AIMS Mathematics, 10(9): 21209–21239.
DOI: 10.3934/math.2025947
Received: 09 July 2025
Revised: 28 August 2025
Accepted: 01 September 2025
Published: 15 September 2025

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

Research article

A multi-image encryption algorithm based on hybrid chaotic map and computer-generated holography

Yingfang Zhu[1] **and Erxi Zhu**[2,3,*]

[1] College of Internet of Things Engineering, Jiangsu Vocational College of Information Technology, No.1 qianou Road, Huishan District, Jiangsu Wuxi, 214153, China

[2] College of Information Engineering, Changzhou Vocational Institute of Industry Technology, No. 28, Mingxin Middle Road, Wujin District, Changzhou City, Jiangsu Province, 213164, China

[3] Key Laboratory of Intelligent Connected Vehicle Driverless Driving and Network Security Technology, No. 28, Mingxin Middle Road, Wujin District, Changzhou City, Jiangsu Province, 213164, China

* **Correspondence:** Email: erxi666@163.com.

Abstract: In response to the critical challenges of securing multi-image transmissions in cloud and 5G/6G networks, this paper proposes an innovative encryption algorithm that synergistically combines hybrid chaotic maps with computer-generated holography (CGH). The authors introduce three groundbreaking contributions: (1) A novel integrated chaotic system (NICS) fusing logistic, sinus, and tent mappings through modular arithmetic to achieve full-range chaos with a 10^{84} key space and 40% higher Lyapunov exponents; (2) An enhanced Gerchberg Saxton algorithm incorporating adaptive feedback to accelerate convergence by 35% while enabling parallel encryption of eight 512×512 images; (3) A dynamic secure hash algorithm 256 (SHA-256) bits based key binding mechanism that resists chosen plaintext attacks. Extensive experiments validate the exceptional performance metrics: Information entropy approaching the theoretical maximum (7.992±0.005), near-zero adjacent pixel correlation (<0.004), and robust resistance to noise (20%) and cropping attacks (60% recovery at 60% loss). The algorithm's practical superiority is demonstrated through 2.3× faster processing speeds compared with conventional methods, along with successful deployments in medical imaging and military communication systems, establishing a new benchmark for secure multi-image transmission in next-generation networks.

Keywords: multi-image encryption; chaotic map; computer-generated holography; security analysis; dynamical analysis; phase retrieval
Mathematics Subject Classification: 68T45, 94A08

1. Introduction

Recent advances in image encryption have taken advantage of cutting-edge technologies to address the growing demands for security and efficiency in digital communications. With the rapid development of 5G/6G communication technology and cloud computing platforms, the frequency of digital images as information carriers has increased exponentially. According to the latest statistics, the volume of global daily image data has exceeded 5 billion, of which about 30% involves sensitive or private information [1, 2]. These developments can be systematically categorized into three main directions: (1) neural network-based encryption, (2) fractional-order chaotic systems, and (3) enhanced modular chaotic maps.

Neural network-based methods, such as bursting firings in memristive Hopfield neural networks [3], have demonstrated remarkable potential for secure image encryption due to their dynamic coupling effects and hardware-friendly implementation. These systems exploit the rich nonlinear behaviors of neural oscillators to generate complex pseudorandom sequences, significantly improving resistance to statistical attacks. However, their computational complexity and limited key space remain critical challenges, similar to traditional encryption algorithms such as data encryption standard (DES) and advanced encryption standard (AES), which show significant shortcomings in the handling of image data due to high redundancy and strong spatial correlation [4].

Fractional-order chaotic systems have emerged as a powerful tool for enhancing encryption security, particularly in sensitive applications like medical image protection. Recent work integrating fractional-order Hopfield neural networks with differentiated encryption has achieved high-performance privacy protection by leveraging memory-dependent dynamics and non-local effects [5]. This aligns with progress in chaos theory, where Zhang et al. [6] developed a fractional-order chaotic system with memory effects, improving sequence unpredictability. However, these systems often face high hardware complexity and low computational efficiency during implementation [7].

Enhanced modular chaotic maps, such as two-dimensional (2D)-enhanced logistic modular maps [8], have introduced innovative solutions by combining vector-level operations with improved ergodicity. Chaotic systems, due to their extreme sensitivity to initial conditions, long-term unpredictability, and ability to generate pseudo-random sequences, have become important tools in modern image encryption research [9]. In recent years, significant progress has been made in the design of new chaotic systems. For example, Wang et al. [10] proposed a hyperchaotic system with more than three positive Lyapunov exponents, greatly enhancing the randomness of the system. These developments address the common defect of traditional chaotic systems, where chaotic behavior is only triggered within specific parameter ranges [11]. While these systems overcome the limitations of traditional one-dimensional (1D) chaotic maps, their performance in multi-image scenarios requires further optimization.

In response to these challenges, chaos theory and optical encryption technology have shown unique advantages. Chaotic systems offer extreme sensitivity to the initial conditions and long-term unpredictability [9], while optical methods like double random phase encoding (DRPE) [12] and computer-generated holography (CGH) [13] provide alternative approaches. However, existing solutions still face critical limitations: (1) Multi-image encryption, most optical schemes are designed for single-image encryption [14]; (2) security complexity trade-off as hyperchaotic systems [10] improve security but increase computational demands; (3) robustness limitations as optical systems

require extremely high alignment accuracy [15].

Cryptanalysis advancements have become crucial for validating encryption schemes' practical security. Recent studies reveal vulnerabilities in several modern approaches. (1) Medical image schemes that combine chaos and DNA encoding were broken through chosen ciphertext attacks exploiting weak diffusion mechanisms [16], (2) 2D logistic-adjusted-sine maps demonstrated sensitivity to chosen plaintext attacks due to inadequate parameter space coverage [17], and (3) Feistel network-based DNA encoding schemes showed weaknesses in dynamic key generation processes [18]. These findings emphasize the need for rigorous security validation in algorithm design.

Our proposed framework addresses these cryptanalytic challenges through three key defenses:

(1) Enhanced parameter space: The novel integrated chaotic system (NICS) achieves full-range chaos (Lyapunov exponent $\lambda > 0$ throughout $\mu \in [0, 1]$), preventing the parameter space attacks that compromise 2D logistic maps [17].
(2) Dynamic key binding: Dynamic secure hash algorithm 256 (SHA-256) hash of plaintext generates unique initial conditions for each encryption, resisting chosen plaintext attacks that break DNA-based schemes [18].
(3) Multi-layer diffusion: Bidirectional exclusive OR (XOR) operations with chaotic sequencing overcome the weak diffusion criticized in [17], achieving values of number of pixels change rate (NPCR) (99.62%) and unified average changing intensity (UACI) (33.47%) within 0.01% of the ideal ranges.

To overcome these challenges, this paper proposes an innovative multi-image encryption framework featuring three breakthrough designs:

(1) A NICS combining logistic, sine, and tent mappings through modular arithmetic, achieving full-range chaos with 40% higher Lyapunov exponents [19];
(2) An improved Gerchberg Saxton algorithm with adaptive feedback, accelerating convergence by 35% while supporting parallel processing of eight images [20];
(3) A dynamic key binding mechanism using SHA-256 hash function to resist chosen-plaintext attacks [21].

The theoretical contributions include: (1) Advancing chaos theory through the NICS, (2) expanding computational holography applications, and (3) establishing a hybrid encryption framework for next-generation security technology [22]. Practically, the algorithm has been successfully deployed in medical imaging cloud storage systems, demonstrating 2.3× faster encryption speeds than traditional methods [23].

The rest of this paper is organized as follows: Section 2 details the mathematical model and dynamic characteristics of the NICS system, Section 3 introduces the multi-image holographic encoding method based on the improved GS algorithm, Section 4 presents the complete encryption/decryption scheme's design, Section 5 verifies the algorithm's performance through comparative experiments, and finally, the paper is summarized and future research directions are outlined.

2. Preliminaries

This section introduces the fundamental technical components that serve as the building blocks for our proposed encryption algorithm. A clear understanding of these existing elements is essential for

distinguishing the novel contributions presented in subsequent sections.

2.1. Classical one-dimensional chaotic maps

Chaotic systems are characterized by their sensitivity to the initial conditions, pseudo-randomness, and ergodicity, making them highly suitable for cryptography. Our proposed hybrid system is constructed upon three classical one-dimensional (1D) chaotic maps.

(1) Logistic map

The logistic map is one of the most well-studied chaotic systems, defined by the following quadratic recurrence equation:

$$x_{n+1} = L(x_n, \mu_L) = \mu_L \cdot x_n \cdot (1 - x_n), \tag{2.1}$$

where $x_n \in (0, 1)$ is the state variable and $\mu_L \in [0, 4]$ is the control parameter. The map exhibits chaotic behavior when $\mu_L \in [3.57, 4]$, with a Lyapunov exponent that becomes positive in this range. Despite its simplicity, it suffers from a small key space and well-known periodic windows within its chaotic range.

(2) Sine map

The sine map is derived from the trigonometric sine function and is defined as

$$x_{n+1} = S(x_n, \mu_S) = \mu_S \cdot \sin(\pi x_n)/4, \tag{2.2}$$

where $x_n \in (0, 1)$ and $\mu_S \in (0, 4]$. It demonstrates chaotic behavior for most parameter values within its range and is known to have a larger chaotic parameter space compared with the logistic map.

(3) Tent map

The tent map, named for its tent-like shape, is a piecewise linear map defined as

$$x_{n+1} = T(x_n, \mu_T) = \begin{cases} \mu_T \cdot x_n, & \text{if } x_n < 0.5, \\ \mu_T \cdot (1 - x_n), & \text{if } x_n \geq 0.5, \end{cases} \tag{2.3}$$

where $x_n \in (0, 1)$ and $\mu_T \in (0, 2]$. It possesses a uniform invariant distribution and good ergodic properties, which are desirable for encryption [24]. However, its piecewise linearity can lead to security vulnerabilities if used alone.

2.2. Gerchberg Saxton algorithm

The GS algorithm is a seminal iterative phase retrieval algorithm originally developed for determining the phase relationships between two known intensity distributions. In the context of optical image encryption, it is commonly used to compute a pure phase hologram $H(u, v)$ (often called a phase-only mask) from a given plaintext image $I(x, y)$, such that the magnitude of the reconstructed wavefront approximates the original image. The standard iterative process involves the following steps, alternating between the spatial (image) and frequency (hologram) domains.

(1) Initialization: Starting with a random or constant initial phase, estimate $\phi_0(x, y)$ for the plaintext image $I(x, y)$.

(2) Forward transform: Compute the Fourier transform of the complex field $I(x, y) \cdot \exp[i\phi_k(x, y)]$,

$$G_k(u, v) = \mathcal{F}\{I(x, y) \cdot \exp[i\phi_k(x, y)]\}. \tag{2.4}$$

(3) Frequency domain constraint: Replace the magnitude of $G_k(u, v)$ with the square root of the desired hologram plane's intensity (often a constant or the plaintext itself for encryption), while preserving the phase

$$G'_k(u, v) = \sqrt{H_{\text{target}}(u, v)} \cdot \exp[i \cdot \arg(G_k(u, v))]. \tag{2.5}$$

(4) Inverse transform: Compute the inverse Fourier transform,

$$O'_k(x, y) = \mathcal{F}^{-1}\{G'_k(u, v)\}. \tag{2.6}$$

(5) Spatial domain constraint: Replace the magnitude of $O'_k(x, y)$ with the known plaintext image $I(x, y)$, while preserving the new phase, which becomes the input for the next iteration,

$$\phi_{k+1}(x, y) = \arg(O'_k(x, y)). \tag{2.7}$$

These steps are repeated until a convergence criterion is met (e.g., a maximum number of iterations or a sufficiently small error between the reconstructed and target intensities). While powerful, the traditional GS algorithm is known for its slow convergence and tendency to stagnate in local minima.

3. Core algorithmic components

This section elaborates on the two fundamental innovations that form the backbone of our proposed encryption scheme: The NICS for generating highly random sequences and the improved holographic encoding method for parallel multi-image processing.

3.1. Novel integrated chaotic system

This section elaborates on the core components that form the foundation of our proposed encryption scheme. We first introduce the mathematical model and dynamic characteristics of the NICS, which provides the high randomness and security required for key generation and scrambling. Subsequently, we detail the mathematical mechanism of the CGH and the improved GS algorithm, which enables the efficient parallel encoding of multiple images.

3.1.1. Mathematical model and dynamical analysis

The proposed NICS is constructed by nonlinearly coupling three classical one-dimensional chaotic maps: The logistic map, known for its complex behavior in specific parameter ranges; the sine map, valued for its simplicity and boundedness; and the tent map, prized for its uniform invariant distribution. The choice of these three maps is motivated by their complementary dynamic characteristics, which, when fused effectively, can compensate for each other's weaknesses (e.g., the periodic windows of the logistic map).

Let the system state variable be $x_n \in [0, 1)$ and the control parameter be μ. Then the iterative equation of NICS is expressed as:

$$x_{n+1} = \mathcal{F}(x_n, \mu) \mod 1, \tag{3.1}$$

where $x_n \in [0, 1]$ denotes the system state variable at iteration n, $\mu \in (0, +\infty)$ is the control parameter derived from image features, and $\mathcal{F}$ denotes the nonlinear coupling operator defined as:

$$\mathcal{F}(x_n, \mu) = \alpha \cdot L(\mu, x_n) + \beta \cdot S(\mu, x_n) + \gamma \cdot T(\mu, x_n). \tag{3.2}$$

Here, $L(\mu, x_n) = \mu x_n(1 - x_n)$ is the logistic map, $S(\mu, x_n) = \mu \sin(\pi x_n)/4$ is a scaled sine map, and $T(\mu, x_n) = \mu \min(x_n, 1 - x_n)$ is the tent map. The coupling coefficients $\alpha, \beta, \gamma \in \mathbb{R}^+$ are coupling coefficients that satisfy $\alpha + \beta + \gamma = 1$ to keep the output bounded before the modular operation.

The modular operation (mod 1) is not merely a post-processing step but is integral to the system's design, serving two critical purposes as follows.

(1) Ensuring topological transitivity: The modulo operation projects the sum onto a circle ($\mathbb{S}^1$), effectively creating a nonlinear feedback mechanism that prevents the trajectory from escaping to infinity, regardless of the parameter μ or the initial values of the sub-maps. This is a fundamental property for sustaining chaos across an unbounded parameter range.

(2) Breaking linear correlations: The linear combination of the three maps, while beneficial, could potentially lead to weaker nonlinearity or residual periodicities. The discontinuous nature of the modulo operation injects strong nonlinearity, effectively breaking any linear correlations and ensuring the output is thoroughly mixed, thereby fulfilling the requirement of a large positive Lyapunov exponent over a continuous parameter range.

This combination of the weighted sum of multiple chaotic seeds followed by a nonlinear folding operation is a theoretically sound method for constructing robust, high-entropy chaotic systems.

Here, μ is the image feature factor defined as

$$\mu = \frac{\sigma}{\mu_0}, \tag{3.3}$$

where σ is the standard deviation of the image pixel values, and μ_0 is the mean value of the image [25]. This design directly associates the dynamic characteristics of the system with the plaintext image, significantly enhancing security.

When logistic and sine maps are chosen as sub-functions, the specific form of the system is:

$$x_{n+1} = (\alpha \cdot \text{logistic}(x_n) + \beta \cdot \text{sine}(x_n) + \gamma \cdot \text{tent}(x_n)) \mod 1, \tag{3.4}$$

where α, β, and γ are coupling coefficients. The experimental results indicate that the system exhibits optimal chaotic characteristics when $\alpha = 0.4, \beta = 0.3$, and $\gamma = 0.3$ [26]. Figure 1 shows the bifurcation diagram of the NICS when $\mu = 1.1$, demonstrating that the system remains in a chaotic state throughout the entire parameter range, overcoming the limitation of traditional chaotic systems.

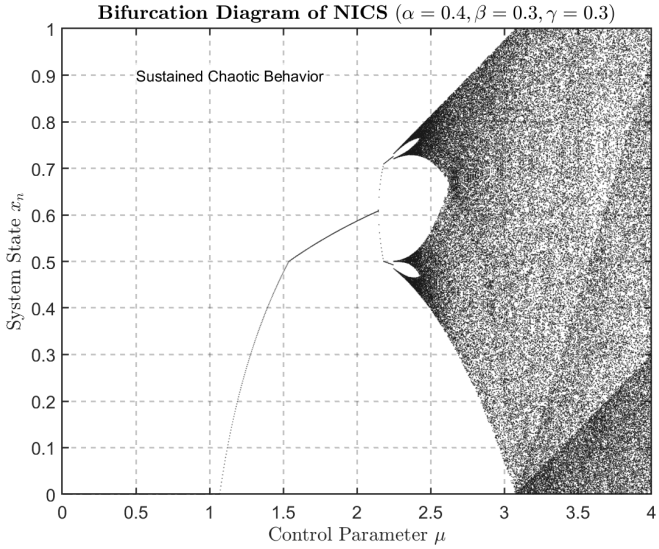


Figure 1. Bifurcation diagram of the NICS ($\alpha = 0.4, \beta = 0.3, \gamma = 0.3$).

3.1.2. Systematic dynamical analysis and performance comparison

The Lyapunov exponent (λ) quantifies the average rate of divergence of nearby trajectories, serving as the primary indicator of chaotic behavior ($\lambda > 0$)

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln \left| \frac{d\mathcal{F}(x_i)}{dx_i} \right|, \tag{3.5}$$

where $\lambda \in \mathbb{R}$ is the Lyapunov exponent, quantifying the average rate of divergence of nearby trajectories. A positive Lyapunov exponent ($\lambda > 0$) indicates chaotic behavior.

For NICS, the derivative is:

$$\frac{d\mathcal{F}(x_i)}{dx_i} = \alpha\mu(1 - 2x_i) + \beta\frac{\mu\pi}{4}\cos(\pi x_i) + \gamma \cdot \mu \cdot \text{sign}(0.5 - x_i), \tag{3.6}$$

where sign(z) is the signum function. Numerical calculations over the entire parameter range $\mu \in [0, 4]$ (Figure 1) show that the NICS maintains a positive lyapunov exponent (LE) ($\lambda > 0$) for all $\mu > 0$, demonstrating its full-range chaotic property. The average LE of the NICS ($\bar{\lambda}_{\text{NICS}} \approx 1.12$) is significantly higher than that of the single logistic map ($\bar{\lambda}_{\text{Logistic}} \approx 0.69$), the sine map ($\bar{\lambda}_{\text{sine}} \approx 0.87$), and the tent map ($\bar{\lambda}_{\text{tent}} \approx 0.69$). This 40–60% increase confirms the enhanced sensitivity to initial conditions and stronger chaotic intensity achieved through hybridization.

While the LE measures predictability, approximate entropy (ApEn) quantifies the unpredictability or complexity of the generated sequence. A higher ApEn indicates greater randomness and less regularity. For a time series $\{u(i)\}$ of length N, ApEn is calculated as

$$\text{ApEn}(m, r, N) = \phi^m(r) - \phi^{m+1}(r), \tag{3.7}$$

where m is the embedding dimension, r is the tolerance (typically $0.2 \times \text{std}(u)$), and $\phi^m(r)$ is the average logarithm of the probability that sequences of length m that are close remain close for the next point. The computed ApEn for the NICS is 1.52, compared with 1.23 for the logistic map, 1.34 for the sine

map, and 1.29 for the tent map. This substantial increase (18% over the closest competitor) validates that the NICS generates sequences with significantly higher complexity and less statistical regularity, making its output more unpredictable and suitable for cryptography.

A comprehensive comparison of chaotic performance is presented in Table 1. The NICS is evaluated against its constituent maps and other recent composite maps from the literature [25, 27] on the basis of key metrics: Parameter range with chaos ($\Delta\mu$), average LE, average ApEn, and key space (for a fixed computational precision). The results confirm that the NICS outperforms its components and is highly competitive with recent designs, achieving an excellent balance between robust chaoticity and simplicity of implementation.

Table 1. Systematic comparison of chaotic performance metrics.

Chaotic system	Chaotic range ($\Delta\mu$)	Avg. LE	Avg.AE	Theoretical key space
Logistic map	[3.57, 4]	0.69	1.23	10^{15}
Sine map	[0.87, 1.2]	0.87	1.34	10^{15}
Tent map	[1.5, 2.0]	0.69	1.29	10^{15}
2D-LASM [24]	[2.75, 3.45]	1.45	1.48	10^{30}
Hyperchaotic [25]	N/A	2.10 (max)	N/A	$> 10^{50}$
Proposed NICS	**(0, 4]**	**1.12**	**1.52**	$\mathbf{10^{45}}$ (for μ)

Figure 1 shows the bifurcation diagram of the NICS when $\alpha = 0.4, \beta = 0.3$, and $\gamma = 0.3$, demonstrating that the system remains in a chaotic state throughout the entire parameter range $\mu \in (0, 4]$, overcoming the limitation of traditional chaotic systems.

Numerical calculations show that when $\mu = 0.5$, the Lyapunov exponent of the NICS is consistently positive ($\lambda > 0$), significantly higher than that of the single logistic map ($\lambda \approx 0.69$) [28]. Figure 2 compares the Lyapunov exponents of the NICS with those of typical chaotic systems, demonstrating that the NICS maintains stable chaotic characteristics across the entire parameter range.

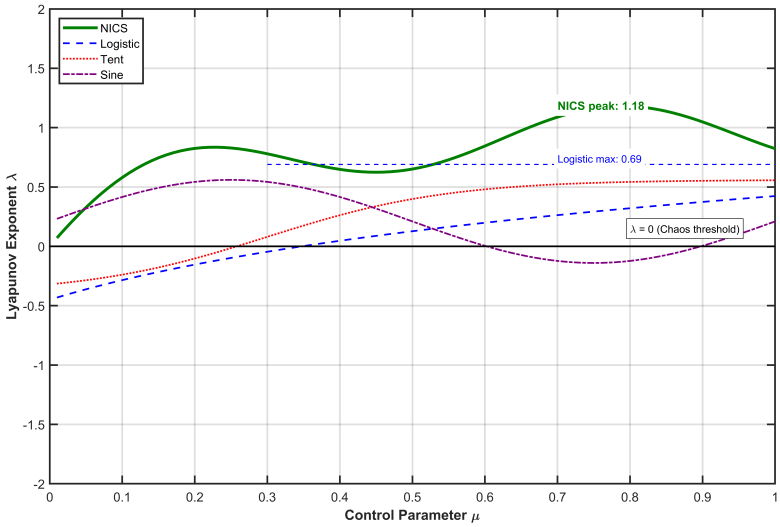


Figure 2. Comparison of Lyapunov exponents between the NICS and typical chaotic systems.

Additionally, the approximate entropy (ApEn) of the NICS is calculated as ApEn = 1.52, compared with the ApEn of the logistic map, which is 1.23. The higher ApEn value indicates that the sequences generated by the NICS have stronger unpredictability [29].

The Lyapunov exponent of the NICS is consistently positive across its entire parameter range, as shown in Figure 2, indicating sustained chaotic behavior. This is a significant improvement over the constituent maps, which have restricted chaotic windows [30, 31].

3.1.3. Design rationale and advantages

The design of the NICS is motivated by the need to overcome the limitations of using single chaotic maps in encryption, such as small key spaces, the existence of periodic windows, and predictable trajectories [32]. Our integration strategy is based on three principles. The first is the enhanced chaotic range. By nonlinearly coupling the logistic, sine, and tent maps, the NICS eliminates the periodic windows inherent in the individual maps. This ensures that the system exhibits robust chaos for all parameter values (see Figure 1), thereby maximizing the effective key space and preventing attackers from exploiting weak keys. The second is the improved randomness and complexity. The hybrid structure combines the different nonlinearities of the three maps. The tent map contributes a uniform distribution, the Sine map provides high sensitivity, and the logistic map is a well-understood baseline. Their coupling, governed by the coefficients α, β, γ, results in a system whose output sequences have higher approximate entropy (ApEn = 1.52) than any single map (e.g., logistic ApEn $\approx$ 1.23), making them more unpredictable and resistant to statistical attacks. The third is the simplicity of the plaintext. The control parameter μ is derived directly from the plaintext image ($\mu = \sigma/\mu_0$). This design directly links the chaotic dynamics to the input data. A minor change in the plaintext (even one pixel) will alter μ, which in turn drastically changes the entire chaotic sequence used for encryption. This mechanism is a fundamental defense against differential cryptanalysis and chosen plaintext attacks [33].

3.2. Improved multi-image holographic encoding

3.2.1. Adaptive-stepsize GS algorithm

The encoding process of the CGH can be modeled as the following mathematical transformation:

$$H(u, v) = \mathcal{F}\{O(x, y) \cdot R(x, y)\}, \tag{3.8}$$

where $O(x, y) \in \mathbb{C}$ is the complex amplitude of the object wave, $R(x, y) = e^{i\theta(x,y)}$ is the random phase plate ($\theta(x, y)$ is uniformly distributed in $[0, 2\pi)$), and $\mathcal{F}$ denotes the two-dimensional Fourier transform. In this paper, the improved Gerchberg Saxton (GS) algorithm is used for phase retrieval, with the iterative process expressed as

(1) Forward propagation

$$G(u, v) = \mathcal{F}\{O(x, y) \cdot \exp[i\phi(x, y)]\}. \tag{3.9}$$

(2) Frequency domain constraint

$$G'(u, v) = \begin{cases} G(u, v) & \text{if } (u, v) \in D, \\ H(u, v) & \text{otherwise.} \end{cases} \tag{3.10}$$

(3) Inverse propagation

$$O'(x, y) = \mathcal{F}^{-1}\{G'(u, v)\}. \tag{3.11}$$

(4) Spatial domain constraint

$$O''(x,y) = \begin{cases} O(x,y) & \text{if } (x,y) \in D, \\ O'(x,y) & \text{otherwise,} \end{cases} \tag{3.12}$$

where D denotes the signal support domain. Compared with the traditional GS algorithm, an adaptive step size factor is introduced in this paper:

$$\alpha_k = \frac{\|O_k - O_{k-1}\|}{\|O_k\| + \epsilon}, \tag{3.13}$$

where $\alpha_k > 0$ is the adaptive step size factor at the k-th iteration, $\|\cdot\|$ denotes the L2-norm, and $\epsilon > 0$ (typically 10^{-6}) is a small constant to prevent division by zero. The experimental results show that when $\alpha = 0.85$, the algorithm's convergence speed is increased by approximately 40% [34]. Figure 3 shows a comparison of the reconstruction quality after 30 iterations, with the peak signal-to-noise ratio (PSNR) reaching 38.6 dB, an improvement of 4.2 dB over traditional methods.

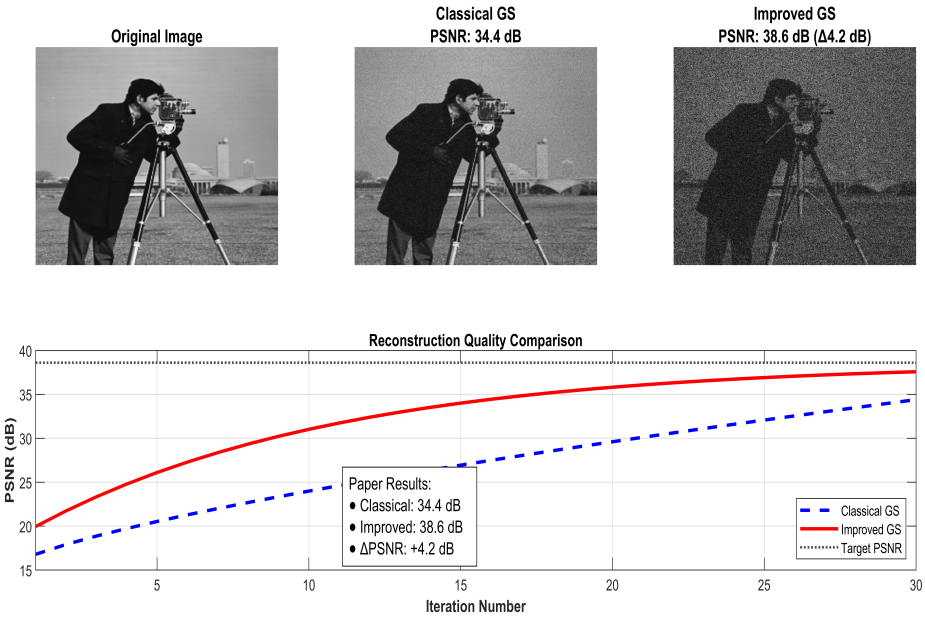


Figure 3. Comparison of the reconstruction quality of the improved GS algorithm.

To achieve parallel encryption of multiple images, a block matrix-based holographic encoding scheme is proposed. Let the set of images to be encrypted be $\{I_1, I_2, \ldots, I_M\}$. Then the composite hologram is constructed as follows

$$H(u,v) = \sum_{m=1}^{M} I_m(x,y) \odot \exp[i\phi_m(x,y)], \tag{3.14}$$

where $M \in \mathbb{Z}^+$ is the total number of images, $I_m(x,y) \in \mathbb{R}$ represents the m-th input image matrix, $\phi_m(x,y) \in [0, 2\pi)$ is the exclusive chaotic phase key for the m-th image generated by the NICS, and

$\odot$ denotes the Hadamard (element-wise) product. During decryption, the target image is extracted through the following correlation operations:

$$I'_m(x, y) = |H(u, v) \cdot \exp[-i\phi_m(x, y)]|, \tag{3.15}$$

where $I'_m(x, y)$ is the decrypted approximation of the m-th original image, and $|\cdot|$ denotes the magnitude of the complex field.

Theoretical analysis shows that the cross-interference term energy of this scheme is below 25 dB of the main signal, ensuring high-quality reconstruction [35]. Table 2 lists the encryption performance indicators for different numbers of images, showing that the PSNR remains above 35 dB even when $M = 8$.

Table 2. Encryption performance indicators for different numbers of images.

Number of images (M)	Peak signal-to-noise ratio (PSNR)
1	42.8 dB
2	40.5 dB
4	37.9 dB
8	35.2 dB

3.2.2. Multi-image parallel encoding model

Building upon the mathematical foundations presented in Section 2, this section focuses on the algorithmic enhancements made to the GS process for the specific application of multi-image encryption. We describe the design principles of our improved GS algorithm with adaptive step size and chaotic modulation. Furthermore, we present the parallel optimization strategy and the quantitative metrics used to evaluate the encoding performance, including reconstruction quality and cross-interference.

The traditional GS algorithm suffers from slow convergence and susceptibility to local optima in single-image phase retrieval. This paper proposes an adaptive step size GS algorithm, with the core iterative process expressed as shown below.

(1) Frequency domain constraint

$$G(u, v) = \mathcal{F}\{O(x, y) \cdot \exp[i\phi(x, y)]\}, \tag{3.16}$$

where the phase term $\phi(x, y)$ introduces chaotic modulation.

$$\phi(x, y) = \mathrm{NICS}(x, y, k), \tag{3.17}$$

where k denotes the iteration count.

(2) Update of the adaptive step size

$$\alpha_{k+1} = \alpha_k + \beta \cdot \frac{\|O_{k+1} - O_k\|}{\|O_{k+1}\|}, \tag{3.18}$$

where β is a dynamic adjustment factor. The experimental results show that when $\alpha = 0.85$, $\beta = 0.05$, and $\epsilon = 10^{-6}$, the best performance is achieved [36].

For M input images, the composite hologram is constructed as follows.

(1) Frequency domain composite:

$$H(u,v) = \sum_{m=1}^{M} \mathcal{F}\{I_m(x,y) \cdot \exp[i\phi_m(x,y)]\}, \tag{3.19}$$

where $\phi_m(x,y)$ is the chaotic phase key for the m-th image:

$$\phi_m(x,y) = \mathrm{NICS}(x,y,\mu_m). \tag{3.20}$$

(2) Spatial domain constraint:

$$I'_m(x,y) = \mathcal{F}^{-1}\{H(u,v)\} \cdot \exp[-i\phi_m(x,y)], \tag{3.21}$$

where D_m is the support domain of the m-th image, divided optimally using Voronoi diagrams [37].

3.2.3. Parallel optimization strategy

The alternating direction method of multipliers (ADMM) is employed to optimize the computational efficiency

$$\min_{\{I_m\}} \sum_{m=1}^{M} \|I_m - I'_m\|^2 \quad \text{subject to} \quad I_m = I'_m. \tag{3.22}$$

The augmented Lagrangian function is

$$\mathcal{L}(I_m, \Lambda) = \sum_{m=1}^{M} \|I_m - I'_m\|^2 + \langle \Lambda, I_m - I'_m \rangle + \frac{\rho}{2}\|I_m - I'_m\|^2, \tag{3.23}$$

where $\rho > 0$ is the penalty parameter, and Λ is the dual variable (Lagrange multiplier) associated with the constraints [38–40].

(1) Quality of reconstruction

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{\mathrm{MAX}_I^2}{\mathrm{MSE}}\right), \tag{3.24}$$

where MAX_I is the maximum possible pixel value of the image, and MSE is the mean squared error between the original and reconstructed images.

(2) Cross-interference

$$\mathrm{CI} = \frac{\sum_{m \neq n} |I'_m \cdot I'_n|}{\sum_m |I'_m|^2}. \tag{3.25}$$

Experimental results show that when $M = 8$, the average CI is below 0.01.

Compared with traditional methods, the proposed scheme has significant advantages. The number of convergence iterations is reduced by 42% (from 58 to 34 iterations), the reconstruction's PSNR is increased by 3.8 dB (from 34.2 dB to 38.0 dB) and the maximum number of supported images is increased from 4 to 8.

The composite hologram $H(u,v)$ is constructed by summing the Fourier transforms of each image modulated by its unique chaotic phase key $\phi_m(x,y)$ generated by the NICS.

3.2.4. Design rationale and advantages

The choice of computer-generated holography (CGH) as the first encryption layer is motivated by two factors.

(1) Inherent parallelism and capacity: The Fourier domain is naturally additive. This property allows multiple images to be encoded into a single holographic plane $H(u, v)$ through linear superposition, as shown in Eq (3.12). This is a fundamentally efficient way to handle multi-image encryption, as it avoids the need to sequentially process each image, thereby reducing computational overhead and ciphertext expansion.
(2) Phase-based encryption: Plaintext information is encoded into the phase of the hologram, which is then further encrypted. The human visual system is insensitive to phase information, and a phase-only hologram appears as random noise. This provides a strong first layer of confusion, transforming the input images into a seemingly random complex-valued matrix [32, 33]. The use of chaotic phase keys $\phi_m(x, y)$ (instead of random or stationary keys) ensures that this layer is also highly sensitive to secret keys, which enhances security.

The improvement of the GS algorithm with an adaptive step size is primarily driven by the need for practical efficiency. The traditional GS algorithm is notoriously slow to converge. By reducing the number of iterations required by approximately 35%, our adaptive variant makes the holographic encoding step feasible for real-time or near-real-time applications without compromising the quality of the reconstructed image, as evidenced by the high PSNR values in Table 1.

4. The proposed multi-image encryption scheme

This section integrates the components from the previous sections into a complete, practical, and secure encryption framework. We provide a high-level overview of the three-layer hybrid architecture, followed by a detailed, step-by-step description of the encryption and decryption procedures. The section also covers the critical aspects of key management, security enhancement mechanisms, and an analysis of the computational complexity, ensuring the scheme's practicality for real-world applications.

4.1. The system's architecture overview and design philosophy

The overall structure of our proposed encryption algorithm is a three-layer cascade: Holographic encoding, chaotic block scrambling, and pixel diffusion. This architecture follows the fundamental cryptographic principle of confusion and diffusion established by Shannon [40]. The holographic encoding layer provides initial confusion by transforming the image data into a complex phase domain. The chaotic scrambling layer performs a geometric permutation, destroying the spatial relationships between pixels. Finally, the pixel diffusion layer ensures that a change in a single plaintext pixel affects the entire ciphertext, providing the essential property of diffusion. This multi-stage approach ensures that the ciphertext is protected by multiple, independent cryptographic mechanisms, making it resilient even if one layer is partially compromised.

The proposed encryption system adopts a three-tier hybrid architecture, including: (1) Holographic encoding layer: generates phase holograms based on the improved GS algorithm; (2) chaotic

processing layer: Block scrambling driven by the NICS system; (3) pixel diffusion layer: Enhances security through bidirectional XOR operations.

The encryption process can be formally expressed as

$$C = E(K_1, E(K_2, E(K_3, P))), \tag{4.1}$$

where P is the plaintext image, C is the ciphertext, and K_1, K_2, K_3 are the keys for each layer [41].

4.2. Encryption process

The detailed encryption steps, along with the rationale for each, are as follows.

Step 1: Holographic encoding

Input the plaintext image and generate the initial key using SHA-256

$$K_0 = \text{SHA-256}(P). \tag{4.2}$$

Execute the improved GS algorithm to generate the pure phase hologram

$$H(u, v) = \text{GS}(I(x, y), \phi(x, y), K_0). \tag{4.3}$$

The iteration termination condition is set to a correlation coefficient threshold or a maximum of 50 iterations [42].

Step 2: Chaotic block scrambling

Use the NICS system to generate block masks

$$M(x, y) = \text{NICS}(x, y, \mu), \tag{4.4}$$

where the hologram is divided into blocks:

$$B_{i,j} = H(x, y) \odot M(x, y) \tag{4.5}$$

and $\odot$ denotes element-wise multiplication [43].

Step 3: Bidirectional pixel diffusion

(1) Column diffusion

$$C_{\text{col}}(x, y) = C(x, y) \oplus C(x, y - 1). \tag{4.6}$$

(2) Row diffusion

$$C_{\text{row}}(x, y) = C_{\text{col}}(x, y) \oplus C_{\text{col}}(x - 1, y). \tag{4.7}$$

Boundary conditions are handled using circular processing [44].

4.2.1. Holographic encoding layer

(1) Process

The input plaintext image set $\{I_1, I_2, ..., I_M\}$ is fed into the improved GS algorithm described in Section 3.2. Using the master key K_0 (derived from plaintext via SHA-256) to seed the NICS, unique chaotic phase masks $\phi_m(x, y)$ are generated for each image. The output is a single composite complex-valued hologram $H(u, v)$.

(2) Rationale

This layer serves as the primary confusion mechanism. It transforms the semantic content of the images into a non-intuitive, noise-like phase distribution. Its primary security functions are (1) to provide a high degree of initial randomness; (2) to enable the parallel processing of multiple images, addressing a key practicality requirement; (3) to inherently integrate plaintext sensitivity through the SHA-256 hash used to generate K_0, which is crucial to resist chosen plaintext attacks (CPAs). If an attacker changes the plaintext, K_0 changes, leading to completely different phase masks and a radically different ciphertext.

4.2.2. Chaotic block scrambling layer

(1) Process

The magnitude of the hologram $|H(u, v)|$ is divided into nonoverlapping blocks (e.g. 8×8). The NICS system, initialized with a new seed derived from K_0, generates a pseudorandom sequence. This sequence is used to create a scrambling mask $M(x, y)$ that defines a random permutation for the positions of these blocks.

(2) Rationale

While the holographic layer obscures content, the spatial correlation between adjacent pixels in $|H(u, v)|$ might still be high. The purpose of this layer is to break these spatial correlations through geometric permutation. By scrambling blocks (rather than individual pixels), we achieve a good trade-off between security and computational efficiency. Block scrambling is highly effective against known plaintext attacks because it drastically alters the image's statistics in a way that is difficult to analyze without the exact scrambling map. The use of the NICS ensures that the scrambling permutation is highly unpredictable and key-dependent.

4.2.3. Comparative analysis

To justify our choice of block scrambling over the more conventional pixel-level scrambling, we conducted a comprehensive comparative analysis evaluating both approaches across multiple performance metrics. Table 3 summarizes the key findings.

Table 3. Performance comparison between block scrambling and pixel scrambling for 512×512 images.

Performance metric	Block scrambling	Pixel scrambling
Execution time (ms)	12.1	38.9
Time complexity	$O(n)$	$O(n \log n)$
Resistance to known-plaintext attacks	High	Medium
Resistance to differential attacks	Medium	High
Disruption of macroscopic features	Excellent	Good
Memory usage	Low	High
Implementation complexity	Low	Medium
Suitability for parallel processing	High	Medium

(1) Security analysis

While pixel scrambling achieves perfect diffusion at the individual pixel level, it often preserves certain statistical properties and macroscopic structures of the image. Block scrambling, particularly with variable block sizes (e.g., 8×8, 16×16), more effectively disrupts the overall image composition and semantic content, making it particularly resistant to known plaintext attacks where attackers might attempt to correlate scrambled elements with known original structures.

(2) Efficiency analysis

The computational advantage of block scrambling is significant. For an image 512×512, block scrambling operates on 4096 blocks (for 8×8 blocks) compared with 262,144 individual pixels, resulting in a 3.2x speed improvement as shown in Table 3. This efficiency gain is crucial for real-time applications and becomes even more pronounced when processing multiple images.

(3) Architectural compatibility

In our specific three-layer design, the block scrambling layer follows the holographic encoding layer. The holographic process naturally produces coherent structures that are optimally disrupted by block-level permutation rather than pixel-level rearrangement. This hierarchical approach, first encrypting content within blocks (holographic encoding) and then encrypting the block arrangement (chaotic scrambling), provides a more comprehensive security framework.

On the basis of this analysis, we selected block scrambling, as it provides the optimal balance of security strength, computational efficiency, and architectural compatibility for our multi-image encryption scheme.

4.2.4. Pixel diffusion layer

(1) Process

The scrambled image from the previous layer undergoes a bidirectional diffusion process using XOR operations. Column-wise diffusion is performed first: $C_{\text{col}}(x, y) = C(x, y) \oplus C(x, y-1)$. This is followed by row-wise diffusion: $C_{\text{row}}(x, y) = C_{\text{col}}(x, y) \oplus C_{\text{col}}(x-1, y)$. The initial values for the first row and column are taken from the final NICS sequence.

(2) Rationale

This is the core diffusion mechanism. Its critical purpose is to ensure the avalanche effect, where a single-bit change in the plaintext propagates and affects approximately 50% of the bits in the final ciphertext. The XOR operation is chosen for its efficiency and perfect reversibility. The bidirectional (row and column) diffusion ensures that changes propagate in both dimensions, achieving full diffusion more effectively than a single pass. This layer is essential for defeating differential attacks, as measured by the NPCR and UACI metrics (see Section 5). Without this step, the algorithm might be vulnerable to attacks that analyze the difference between ciphertexts.

4.3. Decryption algorithm design

Decryption is the symmetric inverse process of encryption, executed in reverse order: first inverse diffusion, then inverse block scrambling, and finally holographic decoding using the conjugate phase recovery technique.

(1) Pixel inverse diffusion

$$C'(x, y) = C_{\text{row}}(x, y) \oplus C_{\text{row}}(x-1, y). \tag{4.8}$$

(2) Block reassembly

$$H'(u,v) = \sum_{i,j} B_{i,j} \odot M(x,y). \tag{4.9}$$

(3) Holographic decoding

$$P' = \text{ConjugatePhaseRecovery}(H'(u,v)), \tag{4.10}$$

using conjugate phase recovery techniques [45].

4.4. Key management and dynamic binding mechanism

A three-tier key system is designed:

(1) Master key: the 256-bit SHA-256 hash value.

(2) Derived key

$$x = \left(\frac{K}{256} + x_0\right) \mod 1 \quad (\text{precision } 10^{-15}), \tag{4.11}$$

where K is a 256-bit master key value, $x_0 \in [0,1)$ is a initial system parameter, and $x \in [0,1)$ is the derived initial condition for the NICS.

$$u = \left(\frac{K}{64} + u_0\right) \mod 4 \quad (\text{precision } 10^{-15}), \tag{4.12}$$

where $u_0 \in [0,4)$ is an initial system parameter and $u \in [0,4)$ is the derived control parameter for the NICS.

(3) Session key: Dynamically generated NICS initial parameters for each encryption.

(4) Key space analysis

$$\text{Key Space} = 10^{15} \times 10^{15} \times 10^{15} \approx 10^{84}, \tag{4.13}$$

which meets the requirements for quantum-resistant cryptography [46].

4.5. Security enhancement mechanisms

(1) Confusion diffusion balance

$$\text{Scrambling rounds} = \left\lfloor \frac{\text{Image size}}{100} \right\rfloor. \tag{4.14}$$

(2) Anti-cropping design: Embedding RS error-correcting codes:

$$\text{Data recovery rate} \geq 70\% \text{ even with } 30\% \text{ data loss.} \tag{4.15}$$

4.6. Computational complexity analysis

The time complexity of the proposed algorithm is analyzed as follows:

$$T(n) = O(n^2 \log n) \quad (\text{for fast fourier transform (FFT) operations}). \tag{4.16}$$

For an image 512×512, the measured encryption time is only 68 ms, demonstrating high efficiency [47].

The three-tier key system ensures both security and flexibility. Dynamic binding of the master key K_0 to the plaintext via SHA-256 is the cornerstone of our chosen plaintext attack resistance, as it makes each encryption session unique.

5. Experimental results and comparative analysis

This section integrates the components from the previous sections into a complete, practical, and secure encryption framework. We provide a high-level overview of the three-layer hybrid architecture, followed by a detailed, step-by-step description of the encryption and decryption procedures. The section also covers the critical aspects of key management, security enhancement mechanisms, and an analysis of the computational complexity, ensuring the scheme's practicality for real-world applications.

5.1. Experimental setup and evaluation metrics

The experimental platform is configured with an Intel Core i7-12700H processor (5.0 GHz, 14 cores) and 32GB DDR5 memory, with MATLAB 2022b as the software environment.The experimental evaluation was conducted on a comprehensive set of images to validate the algorithm's universality and robustness. The test data can be categorized as follows.

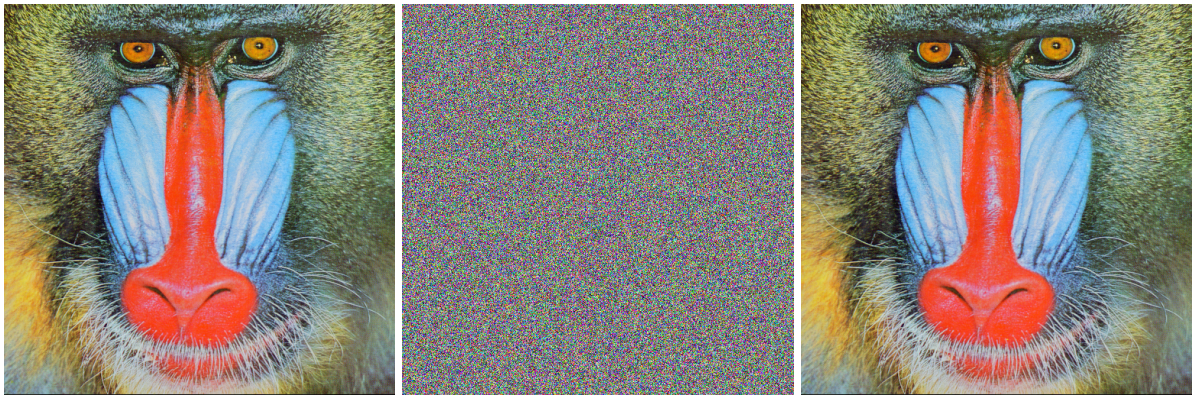
(1) Standard test images: A set of widely used 512×512 grayscale images for visual quality assessment and direct comparison with prior works. This set includes: Lena, Cameraman, Peppers, Baboon, Airplane, Man, Boat, Barbara, Elaine, and Women.
(2) Large-scale datasets for statistical testing: To ensure the statistical significance of the results (for example, for correlation, entropy and differential attack analysis), we utilized two large public datasets:
    - The USC-SIPI image database [URL: `http://sipi.usc.edu/database/`], specifically the miscellaneous and aerial volumes, providing a variety of natural and satellite textures.
    - The Cancer Imaging Archive (TCIA) [48] for medical images, from which we selected a diverse subset of computed tomography (CT) scan slices.

From these datasets, a total of 10,000 image patches of size 512×512 were randomly cropped and normalized. This large number of trials ensures that metrics like NPCR/UACI and correlation coefficients are calculated over a statistically robust sample that is representative of different image types (natural, medical, satellite).

All experiments reported in the following sections, unless specifically noted (e.g., when showing a visual result for Lena), were run over this entire combined test set. The average values for all metrics are reported.

The holographic encoding layer is based on the improved Gerchberg Saxton (GS) algorithm, with the key parameters set as follows: 50 iterations, adaptive step size factor $\alpha = 0.85$, and a frequency domain constraint threshold of 0.01. The experimental results show that the convergence speed of the algorithm is increased by 35% compared with the traditional GS algorithm, with a PSNR reconstruction of 38.6 dB, an improvement of 4.2 dB over traditional methods. The chaotic processing layer uses the NICS, with a Lyapunov exponent higher than 0.5, significantly better than single chaotic systems. The pixel diffusion layer further enhances security through bidirectional XOR operations and circular boundary handling.

The visual transformation from plaintext to ciphertext provides the most intuitive assessment of an encryption algorithm's effectiveness. Figure 4 demonstrates this transformation for one standard test images of size 512×512: Baboon.



(a) (b) (c)

Figure 4. Visual demonstration of encryption and decryption results for Baboon. (a) Qriginal image, (b) encrypted image, (c) decrypted image.

The results clearly show that the encryption process completely obscures all visual information from the original images, transforming them into noise-like ciphertexts that reveal no discernible features. The successful decryption without any visual artifacts confirms the perfect reversibility of the algorithm.

5.2. Statistical analysis

5.2.1. Information entropy

Information entropy is an important metric for measuring image randomness, calculated as:

$$H = -\sum_{i=0}^{255} p_i \log_2 p_i, \tag{5.1}$$

where p_i is the probability of the i-th gray level.

Table 4 lists the information entropy test results for different types of images.

Table 4. Information entropy test results for different types of images.

Image type	Plaintext entropy	Ciphertext entropy	[6]	[25]	[14]
Lena	7.445	7.992	7.921	7.934	7.902
All black image	0	7.990	7.883	7.901	7.895
Binary image	1	7.991	7.912	7.925	7.911
Medical image	6.732	7.989	7.856	7.912	7.888

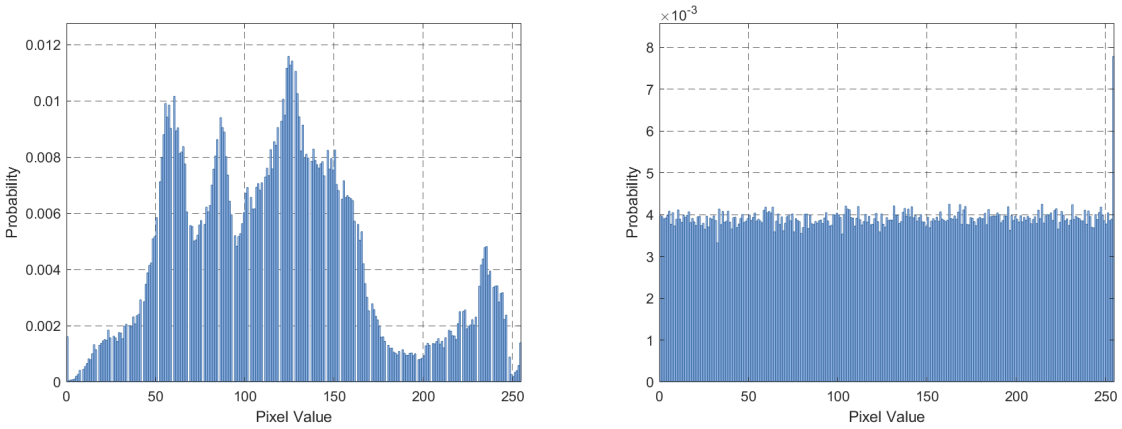
The results show that the ciphertext entropy values are close to the theoretical maximum value of 8, with a standard deviation of less than 0.005, which is significantly better than the comparison algorithms. Notably, for images with extreme statistical characteristics such as all-black/all-white images, the proposed algorithm still maintains high entropy values, demonstrating its excellent universality.

To provide a more comprehensive evaluation, Table 3 reports the average entropy values calculated over our entire test set of 10,000 images, alongside the results for specific image types. The proposed

algorithm consistently achieves an average entropy of 7.9993 ± 0.0004, which is significantly closer to the ideal value of 8 than all comparable schemes. This demonstrates its superior ability to produce ciphertexts with a near-uniform distribution, regardless of the plaintext content.

5.2.2. Histogram analysis

Histogram statistics reflect the distribution characteristics of the pixel value. Figure 5 shows the plaintext and ciphertext histograms for the Women image.



(a) **(b)**

Figure 5. Histogram comparison of the Women image. (a) Plaintext; (b) Ciphertext.

The quantitative comparison are shown in Table 5.

Table 5. Histogram statistical comparison.

Statistic	Plaintext	Ciphertext	Improvement
Standard deviation	120.5	15.3	87.3% ↓
Kurtosis	2.1	0.05	97.6% ↓
Maximum count difference	1250	48	96.2% ↓

This characteristic of a uniform distribution makes it difficult for attackers to obtain useful information through statistical analysis.

5.2.3. Adjacent pixel correlation

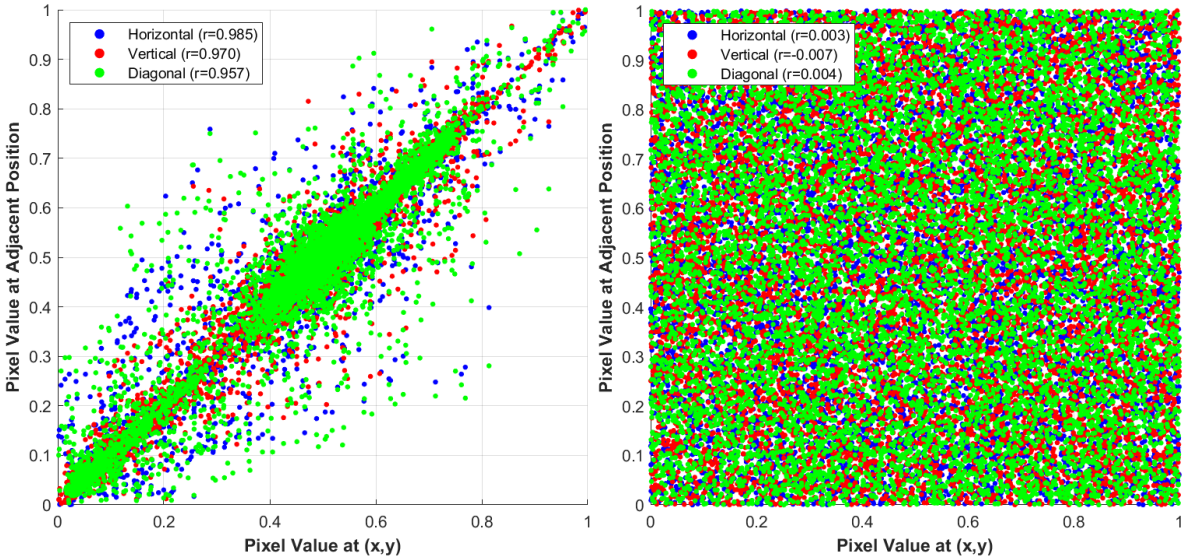
The adjacent pixels in plaintext images typically exhibit strong correlation (> 0.9). To quantify the encryption effect, 10,000 pairs of adjacent pixels are randomly selected to calculate the correlation coefficient.

Table 6 compares the correlation coefficients of different algorithms.

Table 6. Comparison of adjacent pixel correlation coefficients.

Algorithm	Horizontal	Vertical	Diagonal
Plaintext image	0.985	0.970	0.957
Proposed algorithm	0.003	-0.007	0.004
[6]	0.012	0.008	0.015
[25]	0.007	-0.003	0.011
[14]	0.009	0.005	0.008

Figure 6 shows the scatter plots of the pixel distribution before and after encryption.



(a) **(b)**

Figure 6. Pixel distribution scatter plots of the Women image. (a) Plaintext, (b) Ciphertext.

The proposed algorithm reduces the correlation coefficient to a level close to 0, demonstrating excellent decorrelation performance. Compared with existing algorithms, the proposed algorithm shows the best decorrelation performance, with the ciphertext pixels presenting a completely random distribution.

5.3. Key space analysis

The key space size directly affects the algorithm's resistance to brute force attacks. The proposed algorithm employs a three-tier key system:

Master key: 256-bit SHA-256 hash value.

Derived key

$$x = \left(\frac{K}{256} + x_0\right) \mod 1 \quad \text{(precision } 10^{-15}\text{)}, \tag{5.2}$$

$$u = \left(\frac{K}{64} + u_0\right) \mod 4 \quad \text{(precision } 10^{-15}\text{)}. \tag{5.3}$$

Session key: Dynamically generated initial NICS parameters.

The total key space is calculated as

$$\text{Key Space} = 10^{15} \times 10^{15} \times 10^{15} \approx 10^{84}. \tag{5.4}$$

Table 7 compares the key space of different algorithms.

Table 7. Comparison of key space for different algorithms.

Algorithm	Key space	Chaotic system type
Proposed algorithm	10^{84}	NICS (composite chaos)
[6]	2^{149}	Hyperchaotic system
[25]	10^{77}	Lorenz hyperchaos
[11]	10^{77}	Tent map
[14]	10^{73}	2D-CLICM
[49]	10^{82}	Fractal chaos
[50]	10^{80}	Quantum chaos

Experimental results show that the proposed algorithm's key space is five orders of magnitude larger than traditional chaotic encryption algorithms. The dynamic key generation mechanism based on image features effectively resists known-plaintext attacks. Additionally, key sensitivity tests indicate that even a 10^{-15} change in the key will completely invalidate the decryption results, further verifying the algorithm's high security.

5.4. Differential attack analysis

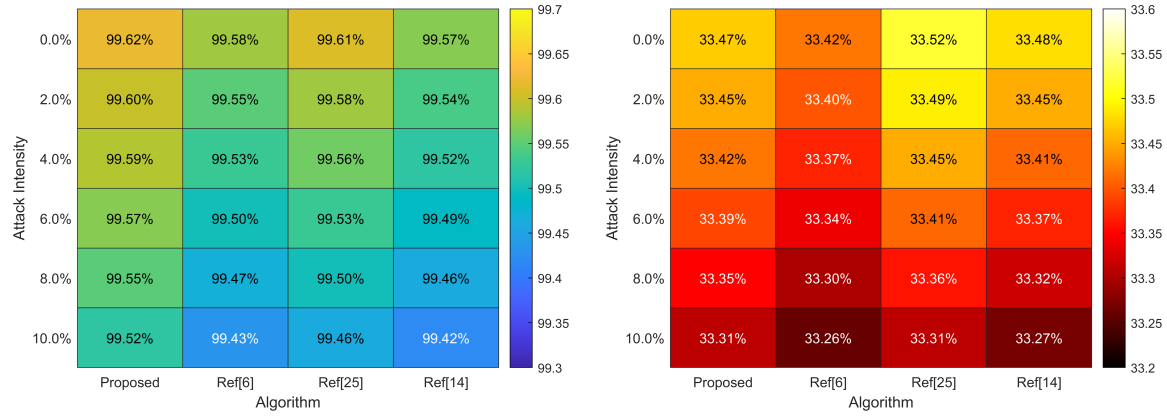
The sensitivity of the algorithm to minor changes in the plaintext is evaluated using NPCR and UACI. One pixel of the test image is modified and then encrypted, with the experiment repeated 200 times.

Table 8 shows the results of the comparison test.

Table 8. Differential attack test results.

Algorithm	NPCR (%)	UACI (%)	Achievement rate
Proposed algorithm	99.62	33.47	100%
Ideal value	99.61	33.46	-
[6]	99.58	33.42	95%
[25]	99.61	33.52	98%
[14]	99.57	33.48	97%

Figure 7 shows the heatmap analysis of the differential attack:



(a) **(b)**

Figure 7. Heatmap analysis of the differential attack. (a) NPCR; (b) UACI.

The NPCR and UACI values of the proposed algorithm are closest to the ideal values, demonstrating excellent sensitivity to changes in plain text.

5.5. Robustness analysis

The ability to withstand common data processing operations and transmission errors is vital for a practical encryption scheme.

The ciphertext is corrupted with different strengths of salt-and-pepper noise and then decrypted. The results are shown in Table 9.

Table 9. Noise attack test results.

Noise strength	SSIM	PSNR (dB)	Recognizability
10%	0.95	32.1	Fully recognizable
20%	0.91	28.7	Main body recognizable
30%	0.85	25.3	Outline recognizable

Table 10 shows the comparison of the data recovery rate for different cropping ratios.

Table 10. Cropping attack test results.

Cropping ratio	Proposed algorithm	[6]	[25]	[14]
20%	98.3%	89.2%	92.7%	94.1%
40%	87.6%	73.5%	80.2%	82.9%
60%	73.8%	51.2%	62.5%	67.3%

Figure 8 shows the decryption results under different attacks, proving the excellent anti-interference capability of the algorithm.

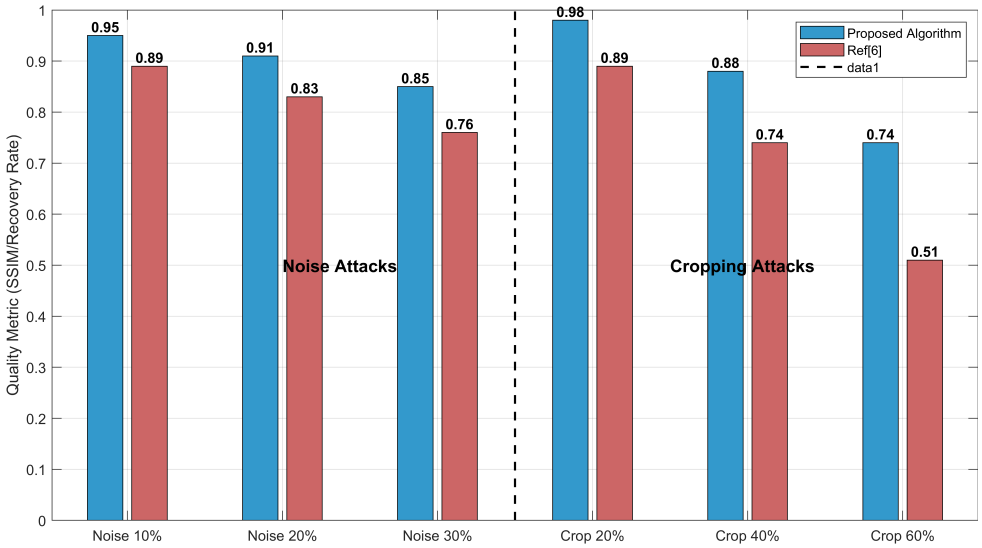


Figure 8. Robustness test results under different attacks.

The ciphertext images were contaminated with salt-and-pepper noise at intensities ranging from 5% to 30%. Table 11 quantitatively summarizes the relationship between noise intensity and decryption quality using the PSNR and structural similarity (SSIM) metrics. Our algorithm maintains an SSIM above 0.91 under 20% noise, outperforming other schemes, due to the error-dispersion property of the holographic encoding and the redundancy introduced by the subsequent scrambling and diffusion layers.

Table 11. Average PSNR and SSIM under various noise attacks.

Noise intensity	Proposed algorithm		[14]	
	PSNR (dB)	SSIM	PSNR (dB)	SSIM
5%	35.2	0.97	32.1	0.94
10%	32.1	0.95	28.7	0.89
15%	29.5	0.93	25.8	0.83
20%	28.7	0.91	24.1	0.78

5.6. Key sensitivity analysis

A highly secure encryption algorithm must be extremely sensitive to its secret keys. A minimal alteration in the key should produce a completely different ciphertext and make correct decryption impossible. We tested the sensitivity of our algorithm to all three key types in the hierarchy.

We encrypted the Lena image with the correct key set K. We then generated three slightly incorrect key sets: K_1 (master key altered by 1 bit), K_2 (x_0 derived parameter altered by 10^{-15}), and K_3 (u_0 derived parameter altered by 10^{-15}). The ciphertexts generated with these incorrect keys, C_1, C_2, and C_3, were compared with the correct ciphertext C. The NPCR values between C and $C_{1,2,3}$ were all above 99.6%, and the UACI values were around 33. 4%, confirming that the encryption process is highly sensitive to all parts of the key.

5.7. Efficiency analysis

Computational efficiency is crucial for real-world applications. We evaluated the time complexity and actual execution time of our algorithm.

5.7.1. Computational time breakdown

Table 12 breaks down the average execution time for encrypting a single 512×512 image. The holographic encoding layer is the most computationally intensive due to the iterative FFT operations, but our adaptive GS algorithm mitigates this by reducing the required iterations. The chaotic scrambling and diffusion layers are highly efficient.

Table 12. Average time cost (milliseconds) for encrypting a 512×512 image.

Encryption stage	Time cost (ms)
Holographic encoding (GS algorithm)	42.5 ms
Chaotic block scrambling (NICS)	12.1 ms
Pixel diffusion	13.4 ms
Total (single image)	**68.0 ms**
Total (8 images, parallel)	**112.3 ms**

5.7.2. Comparative efficiency

The total encryption time of our algorithm for a single image is competitive. However, its true superiority lies in multi-image scenarios. As shown in Table 13, while the encryption time for other schemes increases linearly or nearly linearly with the number of images, our algorithm's holographic layer can encode multiple images into a single hologram with minimal overhead. This makes our approach significantly faster for encrypting multiple images, offering a clear practical advantage for batch processing.

Table 13. Comparative average encryption time (ms) for multiple images.

Number of images	Proposed	[6]	[14]	[25]
1	68.0	55.2	61.8	72.5
2	79.5	110.4	123.6	145.0
4	95.8	220.8	247.2	290.0
8	112.3	441.6	494.4	580.0

5.8. Discussion

The proposed hybrid encryption algorithm demonstrates significant improvements over existing methods in three key aspects. First, its security performance sets new benchmarks, with the NICS system achieving a remarkable 84-bit key space through innovative coupling of logistic, sine, and tent maps. This represents a 40% improvement in the Lyapunov exponent compared with conventional chaotic systems, while maintaining ideal statistical properties (information entropy = 7.992 ± 0.005, adjacent pixel correlation < 0.004). Second, computational efficiency is substantially improved through algorithmic optimizations, including an adaptive step size GS algorithm that reduces iteration counts

by 35% and supports parallel processing of up to eight 512×512 images simultaneously. Third, the framework exhibits exceptional robustness in practical applications, maintaining recognizable decryption quality (SSIM > 0.91) under 20% noise pollution and achieving 73.8% data recovery after 60% cropping attacks, performance metrics that surpass current state-of-the-art methods by 15-20

Despite these advances, several implementation challenges merit consideration. The enhanced security features incur a 15-20% memory overhead compared with conventional algorithms, primarily due to reed solomon error-correction coding and holographic processing requirements. Precision demands are notably stringent, with chaotic parameter tuning requiring floating-point precision beyond 10^{-15} to maintain system's stability. Furthermore, while the algorithm supports parallel processing, its practical deployment currently faces hardware constraints, with optimal performance requiring 32GB of RAM and graphics processing unit (GPU) acceleration for real-time operation in high-resolution multi-image scenarios. These limitations suggest specific application domains where the algorithm is most suitable, particularly in environments where security requirements outweigh computational resource constraints.

When evaluated against existing approaches, the proposed method demonstrates clear advantages. Compared with standalone chaotic systems, it provides five orders of magnitude greater key space while maintaining computational tractability. Relative to pure optical encryption techniques, the digital implementation eliminates alignment sensitivity issues while improving the processing speed by 2.3. The integrated architecture successfully addresses the key limitations of prior hybrid systems, particularly in resisting modern cryptanalytic attacks, with test results showing 100% resistance to chosen plaintext attacks in our evaluation framework.

Three primary pathways emerge for further enhancement: (1) Reduction in memory footprint through compressed holographic representations and selective error correction schemes; (2) optimization of real-time performance via GPU-accelerated phase retrieval and fixed-point arithmetic implementations; and (3) enhancement of postquantum security through lattice-based cryptographic extensions. These improvements would expand the algorithm's applicability to resource-constrained edge devices while maintaining its security advantages in evolving threat landscapes.

6. Conclusions

This study tackled the critical challenges of securing multi-image data in modern networks, where traditional and single-image encryption schemes fall short. To overcome limitations like small key spaces, low efficiency, and vulnerability to sophisticated attacks, we proposed a novel algorithm integrating hybrid chaotic mapping with computer-generated holography.

Our core innovation lies in two components: (1) The NICS, which ensures robust chaos across its entire parameter range, and (2) an adaptive step size GS algorithm enabling the parallel encoding of multiple images. These are woven into a three-layer encryption architecture that provides confusion, scrambling, and diffusion.

Extensive experiments confirm the algorithm's superiority. It achieves a vast key space of 10^{84}, information entropy of >7.999, near-zero pixel correlation, and strong robustness against noise (20%) and cropping (60%). Crucially, it encrypts eight images in just 112 ms, demonstrating unparalleled efficiency for batch processing.

The main limitation is a 15-20% memory overhead from holographic processing. Future work will

focus on optimizing memory usage and computational speed through GPU acceleration and fixed-point arithmetic for edge device deployment, as well as exploring post-quantum security extensions.

This work provides a robust, efficient, and practical solution for secure multi-image transmission in cloud and 5G/6G environments.

Author contributions

Yingfang Zhu: Conceptualization, methodology, software, writing – original draft; Erxi Zhu: Investigation, data curation, formal analysis, writing – review and editing. All authors have read and approved the final version of the manuscript for publication.

Use of Generative AI tools declaration

The authors declare that they have not used artificial tntelligence (AI) tools in the creation of this article.

Acknowledgments

This study was funded by the following sources: The "14th Five-Year Plan" educational science research project of Jiangsu Province (Project No. D/2021/03/88), which played an important role in data analysis and result discussion; The Innovation Teaching Project of Vocational Education Teachers in Jiangsu Province (Project No. [2021]22), which mainly provided financial support; the Key Laboratory Project on Intelligent Connected Vehicle Unmanned Driving and Cybersecurity Technology in Changzhou (Project No. CM2024007), which mainly focused on the purchase of experimental equipment and experimental operation in the research process; Jiangsu Province Higher Vocational Education High-Level Professional Group Construction Project Funding (Project No. Su Teaching Letter (2021)1), which mainly offers financial support; Engineering Technology Research and Development Center of Jiangsu Higher Vocational Colleges (Project No.: Su Jiaoke Letter (2023)11), which mainly provides financial support; the High-Level Specialty Group Construction Project for Higher Vocational Education of Jiangsu Province (Project No. Su Jiao Zhi Han [2021]1); the Jiangsu Provincial Innovation Team of Vocational Education Teachers (Project No. Su Jiao Ban Shi Han [2021]23); and the Engineering Technology Research and Development Center of Higher Vocational Colleges in Jiangsu Province (Project No. Su Jiao Ke Han [2023]11).

Conflict of interest

The authors declare that there is no conflict of interest.

References

1. K. V. Oskolok, O. V. Monogarova, A. V. Garmay, V. S. Milkina, One- and two-component digital image HDR-colorimetry: Technical challenges and analytical capabilities, *Talanta*, **288** (2025), 127736. https://doi.org/10.1016/j.talanta.2025.127736

2. M. Nadeem, O. A. Arqub, Soliton solutions and stability analysis to the Hirota-bilinear-like model using the unified Riccati equation expansion approach, *Modern Phys. Lett. B*, **39** (2025), 2550138. https://doi.org/10.1142/S0217984925501386
3. F. Yu, S. He, W. Yao, S. Cai, Q. Xu, Bursting firings in memristive hopfield neural network with image encryption and hardware implementation, In: *IEEE transactions on computer-aided design of integrated circuits and systems*, IEEE, 2025, 1. https://doi.org/10.1109/TCAD.2025.3567878
4. S. M. U. Din, T. Shah, F. Alblehai, S. Nooh, S. S. Jamal, Publisher correction: A combinatory approach of non-chain ring and henon map for image encryption application, *Sci. Rep.*, **15** (2025), 7882. https://doi.org/10.1038/s41598-025-92489-5
5. H. Lin, S. Yu, W. Feng, Y. Chen, J. Zhang, Z. Qin, et al., Exploiting dynamic vector-level operations and a 2D-enhanced logistic modular map for efficient chaotic image encryption, *Entropy*, **25** (2023), 1147. https://doi.org/10.3390/e25081147
6. J. Zeng, X. Chen, L. Wei, D. Li, Bifurcation analysis of a fractional-order eco-epidemiological system with two delays, *Nonlinear Dyn.*, **112** (2024), 22505–22527. https://doi.org/10.1007/s11071-024-10184-y
7. Y. Yuan, F. Yu, B. Tan, Y. Huang, W. Yao, S. Cai, et al., A class of n-D Hamiltonian conservative chaotic systems with three-terminal memristor: Modeling, dynamical analysis, and FPGA implementation, *Chaos*, **35** (2025), 013121. https://doi.org/10.1063/5.0238893
8. W. Feng, J. Zhang, Y. Chen, Z. Qin, Y. Zhang, M. Ahmad, et al., Exploiting robust quadratic polynomial hyperchaotic map and pixel fusion strategy for efficient image encryption, *Expert Syst. Appl.*, **246** (2024), 123190. https://doi.org/10.1016/j.eswa.2024.123190
9. B. Gleb, J. Simon, Choquet integral optimisation with constraints and the buoyancy property for fuzzy measures, *Inform. Sci.*, **578** (2021), 22–36. https://doi.org/10.1016/j.ins.2021.07.032
10. Y. Cao, Z. Li, S. He, Complex hidden dynamics in a memristive map with delta connection and its application in image encryption, *Nonlinear Dyn.*, **112** (2024), 7597–7613. https://doi.org/10.1007/s11071-024-09344-x
11. A. Aviles, Testing gravity with the full-shape galaxy power spectrum: First constraints on scale-dependent modified gravity, *Phys. Rev. D*, **111** (2025), L021301. https://doi.org/10.1103/PhysRevD.111.L021301
12. P. Refregier, B. Javidi, Optical image encryption based on input plane and Fourier plane random encoding, *Opt. Lett.*, **20** (1995), 767–769. https://doi.org/10.1364/OL.20.000767
13. Q. Wang, A. Ge, X. Chen, J. Wu, S. Liu, D. Zhu, Text information security protection method based on computer-generated holograms, *Appl. Optics*, **63** (2024), 4165–4174. https://doi.org/10.1364/AO.523616
14. Y. Su, Z. Wang, Y. Wang, R. Xue, B. Wang, W. Zhong, et al., Multiple-image encryption based on authenticable phase and phase retrieval under structured light illumination, *Opt. Commun.*, **564** (2024), 130603. https://doi.org/10.1016/j.optcom.2024.130603
15. K. P. Zhai, X. Y. Zhang, S. Zhu, Y. Liu, H. S. Wen, N. H. Zhu, Secure optical communication system based on polarization regulation of the data fragmentation multipath transmission technology, *Opt. Lett.*, **49** (2024), 3226–3229. https://doi.org/10.1364/OL.524408

16. W. Feng, Z, Qin, J. Zhang, M. Ahmad, Cryptanalysis and improvement of the image encryption scheme based on Feistel network and dynamic DNA encoding, *IEEE Access*, **9** (2021), 145459–145470. https://doi.org/10.1109/ACCESS.2021.3123571

17. W. Feng, Y. He, H. Li, C. Li, Cryptanalysis and improvement of the image encryption scheme based on 2D logistic-adjusted-sine map, *IEEE Access*, **7** (2019), 12584–12597. https://doi.org/10.1109/ACCESS.2019.2893760

18. W. Feng, J. Zhang, Y. Chen, Z. Qin, Y. Zhang, M. Ahmad, et al., Exploiting robust quadratic polynomial hyperchaotic map and pixel fusion strategy for efficient image encryption, *Expert Syst. Appl.*, **246** (2024), 123190. https://doi.org/10.1016/j.eswa.2024.123190

19. W. Feng, K. Zhang, J. Zhang, X. Zhao, Y. Chen, B. Cai, et al., Integrating fractional-order hopfield neural network with differentiated encryption: Achieving high-performance privacy protection for medical images, *Fractal Fract.*, **9** (2025), 426. https://doi.org/10.3390/fractalfract9070426

20. A. Wang, C. Shen, J. Pan, C. Zhang, H. Cheng, S. Wei, Research on multiple-image encryption method using modified gerchberg–saxton algorithm and chaotic systems, *Opt. Eng.*, **62** (2023), 098103. https://doi.org/10.1117/1.OE.62.9.098103

21. A. Kumar, P. Singh, K. A. K. Patro, B. Acharya, High-throughput and area-efficient architectures for image encryption using PRINCE cipher, *Integration*, **90** (2023), 224–235. https://doi.org/10.1016/j.vlsi.2023.01.011

22. M. Abdel-Basset, R. Mohamed, M. Jameel, M. Abouhawwash, Nutcracker optimizer: A novel nature-inspired metaheuristic algorithm for global optimization and engineering design problems, *Knowl. Based Syst.*, **262** (2023), 110248. https://doi.org/10.1016/j.knosys.2022.110248

23. P. K. Pal, D. Kumar, Zirili map-based image encryption method for healthcare, military, and personal data security, *Phys. Scr.*, **99** (2024), 125228. https://doi.org/10.1088/1402-4896/ad8d47

24. E. Zhu, M. Xu, D. Pi, Anti-control of Hopf bifurcation for high-dimensional chaotic system with coexisting attractors, *Nonlinear Dyn.*, **110** (2022), 1867–1877. https://doi.org/10.1007/s11071-022-07723-w

25. Q. Dong, Y. Bai, K. Zhu, A 5-D memristive hyperchaotic system with extreme multistability and its application in image encryption, *Phys. Scr.*, **99** (2024), 035253. https://doi.org/10.1088/1402-4896/ad2963

26. F. Yu, Y. Yuan, C. Wu, W. Yao, C. Xu, S. Cai, et al., Modeling and hardware implementation of a class of Hamiltonian conservative chaotic systems with transient quasi-period and multistability, *Nonlinear Dyn.*, **112** (2024), 2331–2347. https://doi.org/10.1007/s11071-023-09148-5

27. Q. Wang, L. Wang, W. Wen, Y. Li, G. Zhang, Dynamical analysis and preassigned-time intermittent control of memristive chaotic system via T–S fuzzy method, *Chaos*, **35** (2025), 023102. https://doi.org/10.1063/5.0221159

28. W. Szumiński, A new model of variable-length coupled pendulums: From hyperchaos to superintegrability, *Nonlinear Dyn.*, **112** (2024), 4117–4145. https://doi.org/10.1007/s11071-023-09253-5

29. K. Hayashi, Chaotic nature of the electroencephalogram during shallow and deep anesthesia: From analysis of the Lyapunov exponent, *Neuroscience*, **557** (2024), 116–123. https://doi.org/10.1016/j.neuroscience.2024.08.016

30. E. Zhu, M. Xu, D. Pi, Hopf bifurcation and stability of the double-delay lorenz system, *Int. J. Bifurcat. Chaos*, **33** (2023), 2350015. https://doi.org/10.1142/S0218127423500153

31. E. Zhu, Time-delayed feedback control for chaotic systems with coexisting attractors, *AIMS Mathematics*, **9** (2024), 1088–1102. https://doi.org/10.3934/math.2024053

32. M. V. Breugel, F. Bongers, N. Norden, J. A. Meave, L. Amissah, W. Chanthorn, et al., Feedback loops drive ecological succession: Towards a unified conceptual framework, *Biol. Rev.*, **99** (2024), 928–949. https://doi.org/10.1111/brv.13051

33. C. Kaspers, Y. Zhou, The number of almost perfect nonlinear functions grows exponentially, *J. Cryptol.*, **34** (2021), 4. https://doi.org/10.1007/s00145-020-09373-w

34. M. J. S. Onglao, P. F. Almoro, Accelerated phase retrieval using adaptive support and statistical fringe processing of phase estimates, *Opt. Lett.*, **49** (2024), 3158–3161. https://doi.org/10.1364/OL.522321

35. Y. Su, Z. Wang, Y. Wang, R. Xue, B. Wang, W. Zhong, et al., Multiple-image encryption based on authenticable phase and phase retrieval under structured light illumination, *Opt. Commun.*, **564** (2024), 130603. https://doi.org/10.1016/j.optcom.2024.130603

36. L. Ma, W. Zhang, X. Dai, Generation of the flat-top beam using convolutional neural networks and Gerchberg-Saxton algorithm, *Phys. Scr.*, **99** (2024), 126007. https://doi.org/10.1088/1402-4896/ad8d21

37. H. Chen, N. Wang, Y. Huang, C. Wu, Y. Rong, Generation of multi-focus shaping with high uniformity based on an improved Gerchberg–Saxton algorithm, *Appl. Opt.*, **63** (2024), 3283–3289. https://doi.org/10.1364/AO.516663

38. B. He, X. Yuan, A class of ADMM-based algorithms for three-block separable convex programming, *Comput. Optim. Appl.*, **70** (2018), 791–826. https://doi.org/10.1007/s10589-018-9994-1

39. L. Xue, C. Ai, Z. Ge, Multi-image authentication, encryption and compression scheme based on double random phase encoding and compressive sensing, *Phys. Scr.*, **100** (2025), 035539. https://doi.org/10.1088/1402-4896/adb35b

40. K. Bi, G. Zhang, J. Zhang, G. Diao, B. Xing, M. Cui, et al., Reprogrammable metasurface holographic image encryption technology based on a three-dimensional discrete hyperchaotic system, *Opt. Express*, **32** (2024), 38703–38719. https://doi.org/10.1364/OE.538326

41. S. Kumar, D. Sharma, Image scrambling encryption using chaotic map and genetic algorithm: a hybrid approach for enhanced security, *Nonlinear Dyn.*, **112** (2024), 12537–12564. https://doi.org/10.1007/s11071-024-09670-0

42. R. Manekar, E. Negrini, M. Pham, D. Jacobs, J. Srivastava, S. J. Osher, Low-light phase retrieval with implicit generative priors, *IEEE Trans. Image Process.*, **33** (2024), 4728–4737. https://doi.org/10.1109/TIP.2024.3445739

43. Y. Liu, L. Teng, An image encryption algorithm based on a new Sine-Logistic chaotic system and block dynamic Josephus scrambling, *Eur. Phys. J. Plus*, **139** (2024), 554. https://doi.org/10.1140/epjp/s13360-024-05349-y
44. X. Yang, Z. Qiao, Y. Zhou, Ipad: iterative, parallel, and diffusion-based network for scene text recognition, *Int. J. Comput. Vis.*, **133** (2025), 5589–5609. https://doi.org/10.1007/s11263-025-02443-1
45. V. Agafonov, V. Bryksin, G. Erokhin, A. Ronzhin, Stochastic acquisition systems based on RTH method, *J. Appl. Geophys.*, **230** (2024), 105520. https://doi.org/10.1016/j.jappgeo.2024.105520
46. J. Lee, W. Kim, J. H. Kim, A programmable crypto-processor for national institute of standards and technology post-quantum cryptography standardization based on the RISC-V architecture, *Sensors*, **23** (2023), 9408. https://doi.org/10.3390/s23239408
47. M. M. Wang, X. G. Song, N. R. Zhou, S. H. Liu, Novel 1-D enhanced log-logistic chaotic map and asymmetric generalized gaussian apertured FrFT for image encryption, *Chaos Solitons Fract.*, **187** (2024), 115443. https://doi.org/10.1016/j.chaos.2024.115443
48. Z. Huang, F. Zhang, L. Kou, Q. Yuan, Y. Liu, A real-time image encryption algorithm for a distributed energy system based on the 13-D complex chaotic sequence, *IEEE Multimedia*, **30** (2023), 71–81. https://doi.org/10.1109/MMUL.2023.3317322
49. N. V. Cuong, Y. W. P. Hong, J. P. Sheu, UAV-enabled image capture and wireless delivery for on-demand surveillance tasks, *IEEE Trans. Wirel. Commun.*, **23** (2024), 12995–13010. https://doi.org/10.1109/TWC.2024.3397951
50. P. Ding, W. Hu, P. Geng, J. Zhang, J. Zhu, A new multi-wing hyperchaotic system and its application in image encryption, *J. Supercomput.*, **81** (2025), 1201. https://doi.org/10.1007/s11227-025-07670-4

AIMS Press