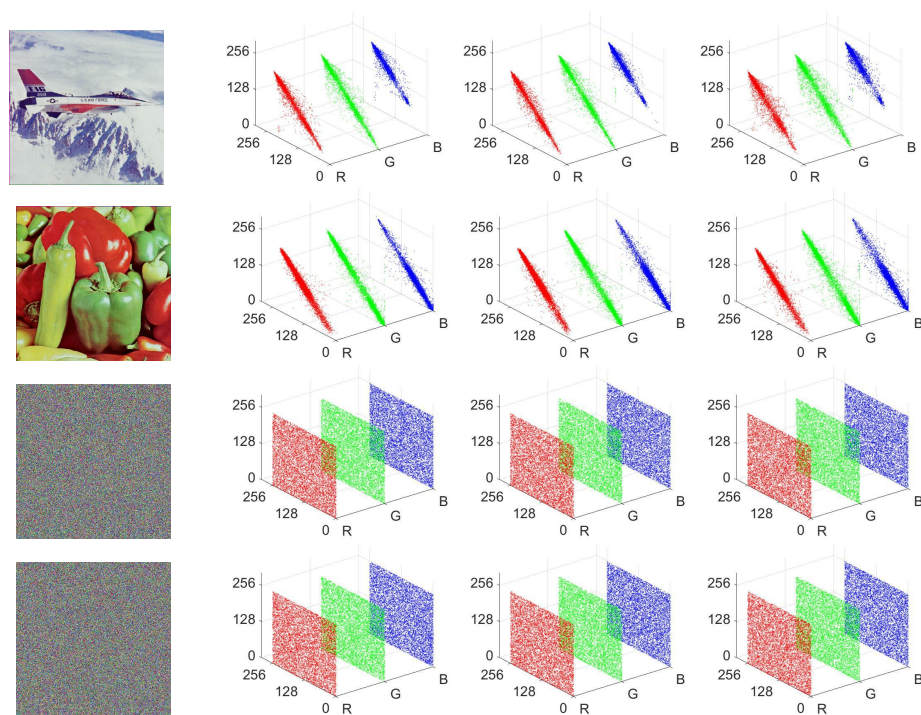


Figure 10. Correlation analysis for the simultaneous encryption of two images by MIEA-CPHS: The first two rows illustrate the original images 4.2.05 and 4.2.07, respectively, alongside their strong correlations across horizontal, vertical, and diagonal orientations. The third and fourth rows depict the corresponding encrypted images and their near-random correlation characteristics. These results visually confirm that MIEA-CPHS effectively eliminates spatial redundancy across multiple distinct inputs.

Furthermore, we numerically assessed the degree of correlation between neighboring pixels by using the standard correlation coefficient derived from probability theory, calculated as [59,60]

$$r = \frac{\text{Cov}(u, v)}{\sqrt{\text{Var}(u) \cdot \text{Var}(v)}}, \quad (32)$$

where u and v denote neighboring pixel intensities, $\text{Cov}(\cdot, \cdot)$ is the covariance, and $\text{Var}(\cdot)$ is the variance. The obtained correlation coefficient values are summarized in Table 7. The results reveal that the original images have high coefficient absolute values (all >0.82), whereas the encrypted outputs show negligible absolute values (<0.0016) across all orientations. This dramatic reduction demonstrates the superior capability of MIEA-CPHS in eliminating spatial redundancy, thereby significantly enhancing its resistance to statistical cryptanalysis.

Table 7. Correlation coefficient for MIEA-CPHS.

Size	Name	Original Image			Encrypted Image		
		Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
256×256	5.1.10	0.8613	0.9051	0.8215	−0.0014	−0.0015	−0.0004
	5.1.12	0.9753	0.9519	0.9384	0.0015	−0.0014	0.0015
	5.1.14	0.8933	0.9474	0.8496	−0.0008	0.0008	0.0005
512×512	5.2.08	0.9026	0.9367	0.8754	−0.0011	0.0015	0.0007
	7.1.01	0.9200	0.9621	0.9048	0.0010	0.0002	0.0003
	7.1.04	0.9668	0.9768	0.9554	0.0006	−0.0001	−0.0012
1024×1024	5.3.01	0.9818	0.9761	0.9672	0.0011	0.0005	−0.0012
	5.3.02	0.9036	0.9133	0.8637	−0.0002	−0.0001	−0.0014
	7.2.01	0.9509	0.9641	0.9424	0.0015	−0.0002	−0.0007

4.7. Differential Attacks

Differential cryptanalysis leverages minute plaintext perturbations to infer keystreams by observing corresponding ciphertext changes [61]. An effective image cryptosystem must therefore be highly sensitive to such perturbations. To evaluate the MIEA-CPHS, we generated two variants of image boat.512 by flipping a single bit in each (see Figure 11(b1,b2)), encrypted them, and computed their differences relative to the original ciphertext. After encryption, the differences between these ciphertexts and the original are indistinguishable from random noise (see Figure 11(f1,f2)). This outcome verifies that flipping a single bit triggers a complete random transformation in the output ciphertext, underscoring the strong resilience of MIEA-CPHS to differential cryptanalysis.

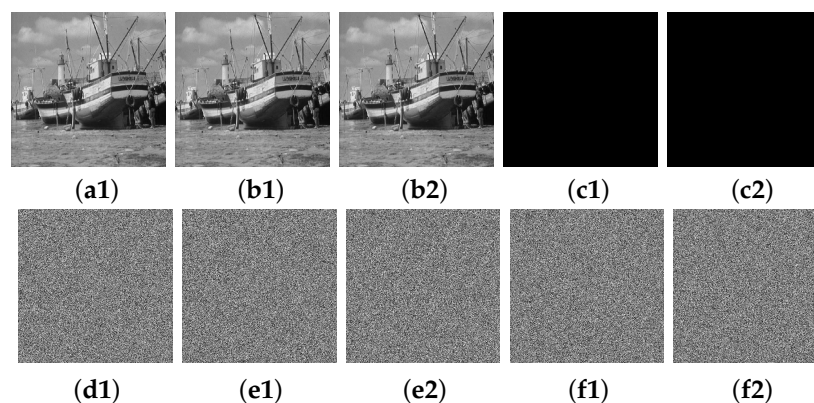


Figure 11. Sensitivity of MIEA-CPHS to single-bit pixel perturbations: (a1) boat.512; (b1) least significant bit (LSB) of pixel at (3, 1) was flipped; (b2) LSB of pixel at (510, 512) was flipped; (c1) difference of (a1,b1), (c2) difference of (a1,b2); (d1) ciphertext of boat.512; (e1) ciphertext of (b1), (e2) ciphertext of (b2), (f1) difference of (d1,e1), (f2) difference of (d1,e2).

To rigorously evaluate the sensitivity of MIEA-CPHS under single-bit perturbations, we adopt two standard statistical measures. The normalized pixel change rate (NPCR) quantifies the percentage of ciphertext pixels that differ when a single bit in the plaintext is flipped, with an ideal value of 99.6094%. Separately, the unified average changing intensity (UACI) captures the average absolute difference in intensity between corresponding pixel pairs, for which the theoretical optimum is 33.4635%. For two pixel matrix $\mathbf{I}$ and $\mathbf{I}'$ of size $R \times C$, these metrics are computed as

$$\begin{cases} \text{NPCR}(\mathbf{I}, \mathbf{I}') = \frac{1}{R \times C} \sum_{i=1}^R \sum_{j=1}^C D(i, j) \times 100\%, \\ \text{UACI}(\mathbf{I}, \mathbf{I}') = \frac{1}{255 \times R \times C} \sum_{i=1}^R \sum_{j=1}^C |\mathbf{I}(i, j) - \mathbf{I}'(i, j)| \times 100\% \end{cases} \quad (33)$$

where $D(i, j) = 1$ if $\mathbf{I}(i, j) \neq \mathbf{I}'(i, j)$, and $D(i, j) = 0$ otherwise.

Tables 8 and 9 summarize the differential analysis results. In each trial, one bit of a randomly chosen plaintext pixel was flipped. MIEA-CPHS achieves mean NPCR and UACI values of 99.61% and 33.46%, respectively, virtually matching their theoretical ideals (99.6094% and 33.4635%). Compared with three recent algorithms, it not only reaches closer to these benchmarks but also exhibits lower score variance across trials, confirming its strong and stable sensitivity to minimal plaintext perturbations.

To formally validate the statistical significance of these results, we conducted hypothesis tests at the significance level $\alpha = 0.05$, following the rigorous framework established by Wu et al. [62]. Note that in randomness testing, the acceptance interval for $\alpha = 0.05$ is narrower (i.e., stricter) than that for $\alpha = 0.01$, requiring the experimental values to cluster more closely around the theoretical ideal. The critical threshold for NPCR ($\mathcal{N}_{0.05}^*$) and the acceptance interval for UACI ($[\mathcal{U}_{0.05}^{*-}, \mathcal{U}_{0.05}^{*+}]$) for the image sizes used in our experiments are as follows:

- For 256×256 : $\mathcal{N}_{0.05}^* = 99.5693\%$, UACI interval: $[33.2824\%, 33.6447\%]$.
- For 512×512 : $\mathcal{N}_{0.05}^* = 99.5893\%$, UACI interval: $[33.3730\%, 33.5541\%]$.
- For 1024×1024 : $\mathcal{N}_{0.05}^* = 99.5994\%$, UACI interval: $[33.4183\%, 33.5088\%]$.

As shown in Tables 8 and 9, all NPCR values obtained by MIEA-CPHS exceed their respective critical thresholds, and all UACI values fall strictly within the theoretical acceptance intervals, thereby passing the statistical tests at the 5% significance level.

Table 8. NPCR values (%) achieved by MIEA-CPHS and three recent algorithms.

Size	Image	[63]	[64]	[65]	MIEA-CPHS
256×256	5.1.09	99.5938	99.6140	99.5865	99.5932
	5.1.10	99.5910	99.6246	99.6124	99.6094
	5.1.11	99.6353	99.6094	99.6155	99.6140
	5.1.12	99.6078	99.6155	99.6063	99.5942
	5.1.13	99.5986	99.6058	99.6094	99.6109
512×512	5.2.08	99.6124	99.6151	99.5895	99.6155
	7.1.01	99.6128	99.5945	99.6231	99.6048
	7.1.03	99.6158	99.6025	99.6067	99.6181
	7.1.05	99.6086	99.5907	99.6174	99.6044
	7.1.07	99.6120	99.6018	99.6304	99.6185
1024×1024	5.3.01	99.6023	99.6170	99.6082	99.6199
	5.3.02	99.6170	99.6197	99.6046	99.6109
	Avg	99.6090	99.6092	99.6092	99.6095
	Std. Dev.	0.0119	0.0103	0.0124	0.0089

Table 9. UACI values (%) achieved by MIEA-CPHS and three recent algorithms.

Size	Image	[63]	[64]	[65]	MIEA-CPHS
256×256	5.1.09	33.5381	33.4780	33.4424	33.3952
	5.1.10	33.4521	33.4174	33.4631	33.5140
	5.1.11	33.5348	33.4891	33.4394	33.5188
	5.1.12	33.4535	33.5213	33.4703	33.4355
	5.1.13	33.4640	33.5093	33.5157	33.4553
512×512	5.2.08	33.4030	33.3891	33.5789	33.4364
	7.1.01	33.4582	33.4022	33.4053	33.4781
	7.1.03	33.5914	33.5162	33.5168	33.5263
	7.1.05	33.4521	33.5354	33.5248	33.4606
	7.1.07	33.5259	33.4824	33.4218	33.4499
1024×1024	5.3.01	33.4238	33.4994	33.3963	33.4352
	5.3.02	33.4290	33.3923	33.4247	33.4589
	Avg	33.4772	33.4693	33.4666	33.4637
	Std. Dev.	0.0568	0.0539	0.0562	0.0393

4.8. Robustness Analysis

During storage or transfer, ciphertext pixels are prone to corruption or loss, making robustness a critical requirement for image cryptosystems [64]. To evaluate the resilience of MIEA-CPHS against ciphertext degradation, we conducted targeted experiments simulating noise attacks and data loss scenarios.

First, we intentionally injected salt-and-pepper noise into the ciphertext of image 2.1.05 at different intensity levels. The noise intensity is characterized by the noise density η . Specifically, we tested $\eta \in \{2\%, 4\%, 6\%, 8\%\}$ (see the first row of Figure 12). Subsequently, all ciphertext images were decrypted using MIEA-CPHS. As shown in Figure 12, even under severe noise corruption (up to $\eta = 8\%$), the decrypted outputs retain sufficient structural fidelity for human interpretation. While perceptual quality declines progressively with increasing noise density, the core semantic features remain largely intact. This demonstrates that MIEA-CPHS exhibits good resilience to noise attacks, confirming its suitability for applications where ciphertext integrity may be compromised.

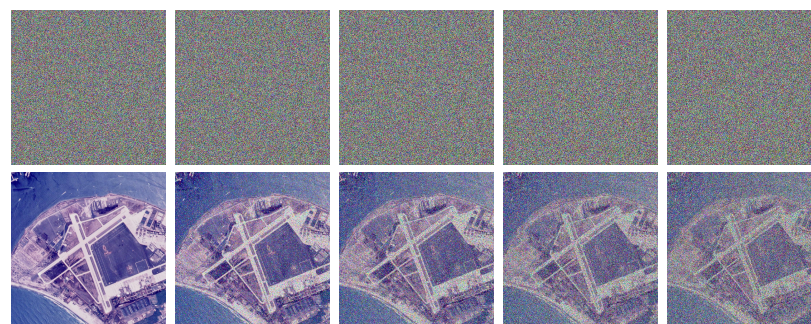


Figure 12. Resilience of the MIEA-CPHS scheme against noise-induced perturbations: The top row presents the original ciphertext alongside versions degraded by additive noise at intensities of 2%, 4%, 6%, and 8%. The bottom row illustrates the images recovered through decryption from these corrupted ciphertexts.

Analogously, data loss scenarios were simulated by excising multiple regions from the ciphertext of image 4.2.03. The resulting truncated ciphertexts and their respective reconstructions after decryption are displayed in Figure 13. Notably, the fidelity of the recovered images diminishes with increasing data removal. Nevertheless, even when a significant portion (a central block of size 288×288) is removed, the essential visual semantics of the source image remain perceptible. This outcome underscores the good resilience of MIEA-CPHS to data loss attacks.

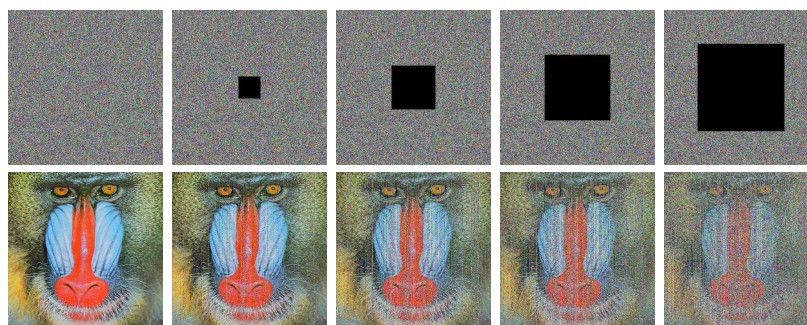


Figure 13. Resilience of MIEA-CPHS to data loss: The top part presents the original ciphertext and its corrupted versions with missing blocks of sizes 72×72 , 144×144 , 216×216 , and 288×288 . The bottom part shows the images recovered through decryption.

4.9. Resistance to Common Attack Models

Cryptanalytic attacks are conventionally classified into four levels based on the adversary's available resources: ciphertext-only attack (COA), known-plaintext attack (KPA), chosen-plaintext attack (CPA), and chosen-ciphertext attack (CCA) [56]. Among these, CPA and CCA constitute the most stringent threat models, as they allow the attacker to adaptively probe the cryptosystem with specific inputs to extract the static secret key or equivalent keystreams. Consequently, a cryptosystem that resists CPA and CCA is inherently secure against the weaker KPA and COA scenarios.

The proposed MIEA-CPHS achieves robust resistance against these attacks through its hash-based adaptive control mechanism, centered on the 48-bit parameter κ . As defined in Section 3.3 (Equation (16)), κ is derived from the SHA-384 hash digest h of the fused plaintext. Critically, the parameter κ governs all subsequent primitives—including hyperchaotic keystream generation (Section 3.4), adaptive dual-mode vector-level hybrid diffusion (Section 3.5), and 2D permutation with adaptive hybrid substitution (Section 3.6). This creates a one-time-pad-like effect where the operational keystreams are unique to each input instance.

In a CPA scenario, an adversary chooses specific plaintexts (e.g., low-entropy images) and analyzes their corresponding ciphertexts to infer the internal state. However, MIEA-CPHS employs a plaintext-dependent keystream generation strategy that neutralizes this attack:

- Every distinct chosen plaintext P_{chosen} yields a unique hash digest, resulting in a unique control parameter κ_{chosen} .
- This κ_{chosen} drives the MIEA-CPHS to generate a specific set of permutation and substitution keystreams exclusive to P_{chosen} .
- Due to the collision resistance and avalanche effect of SHA-384, even a single-bit difference between the chosen plaintext and the target plaintext P_{target} results in $\kappa_{\text{chosen}} \neq \kappa_{\text{target}}$. Consequently, the keystreams derived from the chosen input are mathematically uncorrelated with those used for the target, rendering the analysis of chosen plaintexts useless for cracking the target ciphertext.

In a CCA, the adversary submits forged or chosen ciphertexts to a decryption oracle to extract key information. In MIEA-CPHS, the decryption process is strictly bound to the received hash digest h .

- To decrypt a chosen ciphertext C_{chosen} , the receiver (or oracle) must use the accompanying h_{chosen} to reconstruct κ_{chosen} .
- The resulting decryption keystreams are valid *only* for that specific $(C_{\text{chosen}}, h_{\text{chosen}})$ pair.

- Any information gained from this decryption cannot be generalized to other ciphertexts, as the underlying dynamic parameter κ changes with every hash value. Thus, the static secret key $\mathcal{K}$ remains protected.

In summary, the SHA-384-driven adaptive feedback loop ensures that MIEA-CPHS effectively resists CPA, CCA, KPA, and COA, meeting the high security standards required for modern image transmission.

4.10. Efficiency Analysis

In high-throughput application scenarios such as telehealth, social media, and cloud services, encryption efficiency is also a critical consideration. To address the growing demand for fast and secure image transmission, MIEA-CPHS achieves high encryption efficiency through a series of architectural innovations [47]. It employs a lightweight hyperchaotic map to generate keystreams with minimal computational and resource overhead. Meanwhile, a significance-aware bit splitting and recombination mechanism reduces computational burdens without sacrificing security. Strategically, hash values are utilized to eliminate redundant regeneration of chaotic sequences. Finally, vectorized encryption processing is adopted to significantly boost the encryption throughput, ensuring that the MIEA-CPHS can better meet the encryption efficiency requirements for various high-throughput applications.

When encrypting an image of resolution $M \times N$, all rationally engineered encryption schemes inherently exhibit linear time complexity relative to the total number of pixels, i.e., $\mathcal{O}(M \times N)$, since each pixel requires cryptographic transformation. Thus, the distinction among such methods does not lie in their theoretical complexity class but rather in their practical computational overhead. To objectively underscore the superior computational efficiency of MIEA-CPHS, we conducted a set of comparative experiments under strictly controlled computational environments. This ensured that any observed performance differences could not be attributed to variations in hardware specifications or software settings.

Tables 10 and 11 present a performance comparison between MIEA-CPHS and four recently proposed algorithms. At three standard input dimensions, MIEA-CPHS exhibited significantly faster execution. It takes an average of only 0.6111 s to encrypt two 1024×1024 color images, achieving a total average throughput of up to 87.6152 Mbps. Evidently, compared with many recently reported encryption algorithms, MIEA-CPHS can better meet the efficiency requirements of various high-throughput applications.

Table 10. Average encryption time (in seconds) of MIEA-CPHS versus four recent algorithms.

Algorithm	$256 \times 256 \times 3 \times 2$	$512 \times 512 \times 3 \times 2$	$1024 \times 1024 \times 3 \times 2$
[56]	0.4677	1.8929	8.0234
[40]	0.2509	1.1647	5.5240
[66]	0.1944	0.9828	5.4708
[65]	0.1338	0.5676	2.3916
MIEA-CPHS	0.0314	0.1352	0.6111

Table 11. Average encryption throughput (in Mbps) of MIEA-CPHS versus four recent algorithms.

Algorithm	$256 \times 256 \times 3 \times 2$	$512 \times 512 \times 3 \times 2$	$1024 \times 1024 \times 3 \times 2$	Average
[56]	6.4144	6.3395	5.9825	6.2454
[40]	11.9570	10.3031	8.6894	10.3165
[66]	15.4321	12.2100	8.7739	12.1387
[65]	22.4215	21.1416	20.0702	21.2111
MIEA-CPHS	95.5414	88.7574	78.5469	87.6152

5. Conclusions

This paper addresses a fundamental challenge in secure visual communication: designing image encryption systems that simultaneously ensure high security and computational efficiency. To overcome the limitations of existing schemes, namely, weak chaotic dynamics and deficient cryptographic architectures, we introduce a new 2D hyperchaotic map called 2D-CCHM-EP. By incorporating exponential parameters and strengthening interdependence among state variables, we theoretically establish that the 2D-CCHM-EP exhibits strict local expansiveness across its entire parameter space, effectively suppressing periodic windows and ensuring robust hyperchaotic behavior. Comprehensive numerical analyses, including bifurcation diagrams and phase-space trajectories, validate this aperiodicity and ergodicity. Moreover, the 2D-CCHM-EP demonstrates clear superiority over several recently reported chaotic maps, yielding significantly higher LEs and Kolmogorov–Sinai entropy. It also successfully passes all NIST SP 800-22 randomness tests, verifying the statistical independence of the generated sequences and confirming its status as a highly reliable entropy source for cryptographic applications.

Leveraging this robust chaotic source, we developed the MIEA-CPHS, a multi-image encryption algorithm that employs a novel hierarchical significance-aware encryption strategy. This innovative architecture decomposes image data into high-, medium-, and low-significance layers, applying differentiated encryption rounds (three, two, and one, respectively), thereby optimally balancing security and speed. The algorithm further integrates an SHA-384-based adaptive parameter generation mechanism with high-performance vector-level diffusion, permutation, and substitution operations. Extensive security analyses confirm the algorithm's outstanding performance: it achieves near-ideal Shannon entropy (>7.999), near-zero pixel correlation (<0.0016), and outstanding resistance to differential attacks ($\text{NPCR} \approx 99.61\%$, $\text{UACI} \approx 33.46\%$). Notably, its hierarchical and vectorized design enables an average encryption throughput of 87.6152 Mbps. Regarding algorithmic complexity, while the theoretical time complexity remains linear $\Theta(M \times N)$, our strategy optimizes the practical computational load by allocating intensive operations only to high-significance data, distinguishing it from uniform encryption schemes. This exceptional balance makes MIEA-CPHS highly suitable for modern high-throughput applications like secure cloud storage and real-time media transmission.

Future research will focus on three promising avenues. First, we will develop hardware-efficient implementations of both the 2D-CCHM-EP map and the MIEA-CPHS algorithm, specifically investigating the system's behavior under varying hardware precisions (e.g., finite-precision effects on FPGAs) to ensure robustness against degradation. Second, the hierarchical significance-aware framework will be extended to heterogeneous data modalities, such as video sequences and 3D medical imaging, where adaptive, layer-specific security can significantly enhance both efficiency and protection. Finally, we intend to generalize the underlying chaotic dynamics by constructing higher-dimensional variants of the 2D-CCHM-EP, and further quantify the statistical independence between generated sequences under different sampling conditions, thereby strengthening the cryptographic foundation through even greater complexity and entropy.

Author Contributions: Conceptualization, W.F., Z.Q. and Z.Z.; methodology, W.F., X.Z. and H.W.; software, W.F. and Z.T.; validation, Y.C., B.C. and H.W.; formal analysis, X.Z., Y.C. and B.C.; writing—original draft preparation, W.F., Z.T. and Z.Q.; writing—review and editing, Z.T., X.Z., Z.Q., Z.Z. and K.Q.; project administration, W.F., Z.T. and Z.Q.; funding acquisition, W.F., K.Q. and H.W. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Guangdong Basic and Applied Basic Research Foundation (Grant No. 2023A1515011717), the Special Projects for Key Fields of the Education Department of

Guangdong Province (Grant No. 2024ZDZX1048), the Scientific Research Foundation of Hunan Provincial Education Department (Grant No. 23B0638), and the Key Project of the Panzhihua Municipal Key Laboratory of “Internet+” Big Data and Artificial Intelligence (Grant No. 25HLW0003).

Data Availability Statement: The data presented in this study are openly available in [USC-SIPI] at <https://sipi.usc.edu/database/>, accessed on 13 October 2025].

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Toktas, F.; Erkan, U.; Yetgin, Z. Cross-channel color image encryption through 2D hyperchaotic hybrid map of optimization test functions. *Expert Syst. Appl.* **2024**, *249*, 123583. [\[CrossRef\]](#)
2. Zhou, A.; Yang, C.; Yi, C.; Fan, H. New μ -Synchronization Criteria for Nonlinear Drive–Response Complex Networks with Uncertain Inner Couplings and Variable Delays of Unknown Bounds. *Axioms* **2025**, *14*, 161. [\[CrossRef\]](#)
3. Feng, W.; Zhang, K.; Zhang, J.; Zhao, X.; Chen, Y.; Cai, B.; Zhu, Z.; Wen, H.; Ye, C. Integrating Fractional-Order Hopfield Neural Network with Differentiated Encryption: Achieving High-Performance Privacy Protection for Medical Images. *Fractal Fract.* **2025**, *9*, 426. [\[CrossRef\]](#)
4. Rasouli, M.; Zare, A.; Yaghoubi, H.; Alizadehsani, R. Designing a Secure Mechanism for Image Transferring System Based on Uncertain Fractional Order Chaotic Systems and NLFPID Sliding Mode Controller. *Axioms* **2023**, *12*, 828. [\[CrossRef\]](#)
5. Lai, Q.; Hua, H. Secure medical image encryption scheme for Healthcare IoT using novel hyperchaotic map and DNA cubes. *Expert Syst. Appl.* **2025**, *264*, 125854. [\[CrossRef\]](#)
6. Romero-Arellano, A.; Moya-Albor, E.; Brieva, J.; Cruz-Aceves, I.; Avina-Cervantes, J.G.; Hernandez-Gonzalez, M.A.; Lopez-Montero, L.M. Image Encryption and Decryption System through a Hybrid Approach Using the Jigsaw Transform and Langton’s Ant Applied to Retinal Fundus Images. *Axioms* **2021**, *10*, 215. [\[CrossRef\]](#)
7. Yu, F.; Zhang, S.; Su, D.; Wu, Y.; Gracia, Y.M.; Yin, H. Dynamic analysis and implementation of FPGA for a new 4D fractional-order memristive Hopfield neural network. *Fractal Fract.* **2025**, *9*, 115. [\[CrossRef\]](#)
8. Li, Y.; Li, C.; Li, Y.; Moroz, I.; Yang, Y. A joint image encryption based on a memristive Rulkov neuron with controllable multistability and compressive sensing. *Chaos Solitons Fractals* **2024**, *182*, 114800. [\[CrossRef\]](#)
9. Yu, F.; Gracia, Y.M.; Guo, R.; Ying, Z.; Xu, J.; Yao, W.; Jin, J.; Lin, H. Dynamic Analysis and Application of 6D Multistable Memristive Chaotic System with Wide Range of Hyperchaotic States. *Axioms* **2025**, *14*, 638. [\[CrossRef\]](#)
10. Liu, L.; Wang, J. A cluster of 1D quadratic chaotic map and its applications in image encryption. *Math. Comput. Simul.* **2023**, *204*, 89–114. [\[CrossRef\]](#)
11. Al-Barakati, A.A.; Mesdoui, F.; Bekiros, S.; Kaçar, S.; Jahanshahi, H. A variable-order fractional memristor neural network: Secure image encryption and synchronization via a smooth and robust control approach. *Chaos Solitons Fractals* **2024**, *186*, 115135. [\[CrossRef\]](#)
12. Jackson, J.; Perumal, R. A robust image encryption technique based on an improved fractional order chaotic map. *Nonlinear Dyn.* **2025**, *113*, 7277–7296. [\[CrossRef\]](#)
13. An, D.; Hao, D.; Zhao, R.; Zhang, S.; Lu, J.; Zhang, Y. Visually semantic-preserving and people-oriented color image encryption based on cross-plane thumbnail preservation. *Expert Syst. Appl.* **2023**, *233*, 120931. [\[CrossRef\]](#)
14. Deng, Q.; Wang, C.; Yang, G.; Luo, D. Discrete Memristive Delay Feedback Rulkov Neuron Model: Chaotic Dynamics, Hardware Implementation, and Application in Secure Communication. *IEEE Internet Things J.* **2025**, *12*, 25559–25567. [\[CrossRef\]](#)
15. Ma, X.; Wang, Z.; Wang, C. An image encryption algorithm based on tabu search and hyperchaos. *Int. J. Bifurc. Chaos* **2024**, *34*, 2450170. [\[CrossRef\]](#)
16. Deng, Q.; Wang, C.; Sun, Y.; Deng, Z.; Yang, G. Memristive Tabu Learning Neuron Generated Multi-Wing Attractor with FPGA Implementation and Application in Encryption. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2025**, *72*, 300–311. [\[CrossRef\]](#)
17. Jin, B.; Fan, L.; Zhang, B.; Lei, R.; Liu, L. Image encryption hiding algorithm based on digital time-varying delay chaos model and compression sensing technique. *iScience* **2024**, *27*, 110717. [\[CrossRef\]](#)
18. Deng, Q.; Wang, C.; Sun, Y.; Yang, G. Discrete Memristive Conservative Chaotic Map: Dynamics, Hardware Implementation, and Application in Secure Communication. *IEEE Trans. Cybern.* **2025**, *55*, 3926–3934. [\[CrossRef\]](#)
19. Tang, J.; Zhang, Z.; Huang, T. Two-Dimensional Cosine–Sine Interleaved Chaotic System for Secure Communication. *IEEE Trans. Circuits Syst. II Express Briefs* **2024**, *71*, 2479–2483. [\[CrossRef\]](#)
20. Lai, Q.; Liu, Y. A family of image encryption schemes based on hyperchaotic system and cellular automata neighborhood. *Sci. China Technol. Sci.* **2025**, *68*, 1320401. [\[CrossRef\]](#)
21. Sajid, M.; Chaudhary, H.; Kaushik, S. Chaos Controllability in Non-Identical Complex Fractional Order Chaotic Systems via Active Complex Synchronization Technique. *Axioms* **2023**, *12*, 530. [\[CrossRef\]](#)

22. Li, Y.M.; Deng, Y.; Jiang, M.; Wei, D. Fast Encryption Algorithm Based on Chaotic System and Cyclic Shift in Integer Wavelet Domain. *Fractal Fract.* **2024**, *8*, 75. [\[CrossRef\]](#)
23. Chen, Y.; Huang, H.; Tang, C.; Wei, W. A novel adaptive image privacy protection method based on Latin square. *Nonlinear Dyn.* **2024**, *112*, 10485–10508. [\[CrossRef\]](#)
24. Fedoseev, P.; Pesterev, D.; Rozhkov, V.; Rybin, V.; Butusov, D. Chaotic Encryption Algorithm Based on Gingerbreadman Map with Adaptive Symmetry. *Chaos Theory Appl.* **2024**, *7*, 31–41. [\[CrossRef\]](#)
25. Hosbas, M.Z.; Emin, B.; Kaçar, F. True random number generator design with a fractional order spott b chaotic system. *ADBA Comput. Sci.* **2025**, *2*, 50–55. [\[CrossRef\]](#)
26. Kaya, Y.; Aydin, Z.G. A Chaos-Based Encryption Scheme for Secure Medical X-ray Images. *Comput. Electron. Med.* **2025**, *2*, 53–59. [\[CrossRef\]](#)
27. Dhall, S.; Yadav, K. Cryptanalysis of substitution-permutation network based image encryption schemes: A systematic review. *Nonlinear Dyn.* **2024**, *112*, 14719–14744. [\[CrossRef\]](#)
28. Zhang, C.; Chen, J.; Chen, D. Cryptanalysis of an Image Encryption Algorithm Based on a 2D Hyperchaotic Map. *Entropy* **2022**, *24*, 1551. [\[CrossRef\]](#) [\[PubMed\]](#)
29. You, K.; Chen, P.; Li, C. Cryptanalyzing an Image Encryption Algorithm Underpinned by 3D-BCNN. *IEEE Multimed.* **2024**, *31*, 17–24. [\[CrossRef\]](#)
30. Chen, L.; Li, C.; Li, C. Security Measurement of a Medical Image Communication Scheme based on Chaos and DNA. *J. Vis. Commun. Image Represent.* **2022**, *83*, 103424. [\[CrossRef\]](#)
31. Feng, W.; Qin, Z.; Zhang, J.; Ahmad, M. Cryptanalysis and Improvement of the Image Encryption Scheme Based on Feistel Network and Dynamic DNA Encoding. *IEEE Access* **2021**, *9*, 145459–145470. [\[CrossRef\]](#)
32. Feng, W.; He, Y.; Li, H.; Li, C. Cryptanalysis and improvement of the image encryption scheme based on 2D logistic-adjusted-sine map. *IEEE Access* **2019**, *7*, 12584–12597. [\[CrossRef\]](#)
33. Tuli, R.; Soneji, H.N.; Churi, P. PixAdapt: A novel approach to adaptive image encryption. *Chaos Solitons Fractals* **2022**, *164*, 112628. [\[CrossRef\]](#)
34. Wang, X.; Liu, H. Cross-plane multi-image encryption using chaos and blurred pixels. *Chaos Solitons Fractals* **2022**, *164*, 112586. [\[CrossRef\]](#)
35. Sun, J. 2D-SCMCI Hyperchaotic Map for Image Encryption Algorithm. *IEEE Access* **2021**, *9*, 59313–59327. [\[CrossRef\]](#)
36. Nan, S.; Feng, X.; Wu, Y.; Zhang, H. Remote sensing image compression and encryption based on block compressive sensing and 2D-LCCCM. *Nonlinear Dyn.* **2022**, *108*, 2705–2729. [\[CrossRef\]](#)
37. Zhu, L.; Jiang, D.; Ni, J.; Wang, X.; Rong, X.; Ahmad, M.; Chen, Y. A stable meaningful image encryption scheme using the newly-designed 2D discrete fractional-order chaotic map and Bayesian compressive sensing. *Signal Process.* **2022**, *195*, 108489. [\[CrossRef\]](#)
38. Hua, Z.; Chen, Y.; Bao, H.; Zhou, Y. Two-Dimensional Parametric Polynomial Chaotic System. *IEEE Trans. Syst. Man, Cybern. Syst.* **2022**, *52*, 4402–4414. [\[CrossRef\]](#)
39. Lai, Q.; Hu, G.; Erkan, U.; Toktas, A. A novel pixel-split image encryption scheme based on 2D Salomon map. *Expert Syst. Appl.* **2023**, *213*, 118845. [\[CrossRef\]](#)
40. Hua, Z.; Zhu, Z.; Yi, S.; Zhang, Z.; Huang, H. Cross-plane colour image encryption using a two-dimensional logistic tent modular map. *Inf. Sci.* **2021**, *546*, 1063–1083. [\[CrossRef\]](#)
41. Li, B.; Sun, K.; Wang, H.; Liu, W. An internal perturbation method to counteract the dynamical degradation of digital chaotic maps and its application. *Nonlinear Dyn.* **2024**, *112*, 9603–9615. [\[CrossRef\]](#)
42. El-Den, B.M.; Aldosary, S.; Khaled, H.; Hassan, T.M.; Raslan, W. Leveraging Finite-Precision Errors in Chaotic Systems for Enhanced Image Encryption. *IEEE Access* **2024**, *12*, 176057–176069. [\[CrossRef\]](#)
43. Nardo, L.G.; Nepomuceno, E.G.; Arias-Garcia, J.; Butusov, D.N. Image encryption using finite-precision error. *Chaos Solitons Fractals* **2019**, *123*, 69–78. [\[CrossRef\]](#)
44. Dinu, A.; Frunzete, M. The Lorenz chaotic system, statistical independence and sampling frequency. In Proceedings of the 2021 International Symposium on Signals, Circuits and Systems (ISSCS), Iasi, Romania, 15–16 July 2021; pp. 1–4. [\[CrossRef\]](#)
45. Macovei, C.; Vaduva, A.; Vlad, A.; Zamfir, M. A mean test on the autocorrelation function of a chaotic signal aiming to support the statistical independence sampling distance. In Proceedings of the 2019 International Symposium on Signals, Circuits and Systems (ISSCS), Iasi, Romania, 11–12 July 2019; pp. 1–4. [\[CrossRef\]](#)
46. Karimov, T.; Mikhailov, A.; Rybin, V.; Sheptunova, V.; Babkin, I.; Butusov, D. Attack-Resistant Chaotic Communication System in Non-ideal Physical Channel. *Chaos Fractals* **2025**, *2*, 28–37. [\[CrossRef\]](#)
47. Özkaynak, F. Brief review on application of nonlinear dynamics in image encryption. *Nonlinear Dyn.* **2018**, *92*, 305–313. [\[CrossRef\]](#)
48. Liu, H.; Teng, L.; Zhang, Y.; Si, R.; Liu, P. Mutil-medical image encryption by a new spatiotemporal chaos model and DNA new computing for information security. *Expert Systems with Applications* **2024**, *235*, 121090. [\[CrossRef\]](#)

49. Erkan, U.; Toktas, A.; Lai, Q. Design of two dimensional hyperchaotic system through optimization benchmark function. *Chaos Solitons Fractals* **2023**, *167*, 113032. [\[CrossRef\]](#)
50. Grassberger, P.; Procaccia, I. Estimation of the Kolmogorov entropy from a chaotic signal. *Phys. Rev. A* **1983**, *28*, 2591. [\[CrossRef\]](#)
51. SaberiKamarposhti, M.; Ghorbani, A.; Yadollahi, M. A comprehensive survey on image encryption: Taxonomy, challenges, and future directions. *Chaos Solitons Fractals* **2024**, *178*, 114361. [\[CrossRef\]](#)
52. Yu, F.; He, S.; Yao, W.; Cai, S.; Xu, Q. Bursting Firings in Memristive Hopfield Neural Network with Image Encryption and Hardware Implementation. *IEEE Trans. -Comput.-Aided Des. Integr. Circuits Syst.* **2025**, *44*, 4564–4576. [\[CrossRef\]](#)
53. Verma, V.; Kumar, S. Quantum image encryption algorithm based on 3D-BNM chaotic map. *Nonlinear Dyn.* **2025**, *113*, 3829–3855. [\[CrossRef\]](#)
54. Alvarez, G.; Li, S. Some basic cryptographic requirements for chaos-based cryptosystems. *Int. J. Bifurc. Chaos* **2006**, *16*, 2129–2151. [\[CrossRef\]](#)
55. Yu, F.; Wang, X.; Guo, R.; Ying, Z.; Cai, S.; Jin, J. Dynamical analysis, hardware implementation, and image encryption application of new 4D discrete hyperchaotic maps based on parallel and cascade memristors. *Integration* **2025**, *104*, 102475. [\[CrossRef\]](#)
56. Li, H.; Li, T.; Feng, W.; Zhang, J.; Zhang, J.; Gan, L.; Li, C. A novel image encryption scheme based on non-adjacent parallelable permutation and dynamic DNA-level two-way diffusion. *J. Inf. Secur. Appl.* **2021**, *61*, 102844. [\[CrossRef\]](#)
57. Zhang, B.; Liu, L. Chaos-Based Image Encryption: Review, Application, and Challenges. *Mathematics* **2023**, *11*, 2585. [\[CrossRef\]](#)
58. Yu, F.; He, T.; He, S.; Tan, B.; Shi, C.; Lin, H. Influence of Memristive Activated Gradient on Chaotic Dynamics in Discrete Neural Networks. *Int. J. Bifurc. Chaos* **2025**, *35*, 2550146. [\[CrossRef\]](#)
59. He, S.; Yu, F.; Guo, R.; Zheng, M.; Tang, T.; Jin, J.; Wang, C. Dynamic Analysis and FPGA Implementation of a Fractional-Order Memristive Hopfield Neural Network with Hidden Chaotic Dual-Wing Attractors. *Fractal Fract.* **2025**, *9*, 561. [\[CrossRef\]](#)
60. Yu, F.; Kong, X.; Yao, W.; Zhang, J.; Cai, S.; Lin, H.; Jin, J. Dynamics analysis, synchronization and FPGA implementation of multiscroll Hopfield neural networks with non-polynomial memristor. *Chaos Solitons Fractals* **2024**, *179*, 114440. [\[CrossRef\]](#)
61. Li, C.; Shen, X.; Liu, S. Cryptanalyzing an Image Encryption Algorithm Underpinned by 2-D Lag-Complex Logistic Map. *IEEE Multimed.* **2024**, *31*, 99–109. [\[CrossRef\]](#)
62. Wu, Y.; Noonan, J.P.; Aghaian, S. NPCR and UACI randomness tests for image encryption. *Cyber J. Multidiscip. J. Sci. Technol. J. Sel. Areas Telecommun. (JSAT)* **2011**, *1*, 31–38.
63. Zarei Zefreh, E. PSDCLS: Parallel simultaneous diffusion–confusion image cryptosystem based on Latin square. *J. Inf. Secur. Appl.* **2024**, *83*, 103785. [\[CrossRef\]](#)
64. Qian, K.; Xiao, Y.; Wei, Y.; Liu, D.; Wang, Q.; Feng, W. A robust memristor-enhanced polynomial hyper-chaotic map and its multi-channel image encryption application. *Micromachines* **2023**, *14*, 2090. [\[CrossRef\]](#) [\[PubMed\]](#)
65. Li, H.; Yu, S.; Feng, W.; Chen, Y.; Zhang, J.; Qin, Z.; Zhu, Z.; Wozniak, M. Exploiting Dynamic Vector-Level Operations and a 2D-Enhanced Logistic Modular Map for Efficient Chaotic Image Encryption. *Entropy* **2023**, *25*, 1147. [\[CrossRef\]](#)
66. Feng, W.; Zhao, X.; Zhang, J.; Qin, Z.; Zhang, J.; He, Y. Image Encryption Algorithm Based on Plane-Level Image Filtering and Discrete Logarithmic Transform. *Mathematics* **2022**, *10*, 2751. [\[CrossRef\]](#)

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.