AIMS Mathematics, 11(3): 8242–8270.
DOI:10.3934/math.2026339
Received: 01 February 2026
Revised: 09 March 2026
Accepted: 18 March 2026
Published: 27 March 2026

https://www.aimspress.com/journal/Math

Research article

A two-dimensional hyperchaotic discrete dynamical system and its application

Min Zhao*

School of Mathematics, Nanjing University, Nanjing 210093, Jiangsu, China

* **Correspondence:** Email: zhaominmmmmm@163.com.

Abstract: This paper develops a two-dimensional hyperchaotic discrete dynamical system (2D-HDDS) by extending the exponential-Chebyshev mechanism to a two-dimensional setting through a structured nonlinear feedback coupling. The resulting system combines the stretching effect of exponential dynamics with the folding behavior of Chebyshev mappings. Bifurcation diagrams and Lyapunov-exponent spectra indicate that 2D-HDDS exhibits a comparatively wide hyperchaotic parameter region and high dynamical complexity. Based on the generated keystream, we further construct an image-encryption scheme that integrates dual permutations, a key-dependent dynamic S-box, index-coupled forward and backward nonlinear diffusion, and a lightweight avalanche booster to enhance the propagation of plaintext perturbations. Experimental results show high key sensitivity and strong plaintext sensitivity, with the number of pixels change rate (NPCR) and the unified average changing intensity (UACI) values close to the ideal levels predicted by the standard random-like cipher-image model, while also demonstrating good resistance to statistical and differential attacks.

Keywords: hyperchaotic system; Lyapunov exponent; image encryption; S-box; security analysis
Mathematics Subject Classification: 37D45, 37M10, 68P25, 94A60

1. Introduction

The rapid growth of digital media and networked communication has created an increasing need for image-encryption methods that are not only efficient in implementation but also sufficiently robust for practical security applications. Unlike textual data, digital images usually contain substantial spatial redundancy and strong inter-pixel correlations, which make many conventional text-oriented encryption pipelines less suitable for image and video data in terms of throughput and implementation efficiency [28, 41]. Among the many approaches explored for multimedia security, chaos-based cryptography has received continuing attention because chaotic dynamics possess several features that are potentially useful for confusion and diffusion, including sensitivity to initial conditions and control

parameters, as well as the divergence of nearby trajectories [15]. These characteristics make nonlinear dynamical systems a natural source of pseudorandomness in image-encryption design.

Early chaos-based image-encryption schemes were mainly built from low-dimensional maps because of their simple mathematical forms and ease of implementation. In particular, classical one-dimensional maps such as the logistic map, tent map, and Chebyshev polynomial map were widely used as keystream generators in image ciphers [6, 11]. Matthews first demonstrated the feasibility of using one-dimensional chaotic maps for pseudorandom sequence generation in data encryption [21], and Fridrich later introduced the permutation-diffusion framework that has since become a common structure in chaos-based image encryption [11]. Subsequent studies extended this line of work by combining chaotic keystreams with other design mechanisms, including DNA/RNA-inspired operations [10, 37, 42], cellular automata [8, 26], and compressive sensing [13, 43, 45].

At the same time, existing studies have also pointed out several limitations of image-encryption schemes based solely on classical one-dimensional chaotic maps, including relatively limited key space, narrow chaotic parameter regions, and possible vulnerability to phase-space reconstruction or differential attacks [17, 18, 33]. To address these issues, more recent work has increasingly turned to high-dimensional or hyperchaotic systems with richer dynamical behavior [14, 30, 34, 36], including coupled map lattices [14], cross-modulated sine-cosine systems [16], and multi-attractor hyperchaotic flows [32]. However, for practical digital implementation, many existing two-dimensional chaotic maps may still suffer from finite-precision effects such as dynamical degradation and nonuniform invariant distributions, which can influence the statistical quality of the generated keystream and, in turn, affect encryption performance [7]. From an algorithmic viewpoint, permutation-diffusion structures with only a single permutation stage and weakly coupled local diffusion may also leave room for effective chosen-plaintext or differential cryptanalysis under suitable settings [19, 44].

Motivated by these considerations and inspired by the one-dimensional exponential-Chebyshev system in [20], this paper develops a two-dimensional hyperchaotic discrete dynamical system (2D-HDDS) together with a corresponding image-encryption algorithm. The objective is not to claim a fundamentally new dynamical principle, but to construct a structured two-dimensional extension of the exponential-Chebyshev mechanism through nonlinear feedback coupling and to examine whether such a construction can provide a numerically broader hyperchaotic region and a more satisfactory invariant distribution in practical digital settings. Based on the generated keystream, we then design a byte-level image-encryption framework intended to improve plaintext diffusion and to enhance resistance to common statistical and differential analyses.

The main contributions of this work can be summarized as follows:

- **A two-dimensional extension of the exponential-Chebyshev mechanism.** We extend the exponential-Chebyshev construction from one dimension to two dimensions by introducing nonlinear feedback coupling between two state variables [20]. Numerical investigations based on bifurcation diagrams and Lyapunov-exponent spectra suggest that the resulting 2D-HDDS admits a relatively broad hyperchaotic parameter region and exhibits a reasonably uniform invariant distribution when compared with several representative two-dimensional chaotic systems reported in the recent literature [30, 34, 36].

- **A multi-stage byte-wise permutation-diffusion design driven by 2D-HDDS.** Using the keystream generated by 2D-HDDS, we construct an image-encryption scheme that combines

two chaos-driven Fisher–Yates permutations, an index-coupled forward/backward nonlinear diffusion process, and a lightweight two-pass avalanche-enhancement module. In addition, a key-dependent dynamic S-box, together with odd-multiplicative mixing and byte-wise rotations over $\mathbb{Z}_{256}$, is incorporated to increase byte-level nonlinearity while keeping the implementation relatively simple.

- **Security and performance evaluation under practical testing settings.** Experimental results and supplementary analyses indicate that the proposed scheme has a large key space, high key sensitivity, and good plaintext sensitivity, and that it performs well in the reported tests concerning statistical, differential, and implementation-related behavior [19, 44].

The remainder of this paper is organized as follows. We first present the proposed 2D-HDDS and its dynamical analysis, and then describe the encryption and decryption procedures in detail. Next, security and performance evaluations are reported. Finally, concluding remarks are given.

2. Two-dimensional hyperchaotic discrete dynamical system

This section introduces the proposed 2D-HDDS. Before introducing the proposed model, we recall the standard definition of hyperchaos for discrete dynamical systems.

Definition 2.1 (Hyperchaos [27])**.** Let $\{\lambda_i\}_{i=1,2}$ denote the Lyapunov exponents of a two-dimensional discrete dynamical system. The system is classified as *chaotic* if at least one of its Lyapunov exponents is positive and as *hyperchaotic* if both of its Lyapunov exponents are positive.

Accordingly, the proposed system will be numerically examined through its Lyapunov exponent spectrum to identify parameter regions where two positive Lyapunov exponents occur.

Our aim is to construct a compact discrete-time generator with a wide hyperchaotic parameter regime and high orbit complexity, which can serve as a reliable keystream source for the encryption scheme developed in Section 4.

The well-known Chebyshev map is defined as

$$x_{n+1} = \cos\left(a \cdot \arccos x_n\right), \quad x_n \in [-1, 1], \quad n \in \mathbb{Z}_+ \tag{2.1}$$

and becomes chaotic for $a > 1$, demonstrating superior ergodicity and larger Lyapunov exponents compared to simpler maps like logistic. However, one-dimensional systems suffer from a limited parameter space and low algorithmic complexity, making them vulnerable to phase-space reconstruction, return-map analysis, and differential cryptanalysis [33].

To overcome these limitations, we construct a new two-dimensional coupled map that combines exponential stretching with trigonometric folding. The exponential term amplifies small perturbations, whereas the Chebyshev-type cosine mechanism confines the state to a bounded interval while enhancing mixing. More specifically, our system is obtained by extending the one-dimensional exponential-Chebyshev prototype in [20] to a two-variable coupled form through cross-modulation between the two state variables. Here, we introduce this coupled system as the proposed model, rather than as a reformulation of any benchmark system considered later for comparison. The resulting coupled discrete system is given by

$$x_{n+1} = 1 - 2\left[\cos\Big(\arccos(x_n)\, \exp\Big((|a| + 1)\,[\arccos(y_n)]^2\Big)\Big)\right]^2, \tag{2.2}$$

$$y_{n+1} = 1 - 2\left[\cos\Big(\arccos(y_n)\,\exp\Big((|b|+1)\,[\arccos(x_n)]^2\Big)\Big)\right]^2, \tag{2.3}$$

which can be simplified by using the trigonometric identity $1 - 2\cos^2\theta = -\cos(2\theta)$ as

$$x_{n+1} = -\cos\Big(2\,\arccos(x_n)\,\exp\Big((|a|+1)\,[\arccos(y_n)]^2\Big)\Big), \tag{2.4}$$

$$y_{n+1} = -\cos\Big(2\,\arccos(y_n)\,\exp\Big((|b|+1)\,[\arccos(x_n)]^2\Big)\Big). \tag{2.5}$$

Here, $a, b \in \mathbb{R}$ are control parameters, and the state variables satisfy $(x_n, y_n) \in [-1, 1]^2$. The absolute-value reparameterization, i.e., $|a|$ and $|b|$, makes the map invariant to the sign of the parameters, so that a and $-a$ (resp. b and $-b$) generate identical dynamics. The coupling is realized through the squared $\arccos(\cdot)$ terms embedded in the exponential modulation, which introduces strong nonlinear feedback between the two dimensions.

Remark 2.1. The proposed map differs from many existing cross-modulated constructions in that the coupling is introduced in the angular variable. Consequently, each state variable modulates the effective nonlinear expansion intensity of the other in a state-dependent manner, while the cosine structure preserves the folding mechanism characteristic of Chebyshev-type dynamics.

In the following section, we evaluate the chaotic performance of 2D-HDDS using bifurcation diagrams and Lyapunov-exponent spectra and benchmark its behavior against some representative state-of-the-art two-dimensional chaotic maps.

3. Chaotic performance of 2D-HDDS

We examine the dynamical behavior of 2D-HDDS via bifurcation diagrams and Lyapunov-exponent spectra (see Section 3.4). Such bifurcation-based and multi-parameter explorations are standard in discrete-time nonlinear dynamics across applications [23–25]. We then compare the resulting profiles with those of two recent high-performance two-dimensional maps: the two-dimensional log-logistic-sine chaotic map (2D-LLSCM) [36] and the two-dimensional cross-mode hyperchaotic map based on logistic and sine maps (2D-CLSS) hyperchaotic map [30]. Both references fall into the recent class of transcendental-function-enhanced constructions, where logarithmic/trigonometric nonlinearities and cross-coupling are employed to widen chaotic regimes and improve orbit complexity-properties that are directly relevant for keystream generation in encryption.

3.1. Chaotic maps for comparison

2D-LLSCM. As a benchmark for comparative analysis, we consider the 2D-LLSCM from [36]. This map is included only for comparison with the proposed system in (2.2)–(2.5). Following [36], the 2D-LLSCM is defined by

$$\begin{cases} x_{n+1} = \sin\left(\pi\left(a\log_2(1+x_n)\left(1 - \dfrac{\log_2(1+y_n)}{x_n^3}\right)\right)\right), \\ y_{n+1} = \sin\left(\pi\left(a\log_2(1+y_n)\left(1 - \dfrac{\log_2(1+x_{n+1})}{y_n^3}\right)\right)\right), \end{cases} \tag{3.1}$$

where $a \in (0, +\infty)$ and $(x_n, y_n) \in (0, 1)^2$ [36]. For digital applications such as image encryption, [36] applies a modulo-1 reduction, yielding

$$\begin{cases} x_{n+1} = \sin\left(\pi\left(a \log_2(1 + x_n)\left(1 - \dfrac{\log_2(1 + y_n)}{x_n^3}\right)\right)\right) \bmod 1, \\ y_{n+1} = \sin\left(\pi\left(a \log_2(1 + y_n)\left(1 - \dfrac{\log_2(1 + x_{n+1})}{y_n^3}\right)\right)\right) \bmod 1. \end{cases} \tag{3.2}$$

2D-CLSS. The 2D-CLSS hyperchaotic map in [30] uses a cross-coupled update that blends a logistic-type term with sine transformations. An equivalent form is

$$\begin{cases} x_{n+1} = \sin(\pi(p\, y_n(1 - y_n))), \\ y_{n+1} = \sin(\pi(x_n + y_n)), \end{cases} \tag{3.3}$$

where p is the control parameter [30]. In (3.3), the update of x is driven by a logistic-type nonlinearity evaluated at y_n, whereas the update of y applies a sine map to the coupled sum $(x_n + y_n)$.

3.2. Evaluation strategy and experimental settings

Bifurcation diagrams summarize how long-run orbit statistics change as parameters vary, whereas Lyapunov exponents quantify the mean exponential separation rate of nearby trajectories. In the cryptographic setting, desirable behavior typically includes a wide connected chaotic regime with few periodic windows and strong orbit dispersion, which is conducive to enlarging the effective key space and reducing exploitable structure in the generated keystream [1, 15].

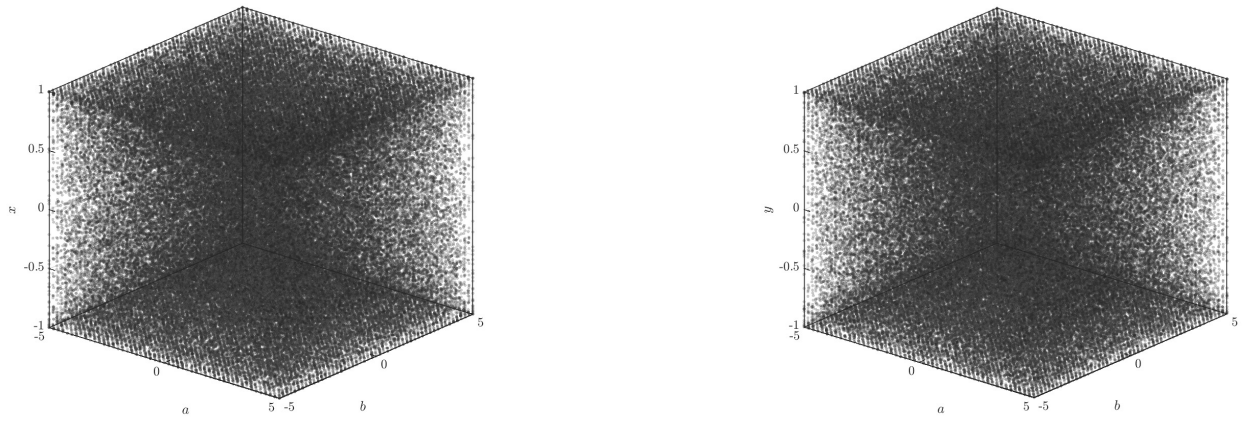
A practical complication is that 2D-HDDS depends on two control parameters (a, b), while 2D-LLSCM and 2D-CLSS each use a single parameter. We therefore report results under two complementary protocols:

- **Two-parameter exploration (2D-HDDS only):** We sweep $(a, b) \in [-5, 5] \times [-5, 5]$ to characterize the global coverage and continuity of chaotic behavior over the full parameter plane.
- **Unified one-parameter comparison (all systems):** We restrict 2D-HDDS to the diagonal slice $a = b = \mu$ and use μ as a common control parameter to align the horizontal axes across systems. For the baselines, we set $a = \mu$ in (3.2) and $p = \mu$ in (3.3).

For the one-parameter bifurcation diagrams, we scan $\mu \in \{-10, -9.95, \ldots, 10.0\}$ with initial conditions $x_0 = 0.4$ and $y_0 = 0.5$. For each μ, we discard the first $N_{\text{tr}} = 500$ iterates as transients and record the subsequent samples for plotting.

3.3. Bifurcation analysis

Two-parameter coverage of 2D-HDDS. The following Figure 1 summarizes the asymptotic behavior of 2D-HDDS under a two-parameter sweep.



(a) 3D bifurcation diagram for the x component.

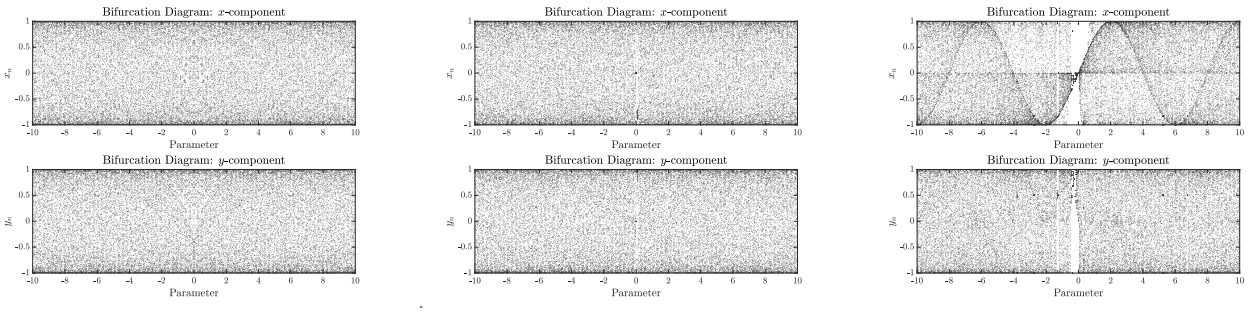
(b) 3D bifurcation diagram for the y component.

Figure 1. Global (two-parameter) 3D bifurcation diagrams of 2D-HDDS over $(a, b) \in [-5, 5]\times[-5, 5]$. After discarding transients, we record the long-run iterates and visualize the resulting point clouds in the (a, b, x) and (a, b, y) coordinates over $(a, b) \in [-5, 5] \times [-5, 5]$.

Across most of the sampled plane, the attractor sections remain broadly distributed with no prominent periodic layers or low-dimensional bands. From the standpoint of keystream generation, such continuity of aperiodic behavior over parameters is desirable, as it reduces the risk that small parameter drifts or coarse parameter choices place the system into short-period windows.

Unified one-parameter comparison. In each panel of the above figure, the two state variables (x_n, y_n) are overlaid, and within the scanned range $\mu \in [-10, 10]$, 2D-HDDS exhibits sustained aperiodic dispersion, whereas the baselines display visibly narrower chaotic sub-intervals interspersed with more structured regions.

To facilitate a like-for-like comparison with 2D-LLSCM and 2D-CLSS, we further restrict 2D-HDDS to the diagonal slice $a = b = \mu$ and plot bifurcation diagrams versus the common control parameter μ. The Figure 2 below reports the resulting diagrams.



(a) 2D-HDDS ($a = b = \mu$).

(b) 2D-LLSCM ($a = \mu$).

(c) 2D-CLSS ($p = \mu$).

Figure 2. Unified-parameter bifurcation diagrams for three 2D chaotic maps. A single control parameter μ is used for a consistent horizontal axis: $a = b = \mu$ for 2D-HDDS, $a = \mu$ for 2D-LLSCM, and $p = \mu$ for 2D-CLSS.

3.4. Lyapunov exponents

Consider a two-dimensional discrete-time system

$$\mathbf{x}_{n+1} = \mathbf{F}(\mathbf{x}_n; \boldsymbol{\mu}), \qquad \mathbf{x}_n \in \mathbb{R}^2, \tag{3.4}$$

where $\mathbf{F}$ is smooth and $\boldsymbol{\mu}$ denotes the control parameter(s). Let $\mathbf{J}_n = D\mathbf{F}(\mathbf{x}_n)$ be the Jacobian evaluated along an orbit $\{\mathbf{x}_n\}_{n\geq 0}$ equivalently via the singular values of the Jacobian cocycle [4, 5]:

$$\lambda_i = \lim_{N\to\infty} \frac{1}{N} \ln \sigma_i \left(\prod_{n=0}^{N-1} \mathbf{J}_n \right), \qquad i = 1, 2, \tag{3.5}$$

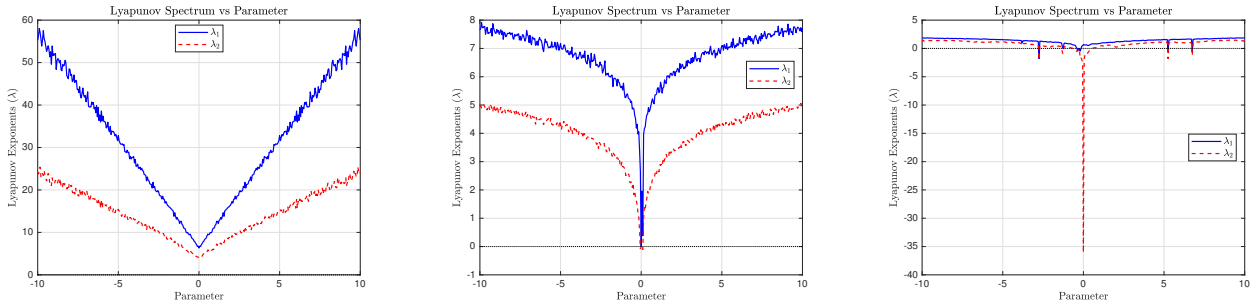
where $\sigma_1 \geq \sigma_2 > 0$ denotes the singular values. In practice, we estimate (λ_1, λ_2) over a finite horizon by propagating an orthonormal basis in the tangent space and applying QR (or Gram–Schmidt) re-orthonormalization while averaging the logarithms of the instantaneous stretching factors [4, 29, 38].

According to Definition 2.1, a bounded system is termed chaotic if $\lambda_1 > 0$. If $\lambda_2 > 0$ as well, then the system is hyperchaotic, indicating exponential divergence along at least two independent directions.

Lyapunov estimation settings. At each grid point (a, b), we compute the two largest Lyapunov exponents (λ_1, λ_2) using the standard Benettin–QR (Gram–Schmidt) method for discrete-time maps. We discard $N_{\text{tr}} = 500$ transient iterations and then iterate for $N = 3200$ steps. The tangent dynamics are propagated via the Jacobian $J_n = DF(x_n, y_n)$, and an orthonormalization (QR/Gram–Schmidt) step is performed every iteration. The exponents are estimated as

$$\lambda_k \approx \frac{1}{N} \sum_{n=1}^{N} \log r_{k,n}, \qquad k = 1, 2,$$

where $r_{k,n}$ denotes the diagonal factors from the QR (or the norms in Gram–Schmidt) at the n-th orthonormalization. We initialize $(x_0, y_0) \in (-1, 1)^2$ (e.g., $(-1 + \varepsilon, 1 - \varepsilon)^2$ with a tiny ε) to avoid exact hits at the endpoints where $\arccos'(\pm 1)$ is singular.



(a) 2D-HDDS ($a = b = \mu$). **(b)** 2D-LLSCM ($a = \mu$). **(c)** 2D-CLSS ($p = \mu$).

Figure 3. Unified-parameter Lyapunov-exponent spectra versus μ for the three maps in Figure 2. Positive λ_1 indicates chaos, while $\lambda_2 > 0$ corresponds to hyperchaos.

Under the unified one-parameter protocol, Figure 3 compares the Lyapunov exponents of 2D-HDDS, 2D-LLSCM, and 2D-CLSS on the same μ axis. Obviously, the trends are consistent with the bifurcation diagrams in Figure 2: 2D-HDDS sustains positive exponents over a wider portion of

$\mu \in [-10, 10]$, and the exponent magnitudes are generally larger over the chaotic segments, indicating faster average divergence of nearby trajectories.

Figure 4 presents the two-parameter Lyapunov-exponent spectra of 2D-HDDS over the parameter plane $(a, b) \in [-5, 5] \times [-5, 5]$, sampled on a uniform 201×201 grid with step size 0.05. For each parameter pair, the Lyapunov exponents are evaluated by the Benettin–Gram–Schmidt method after discarding 500 transient iterations, with at most 3200 subsequent iterations used for estimation. According to Definition 2.1, the figure shows a broad parameter region where both λ_1 and λ_2 are positive, which corresponds to hyperchaotic behavior. In particular, both exponents are positive at all sampled grid points in the reported scan domain, providing numerical evidence of widespread hyperchaotic behavior.

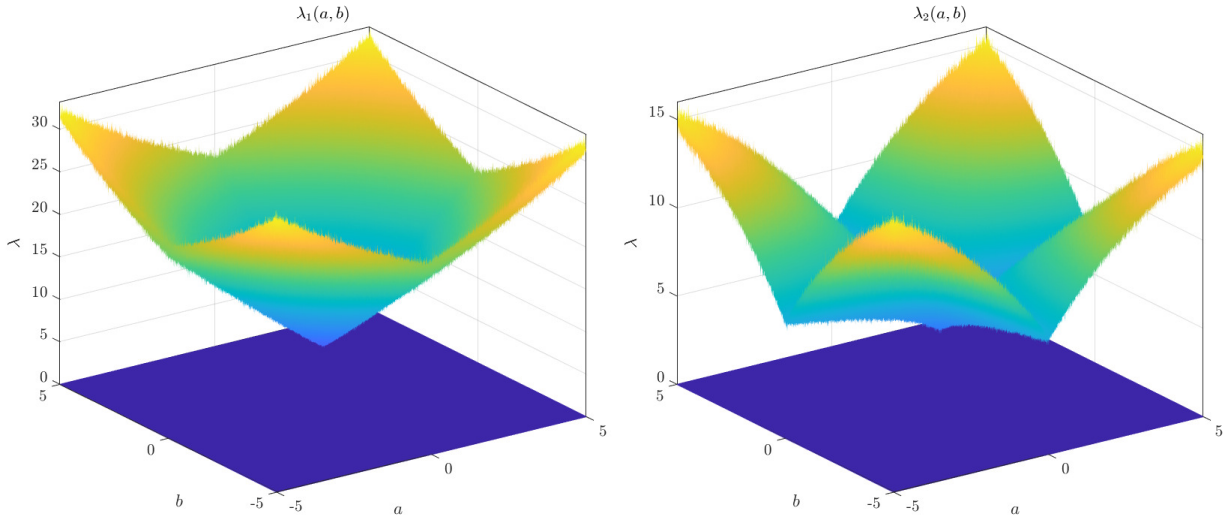


Figure 4. Lyapunov exponents of 2D-HDDS under the two-parameter evaluation. The two figures above report the two-parameter Lyapunov spectrum of 2D-HDDS and show broad regions with $\lambda_1 > 0$ and $\lambda_2 > 0$.

4. Index-coupled chaotic permutation and five-stage reversible diffusion with avalanche booster

This section presents the proposed image encryption algorithm driven by a key-dependent two-dimensional hyperchaotic generator. The scheme operates on 8-bit pixels in a byte-wise manner and is exactly invertible over $\mathbb{Z}_{256}$. In contrast to conventional permutation-diffusion frameworks, the proposed design integrates three key mechanisms: (i) two independent Fisher–Yates permutations to strengthen confusion, (ii) index-coupled nonlinear diffusion that injects long-range, keystream-controlled dependencies into both forward and backward directions, and (iii) a lightweight bidirectional avalanche booster that further amplifies plaintext perturbations toward the theoretical number of pixels change rate/unified average changing intensity (NPCR/UACI) benchmarks while maintaining lossless decryption.

4.1. Preliminaries and key schedule

4.1.1. Notation

Let the plaintext image be an 8-bit array $P \in \{0,\dots,255\}^{M\times N\times C}$ with $C \in \{1,3\}$. We vectorize P into $p \in \{0,\dots,255\}^{L}$, where $L = MNC$ by column-major linearization and fixed channel concatenation. The ciphertext vector is $e \in \{0,\dots,255\}^{L}$ and is reshaped back to the original image size.

All operations are byte-wise. Let $\oplus$ denote XOR on bytes. Let $x \boxplus y$ and $x \boxminus y$ denote addition and subtraction modulo 256, respectively. Define 8-bit rotations

$$\mathrm{ROTL}_8(x,r) = ((x \ll r)\ \mathrm{OR}\ (x \gg (8-r))) \bmod 256, \tag{4.1}$$

$$\mathrm{ROTR}_8(x,r) = ((x \gg r)\ \mathrm{OR}\ (x \ll (8-r))) \bmod 256, \tag{4.2}$$

where $r \in \{0,\dots,7\}$.

We also use a byte-wise multiplicative mixing

$$\mathrm{MUL}_8(x,m) = (x \cdot m) \bmod 256, \tag{4.3}$$

where m is constrained to be odd so that $\mathrm{MUL}_8(\cdot,m)$ is bijective over $\mathbb{Z}_{256}$ and admits a unique inverse multiplier m^{-1} such that $(m \cdot m^{-1}) \bmod 256 = 1$.

4.1.2. Keystream generation and deterministic partitioning

Given a secret key $K = [x_0, y_0, a, b]$, the chaotic map is iterated (after a fixed transient) and deterministically quantized into a stream of 32-bit unsigned words $q_i \in \{0,\dots,2^{32}-1\}$, $i = 1,2,\dots$. For an image length L, the implementation consumes a fixed number of words and partitions them in order as

$$\begin{aligned}\{q_i\} \Rightarrow\ & \underbrace{k^{(\pi_1)}_{1:L}}_{\text{perm-1 drivers}}\ \underbrace{k^{(\pi_2)}_{1:L}}_{\text{perm-2 drivers}}\ \underbrace{k^{(1)}_{1:L}}_{\text{core key}}\ \underbrace{k^{(2)}_{1:L}}_{\text{core key}}\ \underbrace{r^{(1)}_{1:L}}_{\text{rot}}\\ & \underbrace{k^{(3)}_{1:L}}_{\text{core key}}\ \underbrace{k^{(4)}_{1:L}}_{\text{core key}}\ \underbrace{r^{(2)}_{1:L}}_{\text{rot}}\ \underbrace{w^{(F)}_{1:L}}_{\text{fwd index-coupling \& packed params}}\\ & \underbrace{w^{(B)}_{1:L}}_{\text{bwd index-coupling \& packed params}}\ \underbrace{w^{(C)}_{1:L}}_{\text{booster packed params}}\ \underbrace{w^{(D)}_{1:L}}_{\text{booster packed params}}\\ & \underbrace{q^{(S)}_{1:256}}_{\text{S-box seed}}\ \underbrace{\mathrm{IV}_1,\mathrm{IV}_2,\mathrm{IV}_3,\mathrm{IV}_4}_{\text{init bytes}}.\end{aligned} \tag{4.4}$$

Byte-wise subkeys and rotation amounts are extracted exactly as in the code by masking/shifting:

$$k_i^{(t)} = q(\cdot) \bmod 256, \qquad t \in \{1,2,3,4\}, \tag{4.5}$$

$$r_i^{(1)} = \left(\lfloor q(\cdot)/2^8 \rfloor \bmod 8\right), \quad r_i^{(2)} = \left(\lfloor q(\cdot)/2^8 \rfloor \bmod 8\right), \tag{4.6}$$

and $\mathrm{IV}_j = q(\cdot) \bmod 256$ for $j = 1,2,3,4$. The additional words $w^{(F)}, w^{(B)}, w^{(C)}, w^{(D)}$ are further split into packed per-byte parameters:

- **Core packed parameters (from $w^{(F)}$ and $w^{(B)}$):**

$$r_A(i) = \left(\lfloor w_i^{(F)}/2^8 \rfloor \bmod 8\right), \quad m_1(i) = \left(\lfloor w_i^{(F)}/2^{16} \rfloor \bmod 256\right) \mathrm{OR}\ 1, \quad k_5(i) = \left(\lfloor w_i^{(F)}/2^{24} \rfloor \bmod 256\right),$$

$$r_B(i) = \left(\lfloor w_i^{(B)}/2^8 \rfloor \bmod 8\right), \quad m_2(i) = \left(\lfloor w_i^{(B)}/2^{16} \rfloor \bmod 256\right) \mathrm{OR}\ 1, \quad k_7(i) = \left(\lfloor w_i^{(B)}/2^{24} \rfloor \bmod 256\right).$$

- **Avalanche-booster packed parameters (from $w^{(C)}$ and $w^{(D)}$):**

$$k_9(i) = w_i^{(C)} \bmod 256, \quad k_{10}(i) = \Big(\lfloor w_i^{(C)}/2^8 \rfloor \bmod 256\Big), \quad b_C(i) = \Big(\lfloor w_i^{(C)}/2^{16} \rfloor \bmod 256\Big),$$

$$r_3(i) = \Big(\lfloor b_C(i)/2 \rfloor \bmod 8\Big), \quad m_3(i) = b_C(i) \text{ OR } 1, \quad k_{11}(i) = \Big(\lfloor w_i^{(C)}/2^{24} \rfloor \bmod 256\Big),$$

$$k_{12}(i) = w_i^{(D)} \bmod 256, \quad k_{13}(i) = \Big(\lfloor w_i^{(D)}/2^8 \rfloor \bmod 256\Big), \quad b_D(i) = \Big(\lfloor w_i^{(D)}/2^{16} \rfloor \bmod 256\Big),$$

$$r_4(i) = \Big(\lfloor b_D(i)/2 \rfloor \bmod 8\Big), \quad m_4(i) = b_D(i) \text{ OR } 1, \quad k_{14}(i) = \Big(\lfloor w_i^{(D)}/2^{24} \rfloor \bmod 256\Big).$$

By construction, m_1, m_2, m_3, m_4 are always odd, guaranteeing invertibility of the multiplicative mixing.

Remark 4.1. The conversion from floating-point chaotic samples to 32-bit unsigned words is not unique; common choices include direct scaling and truncation, fractional-part extraction, and mixed-coordinate quantization. For simplicity and reproducibility, in the present implementation, we use $q = \text{uint32}\Big(\text{mod}\Big(\Big\lfloor (s_{\text{raw}} + 100) \times 10^{12} \Big\rfloor, 2^{32}\Big)\Big)$, where $s_{\text{raw}} = [x_n, y_n]$ denotes the double-precision chaotic sequence.

4.1.3. Key-dependent dynamic S-box

Using the reserved seed $\{q_t^{(S)}\}_{t=1}^{256}$, we construct a key-dependent bijection $S : \{0, \ldots, 255\} \to \{0, \ldots, 255\}$ by sorting

$$\text{idx} = \text{argsort}(q_1^{(S)}, \ldots, q_{256}^{(S)}), \qquad S(b) = \text{idx}(b + 1) - 1.$$

The inverse S^{-1} exists and is used in decryption.

4.2. The proposed encryption algorithm

In this subsection, based on the keystream, the dynamic S-box, and the auxiliary parameters prepared above, we present the complete framework of the proposed image-encryption algorithm.

4.2.1. Two-layer Fisher–Yates permutation

Two independent permutations are generated using $k^{(\pi_1)}$ and $k^{(\pi_2)}$. Initialize $\pi(i) = i$ for $i = 1, \ldots, L$. For $i = L, L-1, \ldots, 2$,

$$j = (k_{L-i+1} \bmod i) + 1, \qquad \text{swap } \pi(i) \text{ and } \pi(j).$$

First, apply π_1 to obtain $p_i^{(1)} = p_{\pi_1(i)}$, then apply π_2 at the appropriate stage (see below). Both permutations are bijective and inverted by applying π^{-1} (implemented as a scatter).

4.2.2. Core index-coupled nonlinear diffusion (Stages 1–3)

The core diffusion consists of a forward pass producing an intermediate sequence b (Stage 1), a second permutation (Stage 2), and a backward pass producing c (Stage 3). The distinguishing feature is an index-coupled state injection: Besides the immediate neighbor, each update also depends on a

key-driven remote sample selected by $w^{(F)}$ or $w^{(B)}$.

Index-coupled forward state. Let $b_0 = \mathrm{IV}_1$. For $i \geq 2$, define

$$j_F(i) = (w_i^{(F)} \bmod (i-1)) + 1 \in \{1, \ldots, i-1\}, \qquad \mathrm{state}_F(i) = b_{i-1} \oplus \mathrm{ROTL}_8(b_{j_F(i)},\, r_A(i)),$$

and at the boundary $i = 1$, set $b_0 = \mathrm{IV}_1$ and reuse $b_{j_F(1)} = \mathrm{IV}_1$. This state is injected before substitution, ensuring nonlinearity and strong dependency on early bytes.

Stage 1 (core forward update). Let $p^{(1)}$ denote the permuted plaintext after π_1. For $i = 1, \ldots, L$,

$$t_i = S\,(p_i^{(1)} \oplus k_i^{(1)} \oplus\ \mathrm{state}_F(i)), \qquad u_i = (t_i \boxplus b_{i-1} \boxplus b_{j_F(i)} \boxplus k_i^{(2)}) \mod 256, \tag{4.7}$$

$$b_i = \mathrm{ROTL}_8\Big(\mathrm{MUL}_8\,(u_i \oplus k_5(i),\, m_1(i)),\ r_i^{(1)}\Big). \tag{4.8}$$

All components are bijective: S is a permutation; $\mathrm{MUL}_8(\cdot, m_1)$ is invertible since m_1 is odd; and rotation/XOR are invertible.

Stage 2 (second permutation). Apply the second permutation π_2 to b:

$$b'_i = b_{\pi_2(i)}.$$

Index-coupled backward state. Let $c_{L+1} = \mathrm{IV}_2$. For $i \leq L-1$, define a remote index

$$j_B(i) = (i+1) + (w_i^{(B)} \bmod (L-i)) \in \{i+1, \ldots, L\}, \qquad \mathrm{state}_B(i) = c_{i+1} \oplus \mathrm{ROTR}_8(c_{j_B(i)},\, r_B(i)),$$

and at the boundary, use $c_{L+1} = \mathrm{IV}_2$ (and $j_B(L)$ is not used).

Stage 3 (core backward update). For $i = L, \ldots, 1$,

$$t'_i = S\,(b'_i \oplus k_i^{(3)} \oplus\ \mathrm{state}_B(i)), \qquad u'_i = (t'_i \boxplus c_{i+1} \boxplus c_{j_B(i)} \boxplus k_i^{(4)}) \mod 256, \tag{4.9}$$

$$c_i = \mathrm{ROTL}_8\Big(\mathrm{MUL}_8\,(u'_i \oplus k_7(i),\, m_2(i)),\ r_i^{(2)}\Big). \tag{4.10}$$

The output of Stage 3 is the core ciphertext vector c.

4.2.3. Avalanche booster (Stages 4–5)

To further strengthen plaintext sensitivity, we append a reversible two-pass avalanche booster that adds an extra forward feedback chain followed by a backward feedback chain. The booster is designed to accelerate the propagation of local perturbations through the ciphertext while preserving exact invertibility over $\mathbb{Z}_{256}$. Each pass employs the same family of byte-wise bijective transformations–S-box substitution, multiplication by an odd element modulo 256, and 8-bit rotation–and is seeded by an independent initialization byte, IV_3 for the forward pass and IV_4 for the backward pass.

Stage 4 (booster forward). Let $d_0 = \mathrm{IV}_3$. For $i = 1, \ldots, L$,

$$\tilde{t}_i = S\,(c_i \oplus k_9(i)), \qquad \tilde{u}_i = (\tilde{t}_i \boxplus d_{i-1} \boxplus k_{10}(i)) \mod 256, \tag{4.11}$$

$$d_i = \mathrm{ROTL}_8\Big(\mathrm{MUL}_8\,(\tilde{u}_i \oplus k_{11}(i),\, m_3(i)),\ r_3(i)\Big). \tag{4.12}$$

Stage 5 (booster backward). Let $e_{L+1} = \mathrm{IV}_4$. For $i = L, \ldots, 1$,

$$\hat{t}_i = S(d_i \oplus k_{12}(i)), \qquad \hat{u}_i = (\hat{t}_i \boxplus e_{i+1} \boxplus k_{13}(i)) \mod 256, \tag{4.13}$$

$$e_i = \mathrm{ROTL}_8\Big(\mathrm{MUL}_8\,(\hat{u}_i \oplus k_{14}(i),\, m_4(i)),\; r_4(i)\Big). \tag{4.14}$$

The final ciphertext is $e = (e_1, \ldots, e_L)$.

The following Figure 5 illustrates the end-to-end structure of the proposed chaos-driven reversible cipher, highlighting the deterministic keystream partitioning, two permutations, index-coupled nonlinear forward/backward diffusion, and the bidirectional avalanche booster, together with the exact inverse decryption order.

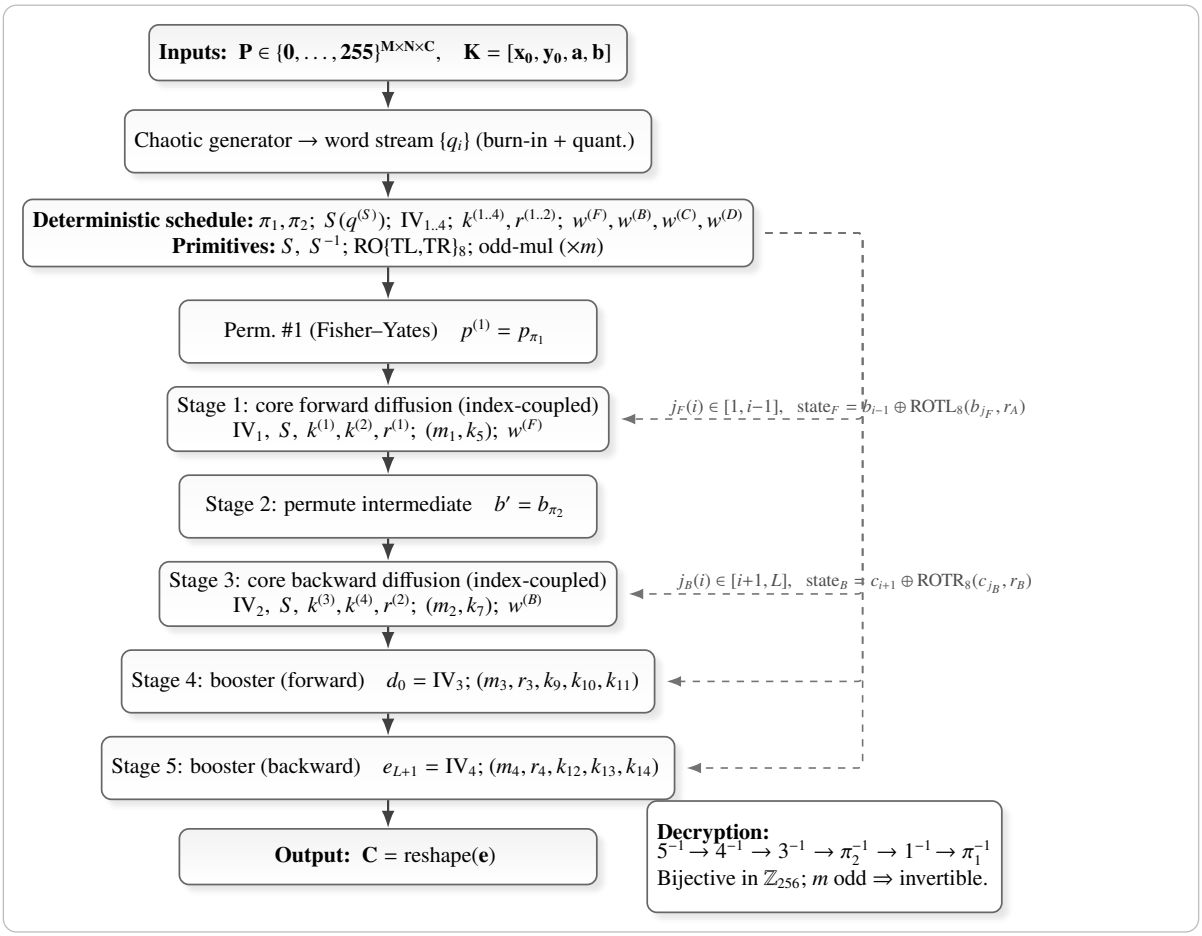


Figure 5. Schematic of the chaos-driven reversible cipher with two permutations, index-coupled core diffusion, and a bidirectional avalanche booster.

Remark 4.2 (random coupling interpretation). The remote-index injections $j_F(i), j_B(i)$ induce a key-driven random coupling between distant sites of the byte sequence. This is analogous to iterated dynamics on a randomly rewired dependency graph, which typically accelerates mixing and decorrelation-properties desirable for resisting statistical and differential cryptanalysis.

4.3. Decryption (exact inverse)

Decryption regenerates the identical keystream partitioning, S, π_1, and π_2, from the same key K, vectorizes the ciphertext into e, and inverts the stages in reverse order:

- Invert Stage 5 using the known neighbor e_{i+1} (or IV_4 at the boundary): Apply ROTR_8, multiply by $m_4(i)^{-1}$ mod 256, XOR with $k_{14}(i)$, subtract e_{i+1} and $k_{13}(i)$ in $\mathbb{Z}_{256}$, then apply S^{-1} and XOR with $k_{12}(i)$ to recover d_i.
- Invert Stage 4 forward using d_{i-1} (or IV_3): Apply ROTR_8, multiply by $m_3(i)^{-1}$, XOR with $k_{11}(i)$, subtract d_{i-1} and $k_{10}(i)$, then apply S^{-1} and XOR with $k_9(i)$ to recover c_i.
- Invert Stage 3 backward by recomputing $j_B(i)$ and $\mathrm{state}_B(i)$ from ciphertext neighbors, then undo rotation, odd multiplication, key-XOR, modular subtraction, S^{-1}, and the final XOR with $\mathrm{state}_B(i)$ to recover b'_i.
- Apply π_2^{-1} to obtain b, invert Stage 1 forward similarly (using $j_F(i)$ and $\mathrm{state}_F(i)$), and finally apply π_1^{-1} to recover p and reshape to obtain P.

Since every component is bijective (permutations, S-box, odd multiplications, rotations, XOR, and modular $\pm$), the overall cipher is strictly reversible and yields lossless decryption.

4.4. Complexity and security analysis

Computational complexity. Both permutations and each of the five diffusion/booster passes require a constant amount of byte-wise operations per index. Therefore, encryption and decryption each run in $O(L)$ time and use $O(L)$ memory, where $L = MNC$ is the total number of processed bytes and the memory footprint is dominated by a few length-L byte buffers. The dynamic S-box construction only sorts 256 elements and thus costs $O(256 \log 256)$, which is negligible in practice.

Key-space security analysis. The security of the proposed cipher against exhaustive search is governed by its *effective* key space. The secret key is $K = [x_0, y_0, a, b]$, and all keystream-derived components (two permutations, the dynamic S-box, the index-coupling sequences, and the diffusion/booster subkeys including $\mathrm{IV}_1, \ldots, \mathrm{IV}_4$) are deterministically generated from K. Under a double-precision digital implementation, each real-valued parameter contributes on the order of 2^{52} distinguishable values over a finite interval, yielding a conservative key-space magnitude of approximately $(2^{52})^4 \approx 2^{208}$, which is far above commonly accepted brute-force security baselines [2, 3]. Moreover, due to the strong key-dependent branching introduced by the dynamic S-box and the index-coupled feedback indices $j_F(i)$ and $j_B(i)$, small perturbations of K lead to substantially different keystream partitions and internal parameters, as will be further supported by the sensitivity results in the next section.

Remark 4.3. Since $|a|$ and $|b|$ remove the sign information, the sign-flipped pairs lead to equivalent keys. Therefore, the effective key space should exclude the redundant sign representations, yielding a constant-factor reduction (at most $4\times$ for (a, b)). For the practical use of the proposed image-encryption scheme, we restrict the parameters a and b to positive values, so that the equivalent-key issue does not arise in the implementation considered here. Accordingly, the key-space estimate is revised from $\mathcal{K}$ to $\mathcal{K}/4$ (equivalently, a reduction of 2 bits), which does not affect the security conclusion.

5. Experimental results and performance analysis

To evaluate the effectiveness and security of the proposed image-encryption framework, we perform a set of standard cryptanalytic and performance-oriented experiments in this section. All simulations are implemented in MATLAB, and the scheme is tested on multiple grayscale images with different resolutions to demonstrate its robustness and scalability.

5.1. Simulation results

The following Figure 6 presents the combined visualization (three rows for the three test images; three columns for plaintext, ciphertext, and decrypted image, respectively). In all cases, the ciphertext exhibits a noise-like appearance with no visually recognizable structures from the plaintext, while the decrypted results match the corresponding plaintexts, confirming the correctness of the encryption-decryption pipeline.

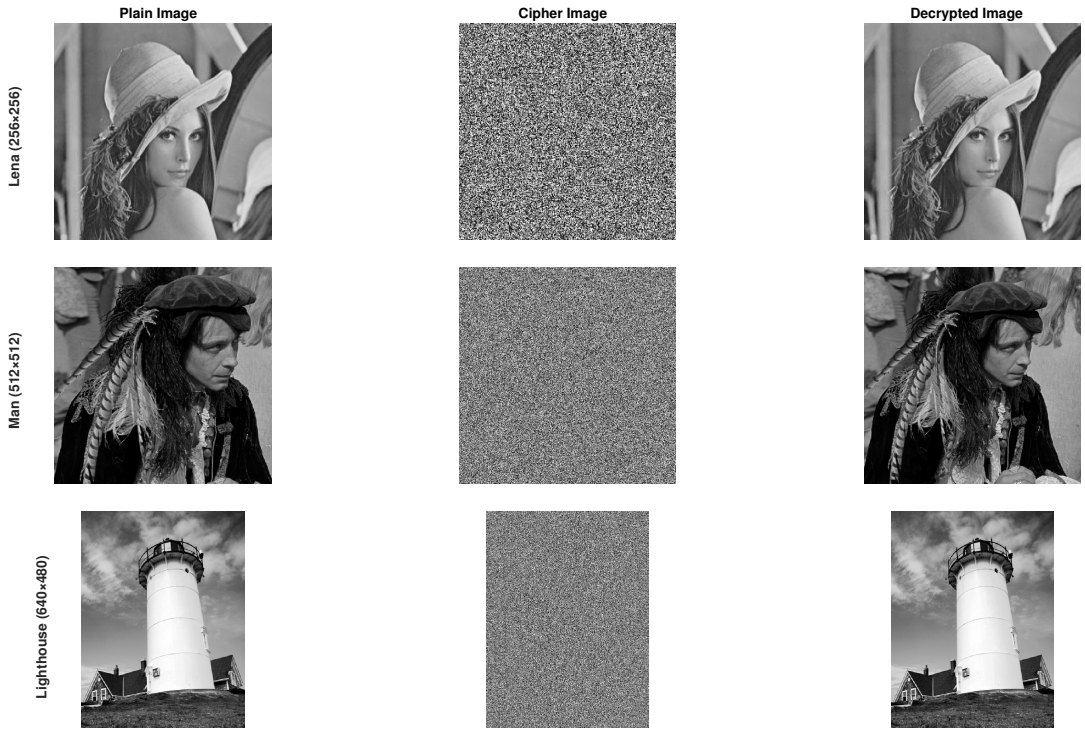


Figure 6. Combined encryption-decryption results on three grayscale images with different resolutions. Rows correspond to (a) Lena (256×256), (b) Man (512×512), and (c) Lighthouse (640×480). Columns show the plaintext, ciphertext, and decrypted image, respectively.

To demonstrate the visual effectiveness and correctness of the proposed cryptosystem across different resolutions, three standard grayscale test images were used: (a) Lena (256×256), (b) Man (512×512), and (c) Lighthouse (640×480). For each image, we performed encryption and then decrypted the ciphertext using the same secret key.

5.2. Key sensitivity experiment

High key sensitivity is a fundamental requirement for secure image encryption: An arbitrarily small perturbation in the secret key should lead to a completely incorrect decryption result, thereby preventing near-key guessing and related-key attempts. In this experiment, we first encrypt a plaintext image using the secret key $K = [x_0, y_0, a, b]$ to obtain the ciphertext C. We then decrypt the same ciphertext using four perturbed keys $K' = K + \Delta \mathbf{e}_t$, where $\Delta = 10^{-15}$ and $\mathbf{e}_t$ denotes the unit vector that perturbs only the t-th component (x_0, y_0, a, or b), while keeping all other components unchanged.

The following Figure 7 summarizes the results in a single combined panel and illustrates the corresponding decryption results mentioned in (5.1).

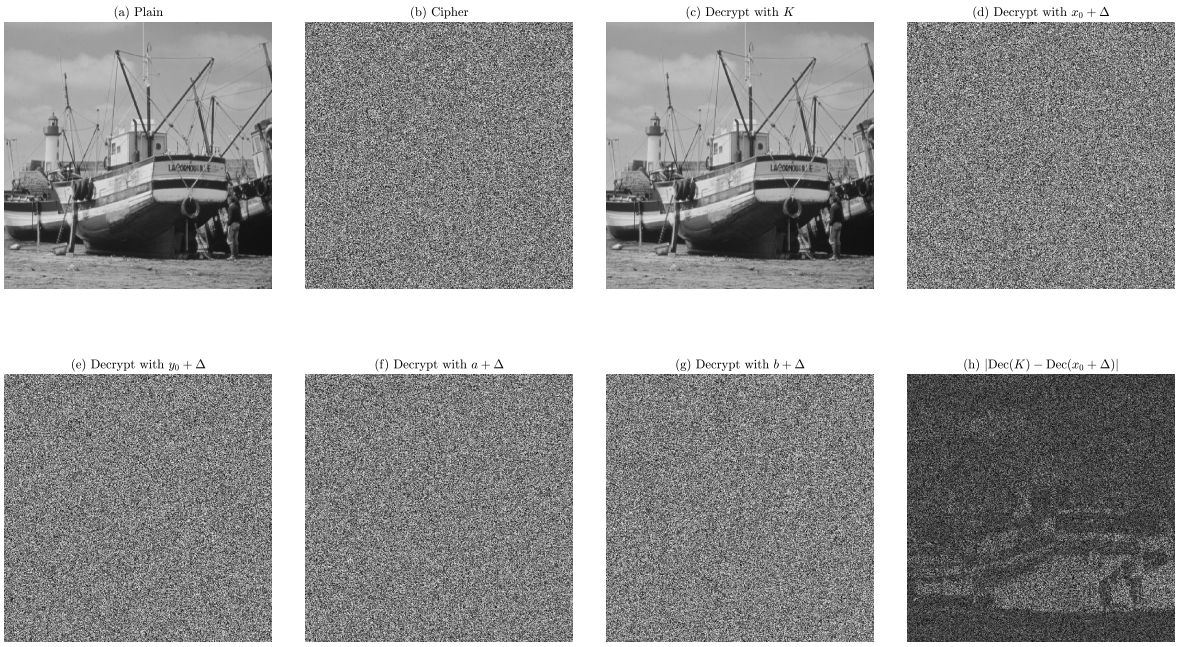


Figure 7. Key sensitivity experiment with $\Delta = 10^{-15}$. The ciphertext is decrypted using the correct key K and four perturbed keys obtained by adding Δ to one component of $K = [x_0, y_0, a, b]$. A tiny key perturbation leads to a completely distorted decryption result. Decryption with the correct key K perfectly reconstructs the plaintext, whereas perturbing any single key component by $\Delta = 10^{-15}$ produces noise-like outputs that reveal no visual information of the original image. This confirms that the proposed scheme exhibits strong key sensitivity: Extremely small key deviations cause complete decryption failure.

Key sensitivity is a critical security requirement for image encryption systems. It refers to the property that a slight change in the secret key should lead to a completely different cipher image when encrypting the same plaintext or result in a totally incorrect decrypted image when decrypting a given ciphertext. An encryption scheme with high key sensitivity can effectively resist brute-force and key-related attacks.

To evaluate the key sensitivity of the proposed encryption algorithm, the cipher image of the

standard test image 512×512 Boats was decrypted using four slightly modified keys, defined as

$$\begin{aligned} K_1 &= [0.87 + 10^{-15},\ 0.93,\ 5.19,\ 8.14], \\ K_2 &= [0.87,\ 0.93 + 10^{-15},\ 5.19,\ 8.14], \\ K_3 &= [0.87,\ 0.93,\ 5.19 + 10^{-15},\ 8.14], \\ K_4 &= [0.87,\ 0.93,\ 5.19,\ 8.14 + 10^{-15}]. \end{aligned} \tag{5.1}$$

It can be observed that even an extremely small perturbation of 10^{-15} in any component of the secret key leads to completely distorted images that exhibit noise-like characteristics and reveal no visual information of the original plaintext.

These experimental results clearly demonstrate that the proposed encryption scheme exhibits excellent key sensitivity. Consequently, it can effectively withstand brute-force attacks and key sensitivity-based cryptanalytic attacks, thereby ensuring a high level of security.

5.3. Ciphertext occlusion (cropping) robustness

In practical applications, encrypted images may be partially corrupted during storage or transmission (e.g., packet loss, occlusion, or local damage). To examine the robustness of the proposed cryptosystem under such ciphertext impairments, we conduct an occlusion/cropping experiment on the ciphertext domain.

Specifically, a plaintext image is first encrypted using the correct key K to generate the ciphertext C. Then, two distorted ciphertexts are constructed by masking different regions of C: (i) a central block occlusion with a given area ratio, and (ii) multiple randomly located block occlusions, where the masked ciphertext pixels are replaced by a constant value. Finally, each distorted ciphertext is decrypted using the correct key K, and the corresponding outputs are reported in the following figure.

As illustrated in Figure 8 below, although the ciphertext is severely occluded in different patterns, the decrypted images still preserve the main visual content of the plaintext, showing a graceful degradation behavior rather than complete loss of recognizability. This property is beneficial for lossy or unreliable communication channels and for fault-tolerant storage, where partial ciphertext corruption may occur and retransmission may be expensive. In this sense, the proposed scheme improves the availability and practical robustness of the encrypted-image pipeline under partial ciphertext loss.

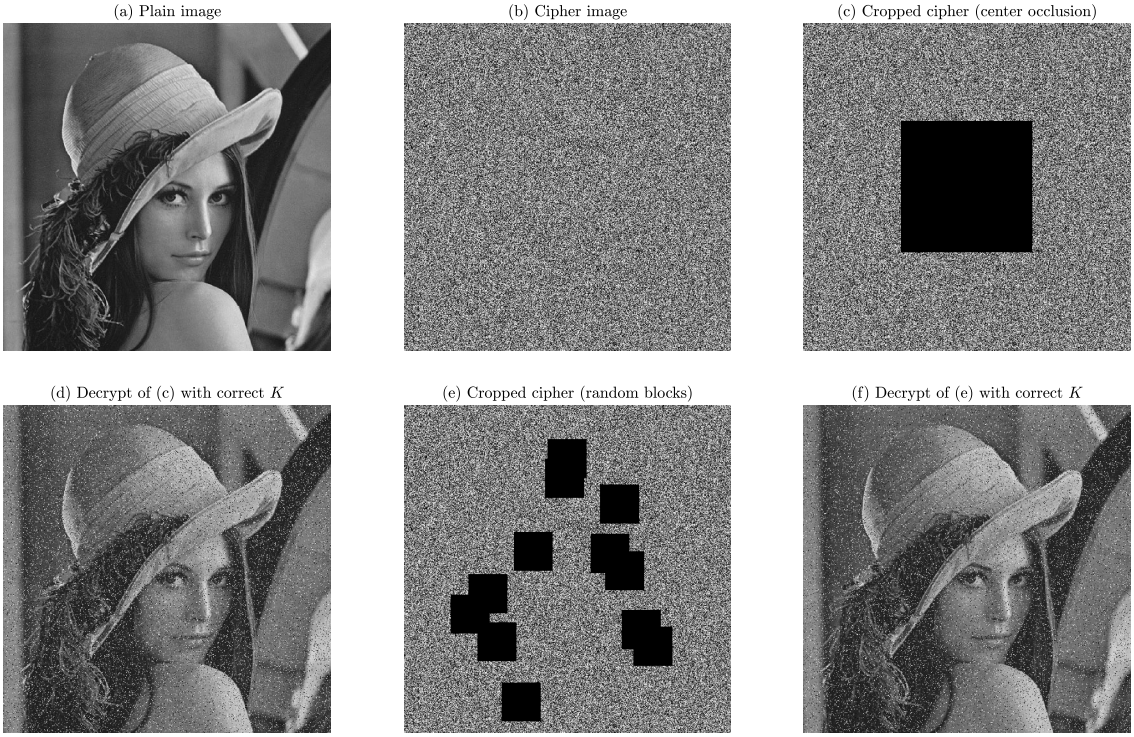


Figure 8. Histogram comparison between plaintext and ciphertext images.

5.4. Plaintext sensitivity analysis

An effective image encryption algorithm should exhibit high sensitivity to minor changes in the plaintext, which is a fundamental requirement for resisting differential attacks. In other words, a slight modification in the plaintext image, such as changing the gray value of a single pixel, should result in a completely different ciphertext image. This property is commonly referred to as the avalanche effect in cryptography.

To quantitatively evaluate the plaintext sensitivity of the proposed encryption scheme, two widely adopted metrics are employed: NPCR and UACI. These metrics are extensively used in the literature to assess the diffusion capability and security performance of image encryption algorithms.

Let C_1 and C_2 denote two cipher images of size $M \times N$, which are generated from two plaintext images differing by only one pixel. The NPCR is defined as

$$\text{NPCR} = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i, j), \tag{5.2}$$

where

$$D(i, j) = \begin{cases} 1, & C_1(i, j) \neq C_2(i, j), \\ 0, & \text{otherwise.} \end{cases} \tag{5.3}$$

The NPCR measures the percentage of pixels that change in the ciphertext when a single pixel of the plaintext is modified.

The UACI metric evaluates the average intensity of differences between two cipher images and is defined as

$$\mathrm{UACI} = \frac{1}{255 \times MN} \sum_{i=1}^{M} \sum_{j=1}^{N} |C_1(i,j) - C_2(i,j)| \,. \tag{5.4}$$

A higher UACI value indicates that the encryption algorithm produces stronger diffusion in terms of pixel intensity variations.

For an ideal random cipher image with 8-bit gray levels, the theoretical expected values of the NPCR and UACI are 99.6094% and 33.4635%, respectively. Values close to these benchmarks imply strong plaintext sensitivity and effective diffusion.

Table 1. Plaintext sensitivity results (NPCR/UACI). In each trial, one pixel location is selected uniformly at random and modified by +1 (mod 256), and the two ciphertexts are compared. Here, $Abs.deviation = |Mean - Theoretical|$.

Algorithm	Image	Metric	Theoretical	Mean (2000 trials)	95% CI	Abs. deviation
Proposed	Lena	NPCR	99.6094%	99.6096%	[99.6090, 99.6102]	0.0002%
	Lena	UACI	33.4635%	33.4899%	[33.4876, 33.4921]	0.0263%
	Baboon	NPCR	99.6094%	99.6092%	[99.6089, 99.6096]	0.0001%
	Baboon	UACI	33.4635%	33.4625%	[33.4614, 33.4636]	0.0011%
	Butterfly	NPCR	99.6094%	99.6097%	[99.6091, 99.6102]	0.0003%
	Butterfly	UACI	33.4635%	33.4702%	[33.4683, 33.4721]	0.0067%
CLSS Ref [30]	Lena	NPCR	99.6094%	99.6198%	[99.6194, 99.6202]	0.0104%
	Lena	UACI	33.4635%	33.3147%	[33.3138, 33.3156]	0.1488%
	Baboon	NPCR	99.6094%	99.6079%	[99.6078, 99.6080]	0.0015%
	Baboon	UACI	33.4635%	33.4455%	[33.4453, 33.4456]	0.0181%
	Butterfly	NPCR	99.6094%	99.6080%	[99.6077, 99.6084]	0.0014%
	Butterfly	UACI	33.4635%	33.3532%	[33.3528, 33.3536]	0.1103%
HELS Ref [34]	Lena	NPCR	99.6094%	99.6027%	[99.5986, 99.6068]	0.0067%
	Lena	UACI	33.4635%	33.5981%	[33.5558, 33.6405]	0.1346%
	Baboon	NPCR	99.6094%	99.5318%	[99.4283, 99.6353]	0.0776%
	Baboon	UACI	33.4635%	33.5244%	[33.4637, 33.5851]	0.0609%
	Butterfly	NPCR	99.6094%	99.5914%	[99.5669, 99.6158]	0.0181%
	Butterfly	UACI	33.4635%	33.5642%	[33.5228, 33.6055]	0.1006%

As reported in Table 1 , the proposed 2D-HDDS-based scheme achieves NPCR values very close to the theoretical expectation (99.609%) on all three 512×512 grayscale test images. To obtain statistically stable estimates, the NPCR and UACI are computed as the mean of 2000 independent trials, where each trial encrypts the original image and a modified version differing by exactly one randomly selected pixel (incremented by 1 (mod 256)). The averaged UACI values are also close to the theoretical benchmark (33.463%), indicating that the proposed diffusion/booster architecture propagates a one-pixel perturbation effectively across the ciphertext.

Furthermore, the reported 95% confidence intervals are consistently narrow and centered around the theoretical values, demonstrating the statistical stability of the proposed scheme. Compared with the

reference algorithms, the proposed method generally exhibits smaller absolute deviations and tighter confidence intervals, indicating more reliable plaintext sensitivity and stronger diffusion consistency.

In comparison with representative recent chaos-based schemes, including the two-dimensional hyperchaotic exponential adjusted logistic and sine map (2D-HELS) cipher [34] and the 2D-CLSS-based method [30], the proposed algorithm yields comparable or slightly improved NPCR/UACI results across the tested images.

In practice, highly structured plaintexts such as all-black, all-white, checkerboard, and stripe patterns are meaningful in chosen-plaintext analysis [31, 35, 40], because they suppress natural-image texture and redundancy and therefore make it easier to expose possible structural weaknesses, such as sparse position tracking, weak diffusion paths, or a readily decoupled permutation layer. To this end, we further carry out a chosen-plaintext style probe using several specially constructed 512×512 grayscale plaintexts.

First, three structured plaintext images were constructed, including an all-black image, an all-white image, and a vertical-stripe image. These plaintext images were encrypted using the same secret key to produce the corresponding ciphertext images. Ideally, even highly structured plaintexts should produce ciphertexts that appear statistically random and visually indistinguishable.

To quantify the diffusion effect, the NPCR and UACI metrics were computed between ciphertext images generated from different structured plaintexts. In particular, the ciphertext corresponding to the all-white plaintext was compared with the ciphertext corresponding to the all-black plaintext, and the ciphertext corresponding to the vertical-stripe plaintext was also compared with that of the all-black plaintext (see Figure 9).

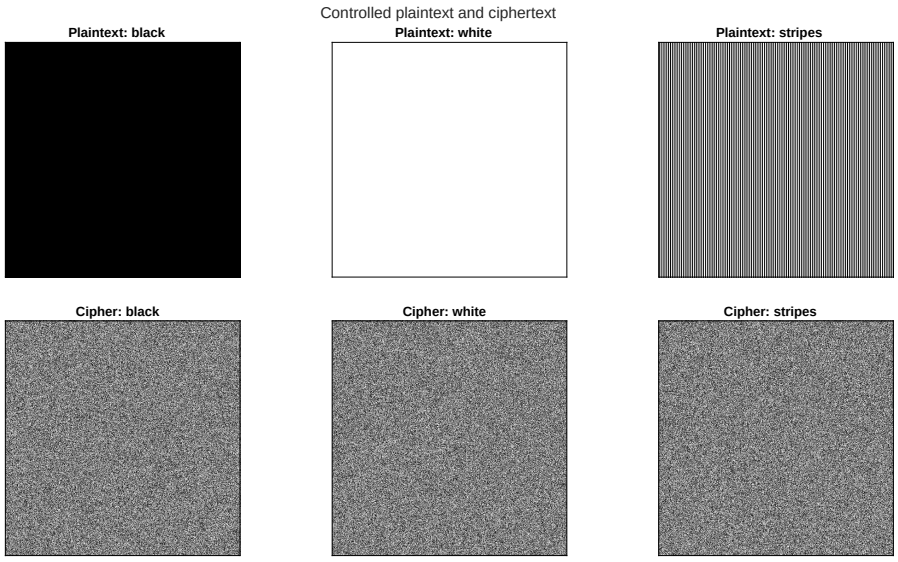


Figure 9. Controlled plaintext images and their corresponding ciphertexts produced by the proposed encryption algorithm.

The obtained results are as follows:

- Cipher(White) vs. Cipher(Black): NPCR = 99.5956%, UACI = 33.3683%.

- Cipher(Stripe) vs. Cipher(Black): NPCR = 99.6174%, UACI = 33.4610%.

These values are very close to the theoretical expectations for ideal image encryption systems (NPCR $\approx$ 99.6% and UACI $\approx$ 33.4%), indicating that the proposed encryption scheme can effectively diffuse large structural differences in the plaintext into significant and unpredictable changes in the ciphertext.

Single-pixel probe experiments were conducted on the two extreme cases: all-black and all-white images. In each trial, five pixel positions were randomly selected and modified by +1 (mod 256). The resulting ciphertext sensitivity was quantified using the NPCR and UACI metrics, as summarized in Table 2. The results indicate that a single-bit change at any position triggers a global avalanche effect, with the NPCR and UACI values consistently approaching the theoretical ideals ($\sim$ 99.6% and $\sim$ 33.4%, respectively). Such high sensitivity confirms that the proposed index-coupled diffusion and avalanche booster effectively propagate local perturbations throughout the entire ciphertext space, providing robust resistance against chosen-plaintext and differential attacks.

Table 2. NPCR and UACI results of the single-pixel chosen-plaintext probe experiment under different plaintext baselines.

(a) All-black baseline.

Row	Col	NPCR (%)	UACI (%)
214	48	99.6105	33.5338
369	96	99.6094	33.4647
1	177	99.6128	33.4920
155	204	99.6326	33.4916
76	276	99.6178	33.5165
Average	–	99.6166	33.4997

(b) All-white baseline.

Row	Col	NPCR (%)	UACI (%)
214	48	99.6143	33.4261
369	96	99.6048	33.4361
1	177	99.5987	33.4223
155	204	99.6181	33.3876
76	276	99.5998	33.4004
Average	–	99.6072	33.4145

These findings confirm that two plaintexts differing in a single pixel produce substantially different ciphertexts, demonstrating plaintext sensitivity and effective diffusion; consequently, the proposed scheme can (empirical rather than formally cryptographic) effectively mitigate differential attacks and provide improved robustness under stronger adversarial models such as known-plaintext and chosen-plaintext scenarios.

5.5. Correlation coefficient analysis

Natural images possess strong local statistical dependencies arising from spatial continuity and structural redundancy, which manifest as high correlations between adjacent pixels. Such dependencies may reveal structural information and can be exploited by statistical cryptanalysis. Therefore, a secure image-encryption scheme is expected to effectively suppress these correlations so that the ciphertext exhibits statistical behavior close to that of a random image, with correlation coefficients approaching zero in the horizontal, vertical, and diagonal directions.

To quantitatively evaluate the decorrelation capability of the proposed encryption scheme, the correlation coefficients of adjacent pixels are computed by exhaustively traversing all possible neighboring pixel pairs in the horizontal, vertical, and diagonal directions. For a given direction, let $\{(x_i, y_i)\}_{i=1}^{N}$ denote the gray-level values of all adjacent pixel pairs in the considered image, where N is

the total number of such pairs determined by the image size. The correlation coefficient is defined as

$$r_{xy} = \frac{\sum_{i=1}^{N}(x_i - \mu_x)(y_i - \mu_y)}{\sqrt{\sum_{i=1}^{N}(x_i - \mu_x)^2}\sqrt{\sum_{i=1}^{N}(y_i - \mu_y)^2}}, \tag{5.5}$$

where μ_x and μ_y denote the mean values of the sequences $\{x_i\}$ and $\{y_i\}$, respectively. Since all adjacent pixel pairs are included, the resulting correlation coefficients are deterministic and free of sampling randomness.

Figure 10 visualizes the distributions of adjacent pixel pairs, and Table 3 below summarizes the corresponding numerical results.

It can be observed that the correlation coefficients of plaintext images are close to unity, whereas those of the ciphertext images are close to zero in all directions. This demonstrates that the proposed scheme provides strong resistance against correlation-based statistical attacks. As the correctly decrypted images are visually identical to the plaintexts, their correlation characteristics coincide with those of the plaintext images and are therefore omitted for brevity.

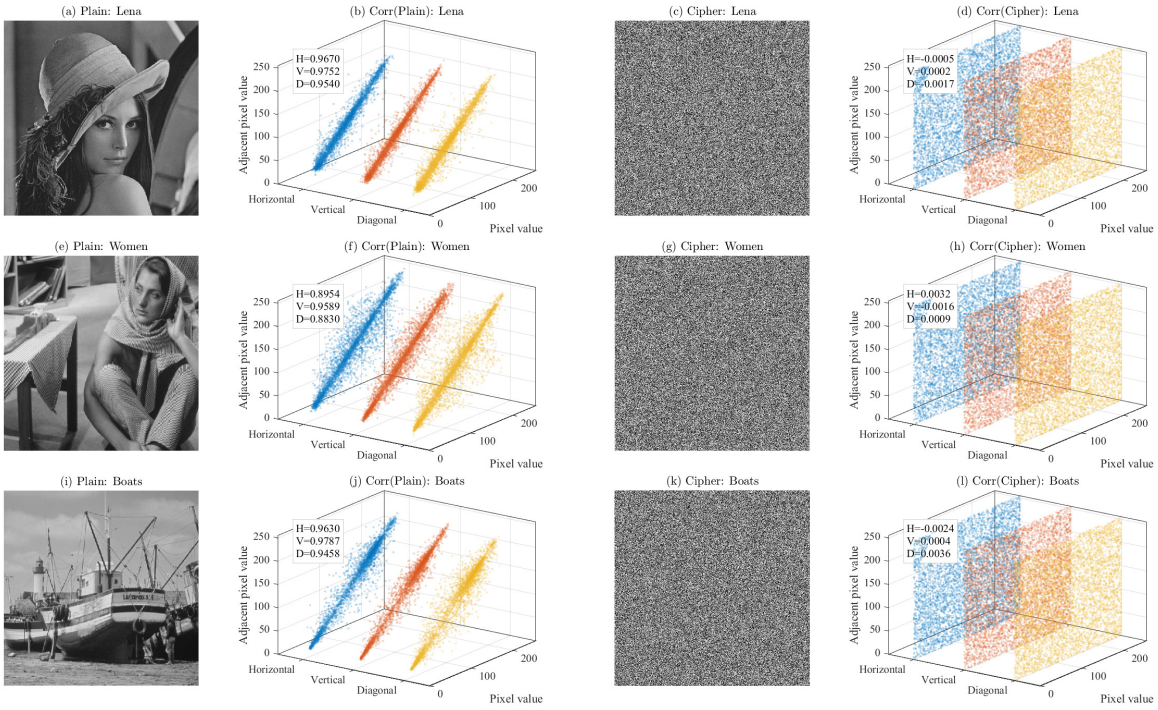


Figure 10. Adjacent-pixel correlation plots for three test images. From left to right: plaintext, stacked 3D scatter plot of plaintext adjacent-pixel pairs, ciphertext, and stacked 3D scatter plot of ciphertext adjacent-pixel pairs. The three layers in each scatter plot correspond to the horizontal, vertical, and diagonal directions.

Table 3. Adjacent-pixel correlation coefficients obtained by full sampling of all neighboring pixel pairs for three test images.

Image	Type	r_{H}	r_{V}	r_{D}
Lena	Plain	0.9670	0.9752	0.9540
	Cipher	-0.0005	0.0002	-0.0017
Women	Plain	0.8954	0.9589	0.8830
	Cipher	0.0032	-0.0016	0.0009
Boats	Plain	0.9630	0.9787	0.9458
	Cipher	-0.0024	0.0004	0.0036

5.6. Histogram analysis

A secure image cipher should effectively suppress the structured gray-level statistics of the plaintext and yield ciphertext intensities that are close to being uniformly distributed over $[0, 255]$. To visually assess this first-order statistical property, Figure 11 reports three representative plaintext-ciphertext pairs and their normalized histograms with 256 bins.

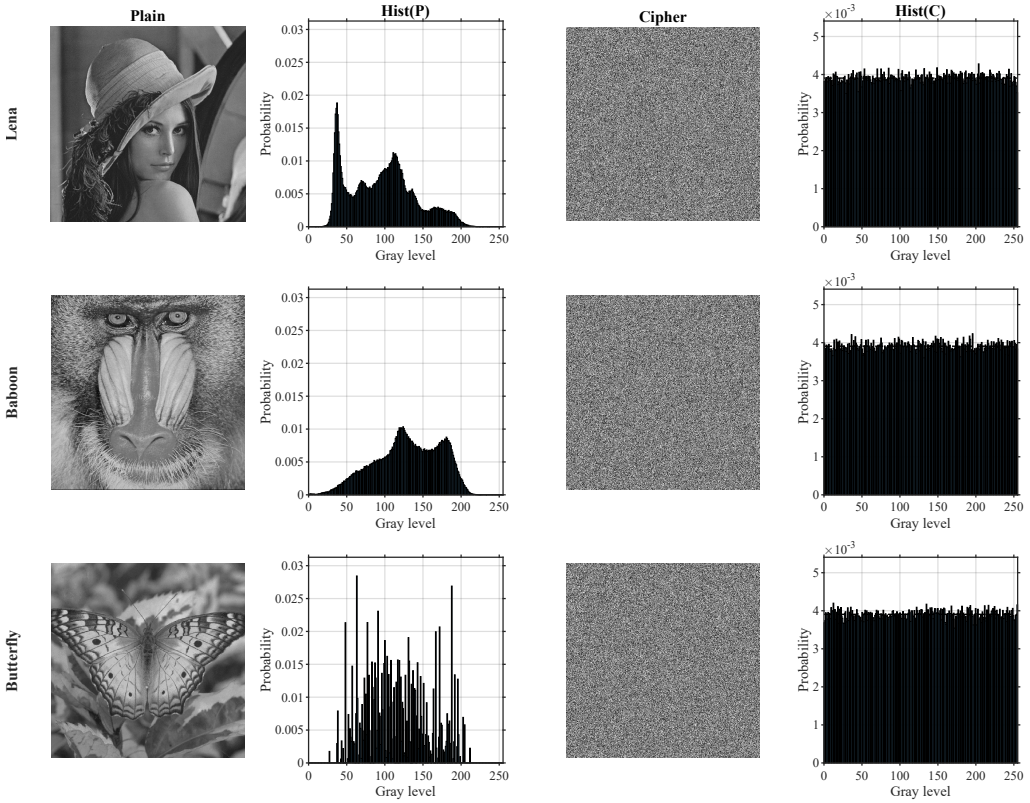


Figure 11. Histogram analysis on three benchmark images. Each row is arranged as Plain/Hist(P)/Cipher/Hist(C). All histograms are normalized to probabilities with 256 bins over $[0, 255]$.

For each sample, the plaintext histogram Hist(P) is plotted using a standard probability scale to highlight the strong non-uniformity of natural images. In contrast, the ciphertext histogram Hist(C) is

displayed with a zoomed vertical axis centered at the theoretical uniform baseline $1/256 \approx 0.003906$, together with the reference line $y = 1/256$. This visualization makes it clear that the ciphertext histograms fluctuate only slightly around the uniform level across the full gray range, indicating that pixel-value statistics are well concealed. Consequently, the proposed scheme exhibits strong resistance against histogram-based statistical attacks.

5.7. Information entropy analysis

Information entropy measures the uncertainty of gray-level distributions and is widely used as a first-order statistical indicator in image-encryption evaluation. For an 8-bit grayscale image with 256 intensity levels, the Shannon entropy is defined as

$$H = -\sum_{i=0}^{255} p(i) \log_2 p(i), \tag{5.6}$$

where $p(i)$ denotes the empirical probability of gray level i. The theoretical upper bound is $H_{\max} = 8$ bits; ciphertext images with entropy close to 8 indicate that the gray-level distribution is nearly uniform and that simple statistical leakage via intensity histograms is effectively suppressed.

In this experiment, we compute the entropy of the plaintext images and the corresponding ciphertext images produced by the proposed 2D-HDDS-based scheme and compare the results with representative recent chaos-based ciphers, including [30] and [34]. Table 4 summarizes the results for three standard 512×512 grayscale test images.

Table 4. Shannon entropy (bits) of plaintext and ciphertext images. The ideal value for 8-bit randomness is $H_{\max} = 8$.

Image	Plain	2D-HDDS (proposed)	2D-CLSS [30]	2D-HELS [34]
Lena	7.2405	7.9993	7.9993	7.9934
Women	7.6321	7.9993	7.9993	7.9970
Boats	7.1238	7.9993	7.9993	7.9937

As shown in the table above, the ciphertext entropies produced by the proposed scheme are consistently close to the ideal upper bound of 8 bits and are competitive with (and in some cases slightly higher than) those obtained by the compared methods. This suggests that the proposed cipher effectively reduces first-order statistical regularities in gray-level distributions and generates ciphertext images with high apparent randomness, which is consistent with the near-uniform histogram behavior reported in Section 5.6. Although entropy alone does not constitute a security proof, these results provide supportive evidence that the proposed design achieves low statistical leakage with respect to intensity distributions.

5.8. Runtime and throughput evaluation

To complement the complexity analysis, we compare the runtime of the proposed scheme with two recent chaotic image encryption methods [12, 34] under the same MATLAB environment.

All tests were performed on a standard desktop computer equipped with a 3.20 GHz CPU and 16 GB RAM in MATLAB. The reported times exclude disk I/O and measure only the core

encryption/decryption procedures. For each test image, the runtime was measured by MATLAB timing functions (e.g., `tic`/`toc`) and averaged over repeated runs.

Six benchmark images with different resolutions were used: Lena and Clock (256×256), Baboon and Women (512×512), and Man and Airport (1024×1024). Since the proposed scheme consists of a constant number of full-image permutations, substitutions, and diffusion passes, its computational cost is expected to scale linearly with the number of pixels, i.e., $O(L)$ with $L = M \times N$ for grayscale images.

Table 5 summarizes the measured encryption and decryption times (T_{enc} and T_{dec}, in seconds) together with the corresponding throughput values for grayscale images of different sizes. Overall, the proposed scheme is consistently faster than both reference methods across all tested image sizes. In particular, it achieves a clear speed advantage over [12, 34], while its runtime grows approximately proportionally with the image size, which is consistent with the claimed linear-time behavior. These results indicate that the proposed design maintains good computational efficiency in addition to its security performance.

Table 5. Runtime and throughput comparison on standard hardware for grayscale images. Here, T denotes runtime (s), and R denotes throughput (MB/s), computed by $R = L/T$, where $L = M \times N$ bytes and $1\,\text{MB} = 10^6$ bytes.

Image	Size	Mode	Proposed		Ref. [34]		Ref. [12]	
			T (s)	R (MB/s)	T (s)	R (MB/s)	T (s)	R (MB/s)
Lena	256×256	Enc.	0.0775	0.8456	0.1593	0.4114	0.2239	0.2927
		Dec.	0.0773	0.8478	0.1559	0.4204	0.2238	0.2928
Clock	256×256	Enc.	0.0782	0.8381	0.1938	0.3382	0.2332	0.2810
		Dec.	0.0779	0.8413	0.1790	0.3661	0.2397	0.2734
Baboon	512×512	Enc.	0.3086	0.8495	0.6129	0.4277	0.9236	0.2838
		Dec.	0.3103	0.8449	0.6064	0.4323	0.9160	0.2862
Women	512×512	Enc.	0.3091	0.8481	0.6149	0.4263	0.9270	0.2828
		Dec.	0.3126	0.8386	0.6102	0.4296	0.9066	0.2892
Man	1024×1024	Enc.	1.2680	0.8269	2.4979	0.4198	3.6128	0.2902
		Dec.	1.2681	0.8269	2.4190	0.4335	3.6853	0.2845
Airport	1024×1024	Enc.	1.2523	0.8372	2.4770	0.4233	3.6628	0.2863
		Dec.	1.2494	0.8391	2.4523	0.4276	3.6775	0.2851

6. Conclusions

6.1. Summary of this work

This paper developed 2D-HDDS together with a corresponding chaos-driven image-encryption scheme. From the viewpoint of structural design, the proposed map combines exponential stretching and Chebyshev-polynomial folding through a nonlinear two-variable feedback coupling. Numerical experiments suggest that this construction admits a relatively broad parameter region with two positive Lyapunov exponents and yields a more uniform invariant distribution than the compared baseline cases, which is favorable for keystream generation in image encryption. Although nonlinear function composition and cross-coupling have been explored in a number of recent two-dimensional chaotic-

map designs, the present work provides a specific realization whose numerical behavior is consistent with the above dynamical features.

Based on the generated keystream, we designed an image cipher consisting of dual Fisher–Yates permutations, a key-dependent dynamic S-box, index-coupled bidirectional diffusion, and a lightweight two-pass avalanche booster. Experimental results indicate that the resulting scheme achieves a large effective key space, high key sensitivity, and good resistance to brute-force, statistical, and differential attacks under the tests considered in this paper. In particular, the combination of index-coupled diffusion and the booster helps enhance plaintext sensitivity, with the observed NPCR/UACI values remaining close to their theoretical reference levels while preserving practical computational efficiency.

6.2. Future perspective

First, lightweight implementations and hardware acceleration (e.g., Field Programmable Gate Arrays (FPGA) [22] and embedded deployments) are worth exploring to enable real-time secure imaging pipelines and resource-constrained applications. Since such platforms often rely on reduced-precision or fixed-point arithmetic, where digital chaos in general—including many chaotic maps used in image encryption—may evolve over a finite state space and suffer from dynamical degradation, such as short cycles or non-uniform state visitation, a more systematic finite-precision analysis would be worthwhile. In this regard, precision-aware design principles and effective anti-degradation mechanisms remain important topics for further study [9]. Second, it would also be of interest to extend the proposed framework to higher-dimensional and higher-bit-depth data, such as hyperspectral cubes or 16-bit medical images, while maintaining acceptable efficiency in practical secure-imaging applications [39].

Use of Generative-AI tools declaration

The author declares that no generative AI tools were used in the development of this manuscript.

Acknowledgments

The author would like to express her sincere gratitude to the editor and the reviewers for their careful reading, valuable comments, and constructive suggestions, which have significantly contributed to improving the quality and clarity of this paper.

Conflict of interest

The author declares that there are no conflicts of interest to disclose.

References

1. G. Álvarez, S. J. Li, Some basic cryptographic requirements for chaos-based cryptosystems, *Int. J. Bifurcat. Chaos*, **16** (2006), 2129–2151. http://dx.doi.org/10.1142/S0218127406015970

2. E. Barker, Recommendation for key management: Part 1–general, In: *NIST special publication 800-57 part 1 revision 5*, National Institute of Standards and Technology (NIST), 2020. http://dx.doi.org/10.6028/NIST.SP.800-57pt1r5

3. E. Barker, A. Roginsky, Transitioning the use of cryptographic algorithms and key lengths, In: *NIST Special Publication 800-131A Revision 2*, National Institute of Standards and Technology (NIST), 2019. http://dx.doi.org/10.6028/NIST.SP.800-131Ar2

4. G. Benettin, L. Galgani, A. Giorgilli, J.-M. Strelcyn, Lyapunov characteristic exponents for smooth dynamical systems and for Hamiltonian systems; a method for computing all of them. Part 1: theory, *Meccanica*, **15** (1980), 9–20. http://dx.doi.org/10.1007/BF02128236

5. G. Benettin, L. Galgani, A. Giorgilli, J.-M. Strelcyn, Lyapunov characteristic exponents for smooth dynamical systems and for Hamiltonian systems; a method for computing all of them. Part 2: numerical application, *Meccanica*, **15** (1980), 21–30. http://dx.doi.org/10.1007/BF02128237

6. A. Belazi, A. A. A. El-Latif, S. Belghith, A novel image encryption scheme based on substitution-permutation network and chaos, *Signal Process.*, **128** (2016), 155–170. http://dx.doi.org/10.1016/j.sigpro.2016.03.021

7. C. Chen, K. H. Sun, S. B. He, An improved image encryption algorithm with finite computing precision, *Signal Process.*, **168** (2020), 107340. http://dx.doi.org/10.1016/j.sigpro.2019.107340

8. P. Cheng, H. X. Zhao, A novel image encryption algorithm based on cellular automata and chaotic system, *Advanced Materials Research*, **998–999** (2014), 797–801. http://dx.doi.org/10.4028/www.scientific.net/AMR.998-999.797

9. C. L. Fan, Q. Ding, Analysis and resistance of dynamic degradation of digital chaos via functional graphs, *Nonlinear Dyn.*, **103** (2021), 1081–1097. http://dx.doi.org/10.1007/s11071-020-06160-x

10. Y. C. Fu, Z. H. Li, F. Huang, W. Ning, H. R. Lyu, Design of a fast image encryption algorithm based on a novel 2D chaotic map and DNA encoding, *Secur. Privacy*, **8** (2025), e70036. http://dx.doi.org/10.1002/spy2.70036

11. J. Fridrich, Symmetric ciphers based on two-dimensional chaotic maps, *Int. J. Bifurcat. Chaos*, **8** (1998), 1259–1284. http://dx.doi.org/10.1142/S021812749800098X

12. Q. S. Gao, X. Q. Zhang, Multiple-image encryption algorithm based on a new composite chaotic system and 3D coordinate matrix, *Chaos Soliton. Fract.*, **189** (2024), 115587. http://dx.doi.org/10.1016/j.chaos.2024.115587

13. L. H. Gong, K. D. Qiu, C. Z. Deng, N. R. Zhou, An image compression and encryption algorithm based on chaotic system and compressive sensing, *Opt. Laser Technol.*, **115** (2019), 257–267. http://dx.doi.org/10.1016/j.optlastec.2019.01.039

14. Z. Y. Hua, F. Jin, B. X. Xu, H. J. Huang, 2D Logistic-Sine-coupling map for image encryption, *Signal Process.*, **149** (2018), 148–161. http://dx.doi.org/10.1016/j.sigpro.2018.03.010

15. L. Kocarev, S. Lian, *Chaos-based cryptography: Theory, algorithms and applications*, Berlin-Heidelberg: Springer, 2011. http://dx.doi.org/10.1007/978-3-642-20542-2

16. A. Kumar, M. Dua, A novel exponent-sine-cosine chaos map-based multiple-image encryption technique, *Multimedia Syst.*, **30** (2024), 141. http://dx.doi.org/10.1007/s00530-024-01334-8

17. C. Q. Li, L. Y. Zhang, R. Ou, K.-W. Wong, S. Shu, Breaking a novel colour image encryption algorithm based on chaos, *Nonlinear Dyn.*, **70** (2012), 2383–2388. http://dx.doi.org/10.1007/s11071-012-0626-5

18. L. D. Liu, J. F. Hu, H. Y. Li, J. Li, Z. S. He, C. L. Han, Parameter estimation of a class of one-dimensional discrete chaotic systems, *Discrete Dyn. Nat. Soc.*, **2011** (2011), 696017. http://dx.doi.org/10.1155/2011/696017

19. Y. S. Liu, L. Y. Zhang, J. Wang, Y. S. Zhang, K.-W. Wong, Chosen-plaintext attack of an image encryption scheme based on modified permutation-diffusion structure, *Nonlinear Dyn.*, **84** (2016), 2241–2250. http://dx.doi.org/10.1007/s11071-016-2642-3

20. G. Q. Long, X. L. Chai, Z. H. Gan, D. H. Jiang, X. He, M. G. Sun, Exploiting one-dimensional exponential Chebyshev chaotic map and matching embedding for visually meaningful image encryption, *Chaos Soliton. Fract.*, **176** (2023), 114111. http://dx.doi.org/10.1016/j.chaos.2023.114111

21. R. Matthews, On the derivation of a "chaotic" encryption algorithm, *Cryptologia*, **13** (1989), 29–42. http://dx.doi.org/10.1080/0161-118991863745

22. M. Maazouz, A. Toubal, B. Bengherbia, O. Houhou, N. Batel, FPGA implementation of a chaos-based image encryption algorithm, *J. King Saud Univ.–Com.*, **34** (2022), 9926–9941. http://dx.doi.org/10.1016/j.jksuci.2021.12.022

23. H. Mouhsine, K. Mokni, M. Ch-Chaoui, Exploring multi-parameter bifurcations and immigration-driven dynamics in a discrete-time Bazykin–Berezovskaya prey-predator model, *Nonlinear Dyn.*, **113** (2025), 34101–34131. http://dx.doi.org/10.1007/s11071-025-11818-5

24. H. Mouhsine, H. B. Ali, K. Mokni, M. Ch-Chaoui, Dynamics unveiled: investigating bifurcations and the strong Allee effect in a discrete-time prey-predator system, *Int. J. Dynam. Control*, **13** (2025), 324. http://dx.doi.org/10.1007/s40435-025-01834-z

25. K. Mokni, H. Mouhsine, M. Ch-Chaoui, Multi-parameter bifurcations in a discrete Ricker-type predator-prey model with prey immigration, *Math. Comput. Simulat.*, **233** (2025), 39–59. http://dx.doi.org/10.1016/j.matcom.2025.01.020

26. P. K. Naskar, S. Bhattacharyya, D. Nandy, A. Chaudhuri, A robust image encryption scheme using chaotic Tent map and cellular automata, *Nonlinear Dyn.*, **100** (2020), 2877–2898. http://dx.doi.org/10.1007/s11071-020-05625-3

27. O. E. Rössler, An equation for hyperchaos, *Phys. Lett. A*, **71** (1979), 155–157. http://dx.doi.org/10.1016/0375-9601(79)90150-6

28. C. E. Shannon, Communication theory of secrecy systems, *Bell System Technical Journal*, **28** (1949), 656–715. http://dx.doi.org/10.1002/j.1538-7305.1949.tb00928.x

29. C. Skokos, The Lyapunov characteristic exponents and their computation, In: *Dynamics of small solar system bodies and exoplanets*, Berlin-Heidelberg: Springer, 2009, 63–135. http://dx.doi.org/10.1007/978-3-642-04458-8_2

30. L. Teng, X. Y. Wang, Y. J. Xian, Image encryption algorithm based on a 2D-CLSS hyperchaotic map using simultaneous permutation and diffusion, *Inform. Sciences*, **605** (2022), 71–85. http://dx.doi.org/10.1016/j.ins.2022.05.032

31. A. H. Tian, Z. Z. Yue, C. B. Fu, Image cryptography algorithm based on a new composite chaotic system and Latin square collaborative mechanism, *Opt. Laser. Eng.*, **193** (2025), 109084. http://dx.doi.org/10.1016/j.optlaseng.2025.109084
32. Q. Z. Wan, C. Y. Chen, T. Q. Liu, H. H. Rao, J. Dong, High-dimensional memristor-coupled multiple neural networks with spatial multi-structure attractors and application in image encryption, *Chaos. Soliton. Fract.*, **199** (2025), 116716. http://dx.doi.org/10.1016/j.chaos.2025.116716
33. B. Wang, X. P. Wei, Q. Zhang, Cryptanalysis of an image cryptosystem based on Logistic map, *Optik*, **124** (2013), 1773–1776. http://dx.doi.org/10.1016/j.ijleo.2012.06.020
34. M. X. Wang, X. P. Fu, L. Teng, X. P. Yan, Z. Q. Xia, P. B. Liu, A new 2D-HELS hyperchaotic map and its application on image encryption using RNA operation and dynamic confusion, *Chaos Soliton. Fract.*, **183** (2024), 114959. http://dx.doi.org/10.1016/j.chaos.2024.114959
35. M. X. Wang, L. Teng, W. J. Zhou, X. P. Yan, Z. Q. Xia, S. Zhou, A new 2D cross hyperchaotic Sine-modulation-Logistic map and its application in bit-level image encryption, *Expert Syst. Appl.*, **261** (2025), 125328. http://dx.doi.org/10.1016/j.eswa.2024.125328
36. M.-M. Wang, X.-G. Song, S.-H. Liu, X.-Q. Zhao, N.-R. Zhou, A novel 2D Log-Logistic-Sine chaotic map for image encryption, *Nonlinear Dyn.*, **113** (2025), 2867–2896. http://dx.doi.org/10.1007/s11071-024-10331-5
37. P. Y. Wang, Y. Xiang, L. L. Huang, A novel image encryption scheme based on a quantum Logistic map, hyper-chaotic Lorenz map, and DNA dynamic encoding, *Electronics*, **14** (2025), 2092. http://dx.doi.org/10.3390/electronics14102092
38. A. Wolf, J. B. Swift, H. L. Swinney, J. A. Vastano, Determining Lyapunov exponents from a time series, *Physica D*, **16** (1985), 285–317. http://dx.doi.org/10.1016/0167-2789(85)90011-9
39. S. Xiao, S. Xu, Z. Chen, Hyperchaotic encryption scheme for hyperspectral images using 3D Zigzag-like transformation and brushing diffusion, *Multimedia Tools Appl.*, **83** (2024), 67371–67405. http://dx.doi.org/10.1007/s11042-023-17970-7
40. Y. X. Zheng, Q. Y. Huang, S. T. Cai, X. M. Xiong, L. Q. Huang, Image encryption based on novel Hill cipher variant and 2D-IGSCM hyper-chaotic map, *Nonlinear Dyn.*, **113** (2025), 2811–2829. http://dx.doi.org/10.1007/s11071-024-10324-4
41. U. Zia, M. McCartney, B. Scotney, J. Martinez, M. AbuTair, J. Memon, et al., Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains, *Int. J. Inf. Secur.*, **21** (2022), 917–935. http://dx.doi.org/10.1007/s10207-022-00588-5
42. S. L. Zhu, X. H. Deng, W. D. Zhang, C. X. Zhu, Image encryption scheme based on newly designed chaotic map and parallel DNA coding, *Mathematics*, **11** (2023), 231. http://dx.doi.org/10.3390/math11010231
43. N. R. Zhou, S. M. Pan, S. Cheng, Z. H. Zhou, Image compression-encryption scheme based on hyper-chaotic system and 2D compressive sensing, *Opt. Laser Technol.*, **82** (2016), 121–133. http://dx.doi.org/10.1016/j.optlastec.2016.02.018
44. R. Zhou, S. M. Yu, Break an enhanced plaintext-related chaotic image encryption algorithm, *Chaos Soliton. Fract.*, **181** (2024), 114623. http://dx.doi.org/10.1016/j.chaos.2024.114623

45. N. R. Zhou, J. P. Yang, C. F. Tan, S. M. Pan, Z. H. Zhou, Double-image encryption scheme combining DWT-based compressive sensing with discrete fractional random transform, *Opt. Commun.*, **354** (2015), 112–121. http://dx.doi.org/10.1016/j.optcom.2015.05.043

AIMS Press

© 2026 the Author(s), licensee AIMS Press. This is an open access article distributed under the terms of the Creative Commons Attribution License (https://creativecommons.org/licenses/by/4.0)