TELKOMNIKA Telecommunication Computing Electronics and Control
Vol. 24, No. 4, August 2026, pp. 1353~1371
ISSN: 1693-6930, DOI: 10.12928/TELKOMNIKA.v24i4.27703

A new hybrid dyadic-tent chaotic function for secure digital image encryption

Anymore Majere, Hiento Suharja, Suryadi MT
Department of Mathematics, Faculty of Mathematics and Natural Sciences, Universitas Indonesia, Depok, Indonesia

Article Info

Article history:

Received Dec 4, 2025
Revised Apr 17, 2026
Accepted May 25, 2026

Keywords:

Chaotic functions
Dyadic map
Hybrid chaotic function
Secure hash algorithm-whitening
Tent map

ABSTRACT

Image encryption is significant for protecting visual data in modern digital communication systems. This study proposes a new hybrid chaotic function that combines the dyadic transformation map and the tent map to create a secure image encryption scheme. To enhance keystream unpredictability, secure hash algorithm 256 (SHA-256) hashing is used as a whitening layer. The chaotic properties of the proposed hybrid map are verified using the Lyapunov exponent, which proves its suitability for cryptographic applications. The performance of the scheme is evaluated using standard grayscale and red, green, and blue (RGB) images. The results show that the encrypted images exhibit near-ideal entropy values (7.9973–7.9999), very low correlation coefficients close to zero, and strong resistance to differential attacks with number of pixels change rate (NPCR) values above 99.6% and unified average changing intensity (UACI) values around 33%. In addition, the whitening process significantly reduces autocorrelation (from 0.0490 to 0.00032) and enables the generated sequences to pass all National Institute of Standards and Technology (NIST) randomness tests. The proposed method also demonstrates low computational complexity with linear time performance. These results indicate that the scheme provides a satisfactory balance between security, efficiency, and practical applicability.

Corresponding Author:

Anymore Majere
Department of Mathematics, Faculty of Mathematics and Natural Sciences, Universitas Indonesia
Depok 16424, Indonesia
Email: anymoremajere2@gmail.com

1. INTRODUCTION

The rapid growth of multimedia communication, cloud computing, and internet of things (IoT) systems has intensified the need for secure image transmission and storage. Digital images frequently contain sensitive personal, medical, and military information, making them attractive targets for cyberattacks [1]. Consequently, efficient and reliable image encryption schemes are essential for protecting visual data in modern communication environments. Image encryption refers to the process of transforming an original image into an unintelligible form using cryptographic algorithms and secret keys to prevent unauthorized access [2]–[4].

Conventional cryptographic algorithms, such as advanced encryption standard (AES) and Rivest–Shamir–Adleman (RSA), provide strong security guarantees but often exhibit high computational overhead when applied to large image datasets and resource-constrained devices [5], [6]. This limitation reduces their suitability for resource-constrained environments, including wireless sensor networks, embedded systems, and IoT devices [7], [8]. As a result, alternative encryption approaches with lower computational complexity have been actively investigated.

Chaos-based image encryption has received significant attention due to the inherent properties of chaotic systems, including sensitivity to initial conditions, pseudo-randomness, and ergodicity [4], [9], [10]. Numerous schemes based on logistic, tent, dyadic, and hénon maps have been proposed for key generation and diffusion mechanisms [3], [11], [12]. These approaches often achieve high computational efficiency and simple implementation.

However, extensive cryptanalysis has shown that single one-dimensional chaotic maps, for example, the dyadic map, frequently fail to provide sufficient confusion and diffusion. They therefore allow residual statistical patterns to remain in encrypted images, thereby increasing vulnerability to statistical and differential attacks [13], [14]. To address these weaknesses, recent studies have proposed hybrid chaotic systems and chaos–hash frameworks that integrate multiple maps and cryptographic primitives [2], [4], [9], [15]–[17].

Despite extensive research on chaos-based image encryption, an inherent trade-off remains unresolved: single one-dimensional chaotic maps often fail to provide sufficient randomness and diffusion for secure encryption, while existing hybrid or high-dimensional chaotic schemes typically incur increased computational complexity, limiting their applicability in lightweight and resource-constrained environments. Addressing this trade-off between security performance and computational efficiency remains an open challenge [2], [4], [16], [18].

In this paper, a new lightweight hybrid chaotic image encryption scheme based on the composition of the dyadic transformation map and the tent map, enhanced by Secure Hash Algorithm 256 (SHA-256)-based whitening, is proposed. By integrating the bit-shifting dynamics of the dyadic map with the piecewise linear structure of the tent map, the proposed scheme improves entropy, key sensitivity, and resistance to statistical attacks while maintaining low computational overhead. The proposed method emphasizes simplicity, reproducibility, and practical deployability for resource-constrained systems.

The proposed scheme is evaluated using comprehensive chaotic and cryptographic analyses, including bifurcation diagrams, Lyapunov exponent analysis, National Institute of Standards and Technology (NIST) randomness testing, histogram and correlation analysis, key sensitivity assessment, robustness evaluation, and runtime measurements.

The main contributions of this research are summarized as follows:

- A novel hybrid dyadic–tent chaotic map integrated with SHA-256 whitening for lightweight image encryption.
- A reproducible encryption framework with explicit parameter settings and a well-defined key structure.
- Comprehensive security, robustness, and performance evaluation using standard cryptographic metrics.
- A comparative analysis demonstrating competitive randomness quality and computational efficiency.

The remainder of this paper is organized as follows: section 2 describes the proposed encryption algorithm, section 3 presents the experimental results and security analysis, and section 4 concludes the paper and discusses future research directions.

2. METHOD

This study utilizes two one-dimensional chaotic maps, the dyadic transformation map and the tent map, to construct a hybrid composition function used for image encryption. The composite function serves as the keystream generator for a substitution–permutation–based encryption procedure.

2.1. The dyadic transformation map

The dyadic transformation map function is defined as:

$$x_{n+1} = 2x_n \ mod \ 1 \tag{1}$$

Alternatively, this can be written as:

$$f(x) = \begin{cases} 2x, & 0 \le x < 0.5 \\ 2x - 1, & 0.5 \le x < 1 \end{cases} \tag{2}$$

This map generates deterministic sequences with random-like behavior due to repeated stretching and folding of the unit interval, making it suitable for cryptographic applications [19]–[21].

2.2. The tent map

The tent map is defined as:

$$x_{n+1} = \begin{cases} rx_n & if\ x_n < 0.5 \\ r(1-x_n) & if\ x_n \geq 0.5 \end{cases} \quad (3)$$

where $r \in [0,2]$ controls the chaotic behavior.

2.3. The hybrid dyadic-tent map

Let $f(x)$ denote the dyadic map and $g(x)$ the tent map. The proposed hybrid map is defined by composition:

$$h(x) = f\big(g(x)\big) = 2 \cdot g(x) \bmod 1. \quad (4)$$

Substituting (3) into (2), and for $x \in [0,1]$ and $r \leq 2$ the composite function becomes:

$$h(x) = \begin{cases} 2rx\,, & 0 \leq x \leq 0.5\ and\ 0 \leq rx < 0.5 \\ 2rx - 1, & 0 \leq x \leq 0.5\ and\ 0.5 \leq rx \leq 1 \\ 2r(1-x)\,, & 0.5 < x \leq 1\ and\ 0 \leq r(1-x) < 0.5 \\ 2r(1-x) - 1, & 0.5 < x \leq 1\ and\ 0.5 \leq r(1-x) \leq 1 \end{cases} \quad (5)$$

All computations are performed in double-precision floating-point arithmetic with $x_n \in (0,1)$. This composition integrates the stretching effect of the tent map with the bit-shifting mechanism of the dyadic map, enhancing entropy and sensitivity to initial conditions. the proposed hybrid dyadic–tent map is iterated to generate both the permutation sequence used for pixel scrambling and the chaotic keystream employed in the diffusion stage of the encryption algorithm.

Figure 1 illustrates the graph of the composite map for $r = 1.5$, showing dense folding and strong transitions across the unit interval. In this study, control parameter r is selected close to its upper bound (e.g., $r \geq 1.5$) to ensure fully developed chaotic behavior, as values near 2 maximize sensitivity to initial conditions and yield positive Lyapunov exponents across the unit interval. Lower values of r were empirically observed to reduce randomness and were therefore excluded [22]–[24].

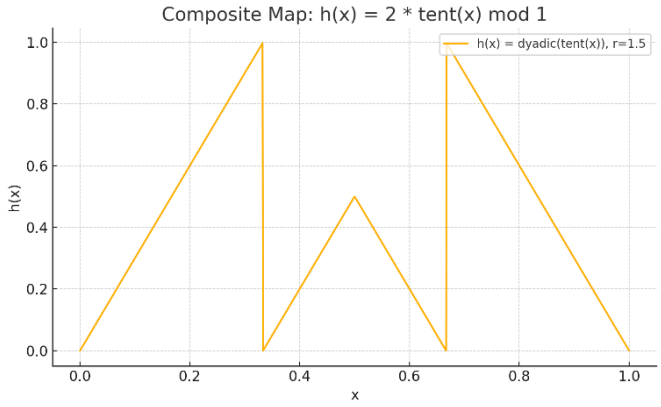


Figure 1. Graph of the hybrid dyadic-tent map for $r = 1.5$

2.4. NIST statistical test suite

To evaluate the intrinsic randomness of the proposed hybrid dyadic–tent map, the NIST statistical test suite (STS) is applied. The suite consists of 15 statistical tests (with 16 results) designed to assess the randomness of a chaos function [10], [24]. Two binary sequences were generated for comparison: a raw sequence and a SHA-256–whitened sequence. The chaotic map was implemented in Python 3 within a Google Colab environment using double-precision arithmetic, with a control parameter $r = 1.6$ and initial condition $x_0 = 0.612345$. After discarding the first 5,000 iterations to eliminate transient effects, the map outputs were quantized to 32-bit integers and concatenated to produce sequences of approximately 5 MB (40,000,000 bits). The whitened sequence was obtained by applying SHA-256 hashing to fixed-size blocks of the raw byte stream, enabling a direct comparison between unprocessed and post-processed chaos outputs. Randomness evaluation was performed using the Python implementation of the NIST statistical test suite developed by Ang [25], executed under Windows PowerShell with Python 3.13 (64-bit). This procedure

isolates the inherent randomness of the proposed chaotic map while assessing the impact of cryptographic whitening. We also calculate entropy and autocorrelation to strengthen our results. The autocorrelation function of the generated keystream is evaluated using fast fourier transform (FFT)-based estimation on a ±1 transformed bit sequence. A secure keystream is expected to exhibit a sharp peak at zero lag and near-zero correlation for all non-zero lags. Both raw and SHA-256-whitened streams are analyzed to evaluate the impact of the whitening stage on statistical independence.

2.5. Encryption and decryption process

The proposed image-encryption scheme employs the same hybrid dyadic–tent chaotic keystream generator used in the NIST statistical evaluation. The generator preserves the identical chaotic dynamics, quantization process, and SHA-256–based whitening mechanism. For image encryption, the generator is generalized to produce variable-length keystreams and incorporates a public per-image initialization vector (IV) to prevent keystream reuse, without altering the underlying statistical properties validated by NIST testing.

We use a fixed secret key $K = (x_0, r)$, where $x_0 = 0.612345$ and $r = 1.600000$ are chosen. To prevent keystream reuse while preserving reproducibility, a public per-image IV is deterministically derived from the image filename as the first 64 bits of the SHA-256 hash, i.e., $\mathrm{IV} = \mathrm{Trunc}_{64}(\mathrm{SHA}-256(\mathrm{filename}))$. A fixed burn-in value of 5 000 iterations is applied to the chaotic system. Input images are processed either in grayscale (L) or red, green, and blue (RGB) mode; palette-based images are first converted to grayscale to ensure uniform 8-bit sampling. The image is serialized into a one-dimensional plaintext vector $p \in \{0, \ldots, 255\}^L$, where $L = MN$ for grayscale images and $L = 3MN$ for RGB images using a concatenated channel order $p = [R \parallel G \parallel B]$. This serialization step is fully deterministic, ensuring that identical inputs and preprocessing choices always yield the same plaintext representation.

For each image, a variable-length keystream of exactly $4L$ is generated using the hybrid dyadic–tent map initialized with K. After discarding a deterministic number of initial iterations equal to $5000 + (IV \ mod \ 100000)$, the chaotic orbit is converted to a 32-bit integer sequence via $u = \lfloor x \cdot 2^{32} \rfloor$, packed into big-endian bytes and truncated to the required length. Cryptographic whitening is then applied block wise by hashing each 32-byte chunk using SHA-256 with IV concatenation, i.e., $SHA-256(IV \parallel chunk)$, and truncating the result to preserve the original length. The resulting whitened keystream is split into three segments: the first 2L-bytes drive a Fisher–Yates permutation that reorders the plaintext vector to achieve confusion, while the remaining two L-byte segments are used for forward and backward diffusion, respectively. Diffusion is performed in two chained passes using modular addition, exclusive OR (XOR) feedback, and data-dependent 8-bit rotations applied to each keystream byte. This significantly enhances avalanche behaviour while remaining fully invertible. The final ciphertext vector is reshaped back into either an $\mathrm{M} \times \mathrm{N}$ grayscale image or an $\mathrm{M} \times \mathrm{N} \times 3$ RGB image. Decryption follows the exact inverse sequence: keystream regeneration, inverse backward diffusion, inverse forward diffusion, application of the inverse permutation, and image reshaping. Because all steps are deterministic and bijective, and because the IV is derived deterministically from the filename, bit-perfect reconstruction of the original image is guaranteed whenever the same key parameters, IV derivation, and preprocessing mode are used. The process is supported by some recent chaos-based permutation strategies [1], [12], [14]. The implementation is summarized in Algorithms 1 and 2 in Table 1.

Table 1. Algorithms 1 and 2: proposed image encryption and decryption procedures

Algorithm 1	Algorithm 2
Input: Image I, secret key $K = (x_0, r)$, base_discard D_0, filename name	**Input**: Cipher image C, secret key $K = (x_0, r)$, base discard D_0, filename name
Output: Cipher image C	**Output**: Recovered image I
1: IV ← Trunc64(SHA-256(name))	1: IV ← Trunc64(SHA-256(name))
2: p ← SerializeImage(I) ▷ grayscale or RGB (R‖G‖B)	2: c ← SerializeImage(C)
3: L ← length(p)	3: L ← length(c)
4: k_s ← Generate Whitened Keystream (4L, K, D_0, IV)	4: k_s ← Generate Whitened Keystream (4L, K, D_0, IV)
5: (S_{perm}, S_1, S_2) ← Split(k_s, [2L, L, L])	5: (S_{perm}, S_1, S_2) ← Split(k_s, [2L, L, L])
6: π ← Fisher Yates Permutation (L, S_{perm})	6: π ← Fisher Yates Permutation(L, S_{perm})
7: $p\pi$ ← Apply Permutation (p, π)	7: π^{-1} ← Invert Permutation(π)
8: c_1 ← Forward Diffusion ($p\pi$, S_1, $IV_{[0]}$)	8: c_1 ← Inverse Backward Diffusion(c, S_2, $IV_{[1]}$)
9: c ← Backward Diffusion (c_1, S_2, $IV_{[1]}$)	9: $p\pi$ ← Inverse Forward Diffusion(c_1, S_1, $IV_{[0]}$)
10: C ← Reshape To Image(c)	10: p ← Apply Permutation($p\pi$, π^{-1})
11: return C	11: I ← Reshape To Image(p)
	12: return I

2.6. Threat model

The proposed image encryption scheme is evaluated under a standard cryptographic threat model consistent with Kerckhoffs's principle, whereby the adversary is assumed to possess full knowledge of the encryption and decryption algorithms, while the secrecy of the system relies solely on the confidentiality of the secret key.

2.6.1. Adversarial capabilities

We assume a computationally powerful adversary with the following capabilities:

a) Complete algorithmic knowledge
The adversary is assumed to know all design details of the scheme, including: the hybrid dyadic–tent chaotic map, the 32-bit quantization procedure, the SHA-256–based whitening mechanism, the permutation–diffusion architecture, and this involves using a public per-image IV that is derived from the image filename.

b) Unknown secret key
The adversary does not know the secret key $K = (x_0, r)$, where x_0 denotes the initial condition and r denotes the control parameter of the chaotic system. These parameters are treated as continuous-valued quantities represented in IEEE-754 double-precision format.

c) Attack models
The adversary may operate under any of the following standard attack scenarios:
- Ciphertext-only attack (COA): access only to encrypted images.
- Known-plaintext attack (KPA): access to one or more plaintext–ciphertext pairs.
- Chosen-plaintext attack (CPA): the ability to select arbitrary plaintext images and obtain their corresponding ciphertexts.

d) Computational resources.
The enemy is assumed to have substantial computational power; however, exhaustive search remains constrained by practical limits of computational feasibility and floating-point precision. This model ensures that the proposed scheme is evaluated under conservative and widely accepted cryptographic assumptions.

2.7. Security evaluation of image encryption algorithm

The security of the proposed scheme is analyzed with respect to the following attack classes: brute force, statistical, differential, and keystream reuse attacks.

2.7.1. Key-space analysis

Key space analysis is conducted to evaluate the resistance of the proposed encryption scheme against brute-force attacks [6]. The secret key of the proposed algorithm mainly consists of the initial condition x_0, the control parameter r, and the transient removal parameter $discard$ of the chaotic system.
All key parameters are assumed to be represented with double-precision floating-point accuracy, which provides a precision of approximately 10^{-15}. The total key space is calculated by considering the valid ranges and precision of each key parameter. A sufficiently large k-space ensures that exhaustive key search attacks are computationally infeasible. We calculate k-pace in the results section.

2.7.2. Histogram analysis

Histogram analysis is employed to evaluate the statistical distribution of pixel intensities in the original and encrypted images [6]. For both grayscale and color images, the frequency of each gray-level value in the range [0, 255] is computed. For color images, the histograms of the red, green, and blue channels are analyzed separately. The histograms of the plain images are compared with those of the corresponding cipher images to examine the ability of the proposed encryption scheme to conceal statistical information. A uniform distribution in the encrypted histogram indicates strong resistance against histogram-based statistical attacks [1].

2.7.3. Correlation analysis

In natural images, there exists a strong correlation among adjacent pixels due to the continuity of visual information [6]. To effectively conceal the structural characteristics of the plain image, an encryption algorithm should significantly reduce this correlation. Therefore, correlation analysis is employed to evaluate the effectiveness of the proposed scheme in decorrelating neighboring pixels. The security of the algorithm is assessed by examining whether the adjacent pixels in the encrypted image are randomly distributed over the entire image region. A low correlation coefficient indicates that the proposed method achieves strong confusion and diffusion properties.

2.7.4. Information entropy and local entropy analysis

Information entropy is employed to evaluate the randomness and unpredictability of the cipher images [6], [10]. A higher entropy value indicates that the encrypted image contains less statistical information and is more resistant to statistical attacks. For an 8-bit image, the information entropy H is defined as: $\mathrm{H} = -\sum_{\mathrm{i}=0}^{255} \mathrm{p(i)} \log_2 \mathrm{p(i)}$, where $p(i)$ denotes the probability of occurrence of pixel value i in the cipher image. For a perfectly random 8-bit image, the theoretical entropy value is 8. To further examine the local randomness of the cipher images, the local information entropy is calculated. The cipher image is first divided into T non-overlapping blocks of equal size. The entropy of each block is then computed, and the local entropy is defined as: $H_{\text{local}} = \frac{1}{T}\sum_{t=1}^{T} H_t$, where H_t represents the entropy of the t-th block.

In the experiments, each cipher image is divided into fixed-size blocks, and the local entropy values are computed to assess the uniformity of randomness in different image regions. High global and local entropy values close to the theoretical limit demonstrate that the proposed scheme produces highly random cipher images and exhibits strong resistance to statistical attacks.

2.7.5. Key sensitivity analysis

We conduct key sensitivity using a wrong-key decryption experiment to evaluate the effect of slight variations in the secret key. A plaintext image is first encrypted using the correct key $K_1 = (x_0, r)$. The resulting ciphertext is then decrypted using both the correct key K_1 and a slightly modified key K_2, where K_2 differs from K_1 by a minimal perturbation in one parameter ($x_0 + 10^{-15}$ or $r + 10^{-15}$), while all other parameters remain unchanged. The correctness of decryption is verified by comparing the reconstructed image with the original image using mean squared error (MSE) and peak signal-to-noise ratio (PSNR). A secure encryption scheme is expected to produce exact reconstruction under the correct key (MSE = 0), while even a negligible deviation in the key should result in complete decryption failure [6], [14].

2.7.6. Number of pixels change rate (NPCR) and unified average changing intensity (UACI) evaluation

To assess the security performance of the proposed encryption scheme, the NPCR and the UACI are employed. These metrics are used to evaluate the avalanche effect and measure the sensitivity of cipher images to slight changes in either the plaintext or the secret key [6]. Let two cipher images be denoted as C_1 and C_2, with image size $M \times N$ and C color channels. The NPCR is defined as:

$$\mathrm{NPCR} = \frac{1}{\mathrm{p}}\sum_{\mathrm{i}=1}^{\mathrm{M}}\sum_{\mathrm{j}-1}^{\mathrm{N}}\sum_{\mathrm{k}=1}^{\mathrm{C}} \mathrm{D(i,j,k)} \times 100\%$$

where $P = M \times N \times C$, and

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

The UACI is calculated as:

$$\mathrm{UACI} = \frac{1}{\mathrm{p}}\sum_{\mathrm{i}=1}^{\mathrm{M}}\sum_{\mathrm{j}=1}^{\mathrm{N}}\sum_{\mathrm{k}=1}^{\mathrm{C}} \frac{|\mathrm{C_1(i,j,k)} - \mathrm{C_2(i,j,k)}|}{255} \times 100\%$$

For grayscale images, $C = 1$, whereas for color images, $C = 3$.

The value 255 represents the maximum pixel intensity for 8-bit images. The metrics were assessed in the following categories;

- NPCR and UACI in the plaintext domain (differential attack)
  To evaluate the resistance of the proposed scheme against differential attacks, NPCR and UACI are first computed in the plaintext domain. Two plain images are generated, where the second image differs from the first by only one pixel. Both images are encrypted using the same secret key to obtain two cipher images.
- The NPCR and UACI values are then calculated between the two cipher images to measure the diffusion capability and avalanche effect in the plaintext domain. High NPCR and UACI values indicate that a slight modification in the plain image results in significant changes in the encrypted image, demonstrating strong resistance to differential attacks [1], [26].
- NPCR and UACI in the key sensitivity domain
  In addition, NPCR and UACI are employed to analyze the sensitivity of the proposed scheme to small variations in secret keys. Two secret keys, denoted as K_1 and K_2, are selected such that they differ only by a very small amount in one chaotic parameter, while all other parameters remain unchanged. Using

these two closely related keys, the same plain image is encrypted separately to generate two corresponding cipher images. The NPCR and UACI values are then computed between these two encrypted images using the same formulas.

This experiment evaluates the avalanche effect in the key domain. High NPCR and UACI values indicate that a slight perturbation in the secret key leads to substantial changes in the cipher image, confirming the high key sensitivity and security of the proposed algorithm [8], [26]. Remark: It should be noted that the two analyses evaluate avalanche properties in the plaintext and key domains, respectively. Therefore, their NPCR and UACI values are not expected to be identical [26].

2.7.7. Noise and occlusion attack analysis

Noise attack: to evaluate the robustness of the proposed encryption scheme against channel noise, a noise attack analysis is performed. Different levels of salt-and-pepper noise are added to the encrypted images to simulate transmission errors and external interference. The noisy cipher images are then decrypted using the correct secret key. The visual quality of the decrypted images is analyzed to determine whether meaningful information can still be recovered under noisy conditions. This experiment evaluates the stability and robustness of the proposed algorithm in practical communication environments [12], [15].

Occlusion attack: occlusion attack analysis is conducted to assess the ability of the proposed scheme to resist partial data loss. In this experiment, certain regions of the encrypted images are deliberately removed or blocked to simulate packet loss and cropping attacks [6], [12], [15]. The occluded cipher images are subsequently decrypted using the correct secret key. The decrypted results are examined to evaluate the impact of partial data loss on image reconstruction and to verify the robustness of the proposed encryption scheme. In the noise attack experiments, salt-and-pepper noise with a density of 0.02 (2% corrupted pixels) is added to the encrypted images to simulate transmission interference.

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[I(i,j) - K(i,j)]^2$$

where:

- I: original image
- K: decrypted image
- $M \times N$: image size

$$PSNR = 10log_{10}\left(\frac{255^2}{MSE}\right)$$

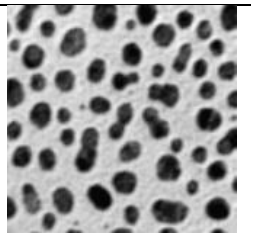
2.8. Time complexity and speed analysis

The computational complexity of the proposed encryption and decryption algorithms is analyzed to evaluate their practical feasibility in real-world applications. Let $L = M \times N \times C$ denote the total number of pixel values in an image, where M and N represent the image dimensions and C denotes the number of color channels. The keystream generation, SHA-256 whitening, permutation, and diffusion processes all require linear traversal of the image data. Consequently, each encryption and decryption operation has a time complexity of $O(L)$, which is consistent with the design principles of efficient chaos-based image encryption schemes reported in recent studies [6], [14]. To further evaluate the practical performance of the proposed scheme, the encryption and decryption times are measured for different test images on a standard computing platform. The average execution time is recorded and analyzed to assess the computational efficiency of the proposed algorithm. Similar experimental setups have been widely adopted in recent image encryption research to validate real-time feasibility and scalability [16], [27].

2.9. Experiment data set

The evaluation was conducted using a compact yet diverse set of standard uncompressed bitmap (BMP) images in Table 2 to avoid compression artifacts and preserve exact pixel values. The dataset includes classical natural images (baboon and cameraman), an astronomical image (earth) representing large-scale structured scenes, and a texture image (blobs) exhibiting repetitive and highly correlated patterns. Both grayscale and RGB images are considered, and multiple spatial resolutions [(256×256, 512×512), and non-square (256×254, 749×768) images] are used to demonstrate support for arbitrary image dimensions. This selection enables a fair assessment of statistical security, differential security, correctness, and performance across diverse image characteristics while keeping the experimental setup reproducible and computationally efficient. All image encryption/decryption experiments are conducted using Python 3 in a Google Colab environment.

Table 2. Image Data to be used in the Analysis

File name	Baboon	Cameraman	Earth	Blobs
Image				
Size RGB/ grayscale	512×512 RGB	256×256 Grayscale	749×768 RGB	256×254 Grayscale

3. RESULTS AND DISCUSSION

To evaluate the chaotic behavior of the proposed hybrid dyadic–tent map, four complementary analyses were conducted. First, the bifurcation diagram was produced by sweeping the control parameter $r \in (0,2)$ to visualize orbit transitions and parameter sensitivity. Second, the Lyapunov exponent curve was computed to quantify the mean exponential divergence of nearby trajectories. Third, a Lyapunov surface (heatmap) $\lambda(r, x_0)$ was generated over a grid of (r, x_0) to assess robustness of chaotic behavior with respect to both the control parameter and the initial condition; for clarity, the colormap is clipped to $[-1.5,1.5]$ and the theoretical threshold at $r = 0.5$ (where $\ln(2r) = 0$) is highlighted. Finally, the NIST randomness test suite, as discussed in 2.5 [10], [28].

3.1. Bifurcation diagram

The bifurcation diagram in Figure 2. shows a transition from structured dynamics at lower r to fully developed chaos as r increases. For $r \lesssim 1$, the orbit occupies a restricted subset of $[0,1]$, indicating incomplete mixing. As r approaches and exceeds unity, the attractor rapidly expands to fill the entire unit interval, with no visible periodic windows, reflecting strong sensitivity to initial conditions and uniform state-space coverage. This behavior confirms that the hybrid dyadic–tent map operates in a robust chaotic regime for the parameter range used in our keystream generator.

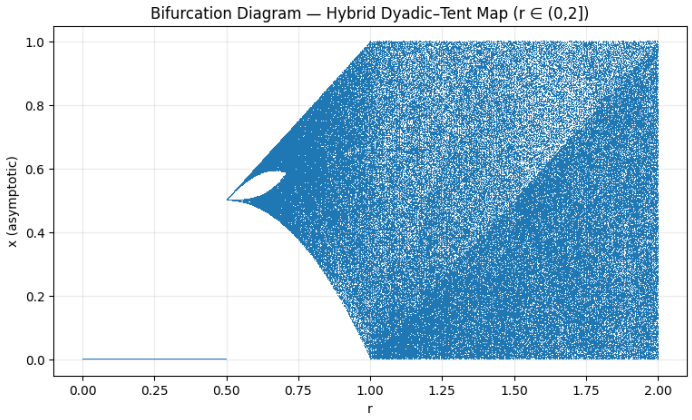


Figure 2. Bifurcation diagram of the composition function [hybrid dyadic-tent map] with parameter r

3.2. The Lyapunov exponent diagram

To quantify the chaotic behaviour of the proposed hybrid dyadic–tent map, we have evaluated its Lyapunov exponent. The Lyapunov exponent measures the average exponential rate of divergence between nearby trajectories. For a one-dimensional smooth map $f: \mathbb{R} \to \mathbb{R}$ generating an orbit: $x_1, x_2, \ldots, x_{i+1} = f(x_i)$, the Lyapunov number is defined as: $L(x_1) = \lim_{n\to\infty} |f'(x_1)f'(x_2)\ldots f'(x_n)|^{\frac{1}{n}}$. If this limit exists and $f'(x_j) \neq 0$, the Lyapunov exponent is: $\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{j=1}^{n} \ln | f'(x_j) |$.

A positive Lyapunov exponent exhibits chaos, since trajectories that start arbitrarily close diverge exponentially; a negative exponent indicates convergence to fixed points or periodic cycles; and values near zero correspond to bifurcation boundaries [9], [29]. In this case, for almost all $x \in (0,1)$, excluding a set of measure zero corresponding to discontinuity points, the derivative of the hybrid map satisfies: $| h'(x) | = 2r$. Consequently, the Lyapunov exponent admits the closed-form expression:

$$\lambda(r) = \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \ln | h'(x_n) | = \ln(2r).$$

This immediately implies a chaos threshold at: $\lambda = 0 \iff r = 0.5$, such that the system is:

– Non-chaotic (contracting) for $0 < r < 0.5$
– Critical at $r = 0.5$
– Chaotic (uniformly expanding) for $r > 0.5$. This validates both the correctness of the implementation and the choice of $r = 1.6$ as a strongly chaotic operating point

To validate the analytical Lyapunov exponent and to ensure robustness under finite precision arithmetic, we compute the numeric Lyapunov exponent via orbit averaging:

$$\lambda_{\text{num}} = \frac{1}{N-N_0} \sum_{n=N_0+1}^{N} \ln | h'(x_n) |,$$

where N_0 denotes the transient (burn-in) length. In the implementation:

– Total iterations: $N = 20{,}000$
– Transient discard: $N_0 = 2{,}000$

The derivative is evaluated branch-wise at each iteration, rather than hard-coding $ln(2r)$, ensuring that the numerical procedure remains valid even under perturbations or future generalizations of the map. This approach follows best practices in numerical chaos analysis. Figure 3 visualizes the results.

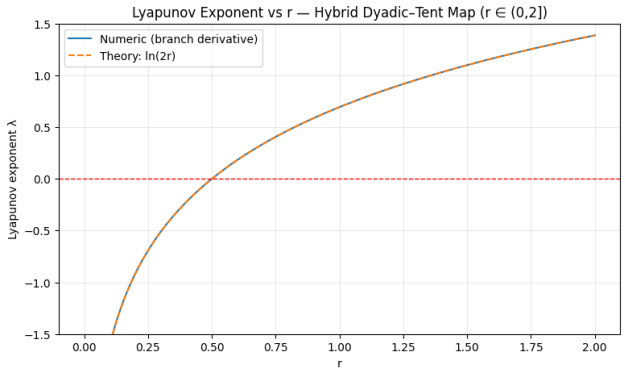


Figure 3. Lyapunov exponent diagram for the hybrid dyadic–tent map over $r \in [0.1,2]$. The lime-colored curve plots λ, and the horizontal line at $\lambda = 0$ marks the transition between periodic and chaotic regimes, in agreement with the theoretical definitions of the Lyapunov number and exponent

3.3. Lyapunov heatmap $\lambda(r, x_0)$

To examine the joint dependence of chaos on the control parameter and initial condition, we compute a two-dimensional Lyapunov surface over: $r \in (0,2)$ (250 points) and $x_0 \in (0,1)$(200 points). Each grid point uses $12{,}000$ iterations, with a $2{,}000$-iteration transient removed. Because $\lambda(r) \to -\infty$as $r \to 0^+$, raw colormap scaling obscures the transition region. Therefore, for visual clarity only, the heatmap is clipped to $\lambda \in [-1.5, 1.5]$, and the theoretical chaos boundary at $r = 0.5$ is explicitly marked. Importantly, this clipping does not alter the computed values and serves purely as a visualization aid, a practice commonly adopted in chaos visualization studies.

Figure 4 shows the Lyapunov exponent heatmap $\lambda(r, x_0)$ for the hybrid dyadic–tent map. The Lyapunov exponent depends primarily on the control parameter $r$and is nearly independent of the initial condition x_0. A clear transition from negative to positive Lyapunov exponents occurs at $r = 0.5$, consistent with the theoretical prediction $\lambda = ln(2r)$. The color scale is clipped to $[-1.5,1.5]$ to emphasize the chaos transition.

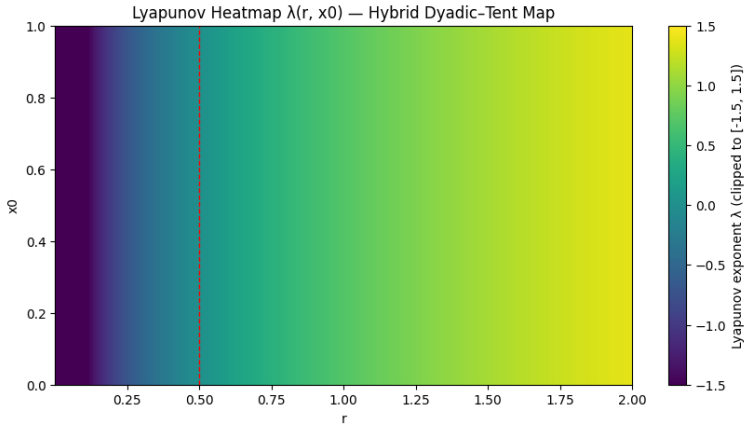


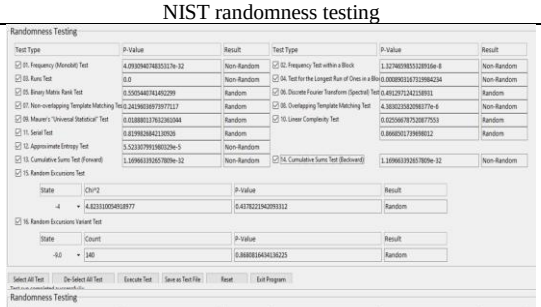
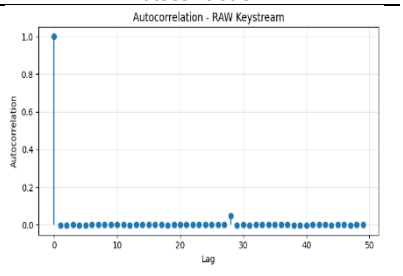
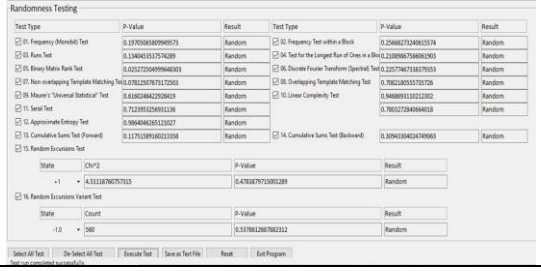
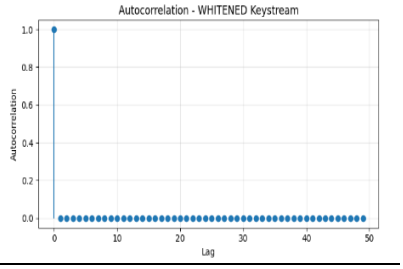
Figure 4. The Lyapunov exponent heatmap

3.4. NIST randomness test results

The randomness properties of the proposed hybrid dyadic–tent map was evaluated using the NIST statistical test suite on both raw and SHA-256–whitened binary sequences of approximately 5 MB. The comparison results are summarized in Table 3.

- The raw chaotic sequence fails several NIST tests, with p-values falling below the significance threshold ($\alpha = 0.01$). This indicates the presence of short-range correlations and insufficient randomness, which is a known limitation of low-dimensional chaotic systems.
- After applying SHA-256 whitening, the keystream successfully passes all NIST tests, with uniformly distributed p-values and acceptable pass proportions. This indicates a significant improvement in statistical randomness.
- The whitening process effectively removes residual patterns and enhances performance across frequency, entropy-based, and pattern-matching tests. Similar improvements through post-processing have been widely reported in recent studies on chaos-based cryptosystems.
- Autocorrelation analysis further supports these results. The maximum absolute autocorrelation decreases from 0.049024 (raw sequence) to 0.000320 (whitened sequence), indicating a substantial reduction in linear dependencies.
- The whitened sequence approaches the behaviour of an ideal random source, making it suitable for cryptographic applications where high randomness is required.

Table 3. NIST test suite results comparison between hybrid dyadic-tent map generated sequences (raw and SHA-256 whitened)

	NIST randomness testing	Autocorrelation
Raw sequence		
SHA-256 whitened sequence		

These results confirm that the whitening mechanism effectively eliminates linear dependencies and enhances resistance to correlation-based cryptanalysis. The byte-value distribution of the composite map keystream, Figure 5, shows a flatter and more uniform histogram as compared to that produced by the tent map/dyadic map alone [18]. The composite structure eliminates visible biases in the byte frequencies and significantly reduces variance, indicating enhanced statistical uniformity. This improvement reflects the fact that function composition strengthens the underlying chaotic behavior by combining the stretching–folding characteristics of both maps [24], [30]. As a result, the hybrid dyadic–tent map produces keystreams with superior randomness quality, making it an excellent candidate for cryptographic applications requiring high unpredictability and uniform statistical distributions.

With values even more closely centered around zero than the tent map, the composite map keystream boasts the better autocorrelation properties. The absence of dominating peaks indicates excellent statistical independence between subsequent data. This confirms the previous observation that the composite map increases the randomness of the tent map. The resulting keystream is secure and unpredictable, making it suitable for encryption systems requiring strong statistical randomness. Table 4 shows the encryption and decryption results for the four test images. The encrypted images show fully randomized pixel patterns with no visible structure, while the decrypted images perfectly match the originals, demonstrating the correctness and reversibility of the proposed hybrid dyadic–tent encryption algorithm.

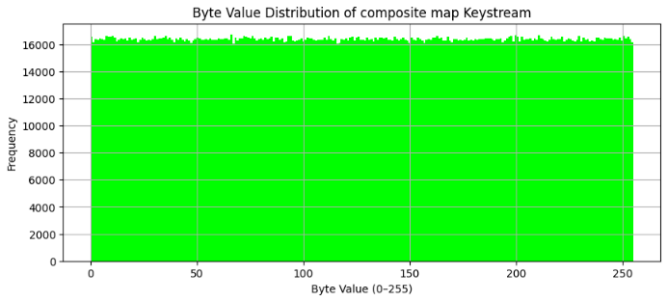


Figure 5. Composite map keystream distribution

Table 4. Encryption and decryption results

Image	Result		
Baboon	Original	Encrypted	Decrypted
Cameraman	Original	Encrypted	Decrypted
Earth	Original	Encrypted	Decrypted
Blobs	Original	Encrypted	Decrypted

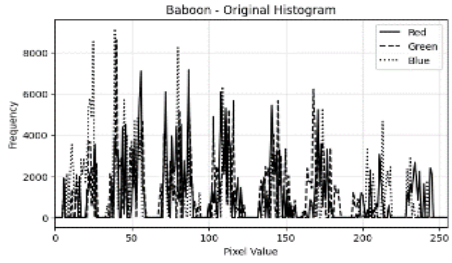
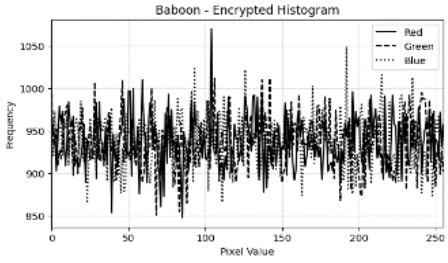
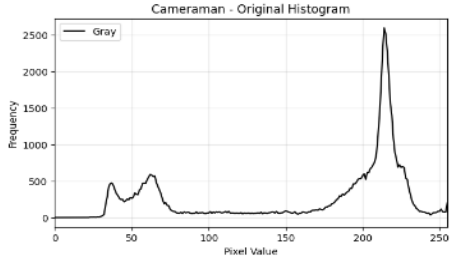
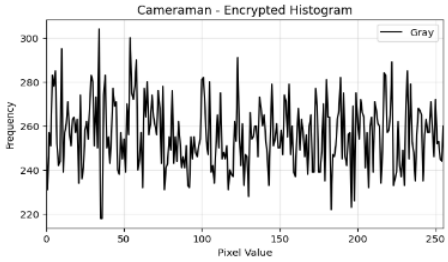
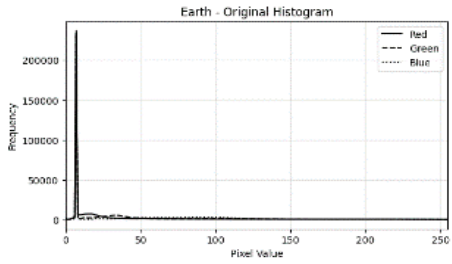
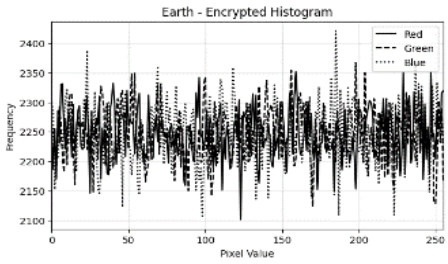
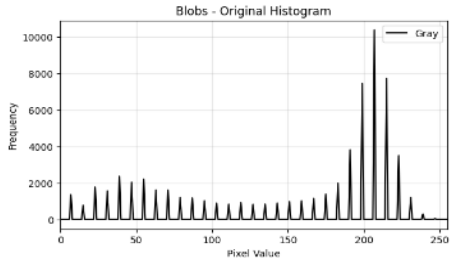
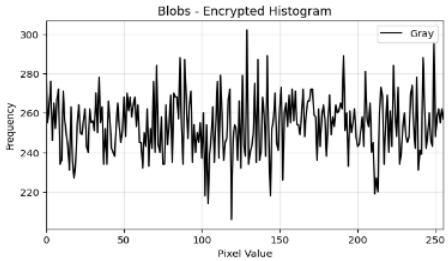
3.5. Key space analysis results

The secret key of the proposed encryption scheme consists of the chaotic initial value x_0, the control parameter r, and the transient removal parameter $discard$. Assuming a computational precision of 10^{-15}, each continuous parameter can provide at least 10^{15} possible values. Consequently, the total key space of the proposed scheme is larger than 10^{45}, which is approximately equivalent to 2^{149}. This key space is significantly greater than the minimum-security requirement of 2^{128} for modern cryptographic systems [6], [31]. Such a large key space makes brute-force attacks computationally infeasible using current and foreseeable computing technologies. Therefore, the proposed encryption algorithm exhibits strong resistance against exhaustive key search attacks.

3.6. The histogram analysis

Table 5 presents the histogram distributions of the original and encrypted images. The original images exhibit highly non-uniform distributions with pronounced peaks, reflecting strong statistical redundancy and inherent pixel correlation. In contrast, the encrypted images show nearly uniform distributions across all intensity levels for both grayscale and RGB channels, with no observable dominant patterns. This noise-like distribution indicates that the proposed encryption scheme effectively suppresses plaintext-dependent statistical characteristics and significantly reduces information leakage. As a result, the ciphertext images exhibit strong resistance against histogram-based statistical attacks, consistent with observations reported in recent studies [9], [10], [20], [32], [33].

Table 5. Visual evidence of pixel randomization through RGB histograms

Image	Histogram	
	Original	Encrypted
Baboon		
Cameraman		
Earth		
Blobs		

3.7. Correlation analysis

The correlation coefficients of adjacent pixels in the horizontal, vertical, and diagonal directions for different test images are summarized in Table 6. The values are reduced from those close to 1 in the original images to near 0 in the encrypted images, demonstrating strong decorrelation capability. This significant reduction indicates that the proposed encryption scheme effectively removes dependencies among neighbouring pixels. As a result, the encrypted images exhibit no predictable relationships between adjacent pixels, ensuring resistance against correlation-based statistical attacks [9], [10], [20], [26].

Table 6. Correlation coefficients of adjacent pixels

Image	Direction	Red		Green		Blue	
		$r_{0riginal}$	$r_{encrypted}$	$r_{0riginal}$	$r_{encrypted}$	$r_{0riginal}$	$r_{encrypted}$
Baboon	Horizontal	0.921207	-0.020585	0.864436	-0.005261	0.746372	-0.007235
	Vertical	0.875919	-0.016692	0.785652	0.005030	0.887077	-0.028206
	Diagonal	0.875279	0.004327	0.746372	-0.007235	0.850677	-0.009936
Cameraman	Horizontal	0.923035	0.007845				
	Vertical	0.947424	-0.021393				
	Diagonal	0.894593	0.001726				
Earth	Horizontal	0.944251	-0.011725	0.947261	-0.002734	0.958799	-0.000040
	Vertical	0.939083	-0.010756	0.947414	0.000575	0.951071	0.000168
	Diagonal	0.911267	-0.000829	0.914341	-0.027285	0.938308	-0.024668
Blobs	Horizontal	0.981271	0.007059				
	Vertical	0.983954	0.017409				
	Diagonal	0.962553	-0.009113				

3.8. Sensitivity analysis

The results of the key sensitivity analysis are summarized in Table 7. Decryption using the correct key K_1 reconstructs the original image exactly, with zero reconstruction error (MSE = 0) and infinite PSNR. In contrast, decryption using slightly modified keys K_2 and K_3 produces completely noise-like images. The corresponding PSNR values range from approximately 6.40 dB to 8.16 dB across all test images, indicating that no meaningful visual information can be recovered. These results demonstrate that even minimal perturbations in the secret key led to complete decryption failure, confirming the high key sensitivity of the proposed scheme. Compared with recent chaos-based image encryption methods, which typically report low PSNR values under wrong-key conditions, the proposed scheme achieves comparable behaviour, indicating effective resistance to key-related attacks [6], [8], [10], [31].

3.9. NPCR and UACI

Table 8 shows the NPCR and UACI results in both the plaintext and secret key domains. In the plaintext domain, NPCR values exceed 99.66% for all test images, which is close to the theoretical ideal of 99.6% for 8-bit images, while UACI values are generally around the expected benchmark of approximately 33%. These results indicate effective diffusion and strong resistance to differential attacks [1], [6]. In the secret key domain, slight perturbations of the key yield NPCR values above 99.58% and UACI values close to 33%, demonstrating high sensitivity of the ciphertext to key variations and confirming a strong avalanche effect. Compared with other studies such as [34], which reports NPCR = 99.6% and UACI = 31.706, the proposed method achieves comparable NPCR performance while producing higher UACI values in most cases, indicating enhanced intensity variation and diffusion capability [1], [6], [32].

3.10. Information entropy

The global and local information entropy values of the encrypted images are presented in Table 9. The global entropy values range from 7.9973 to 7.9999, which are very close to the theoretical maximum value of 8 for 8-bit images. This indicates that the proposed encryption scheme produces cipher images with highly uniform gray-level distributions and effectively eliminates statistical redundancy [6], [29], [35].

The local entropy values range from 7.1756 to 7.7378, showing good but slightly lower randomness at the local level. This suggests that while global diffusion is strong, local mixing can be further improved, likely due to the one-dimensional diffusion structure [14], [30], [35]. Compared with results reported in [36], which show noticeable entropy variation across different regions, the proposed scheme achieves comparable global entropy while maintaining more consistent local entropy levels. These results, together with the NPCR and UACI analysis, indicate strong resistance to statistical and differential attacks.

Table 7. Key sensitivity analysis results (correct key vs. wrong-key decryption using K_2 and K_3)

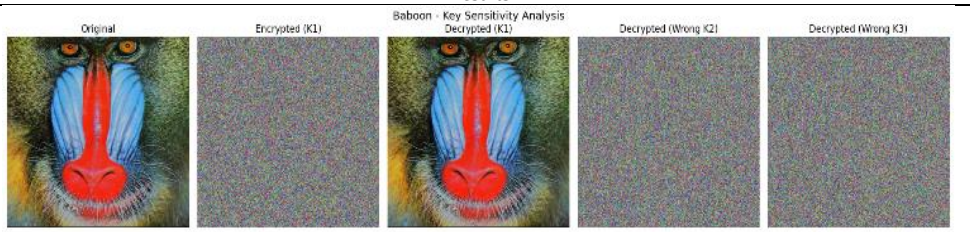
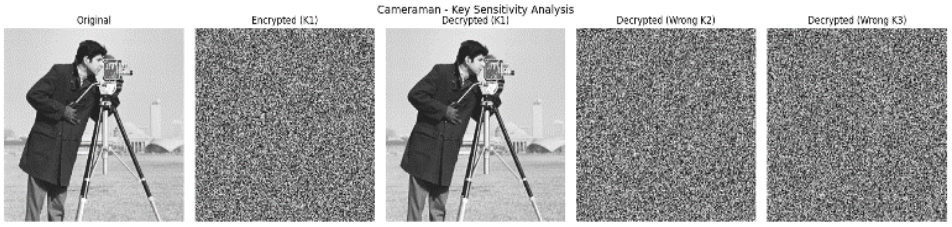
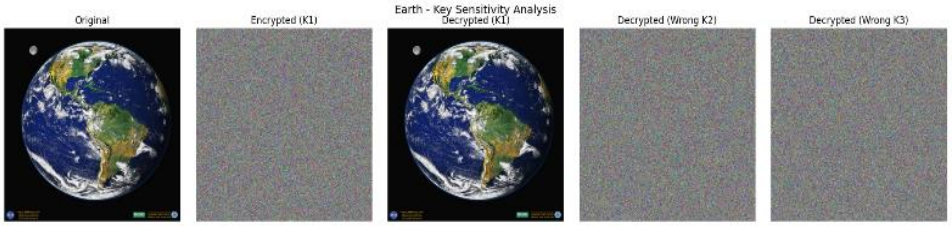
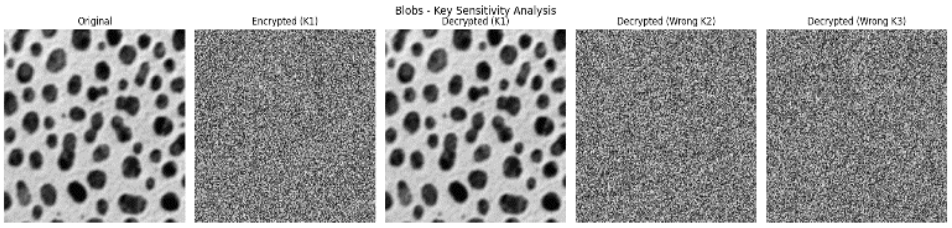
Image	Results
Baboon	
Cameraman	
Earth	
Blobs	

Table 8. NPCR and UACI results for both plaintext and secret key domains

Image	Plaintext domain		Secret key domain	
	NPCR (%)	UACI (%)	NPCR (%)	UACI (%)
Baboon	99.6685	32.1610	99.5972	33.4762
Cameraman	99.8032	42.2708	99.6124	33.3013
Earth	99.6736	35.8294	99.6152	33.4998
Blobs	99.8877	46.6295	99.5894	33.3784

Table 9. Entropy information results

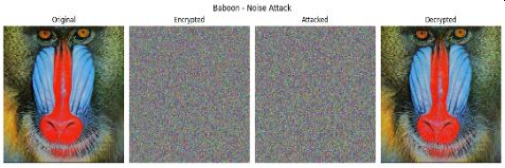
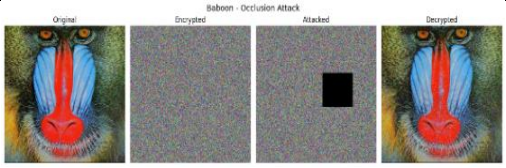
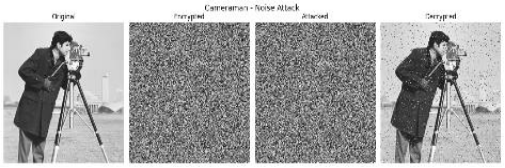
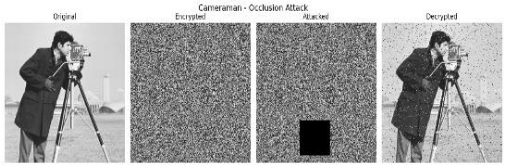
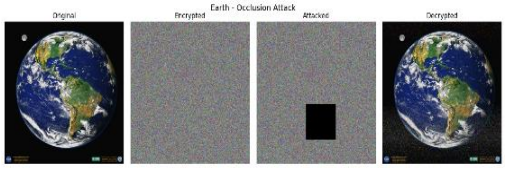
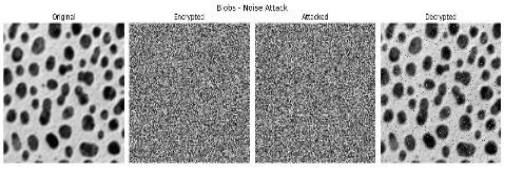
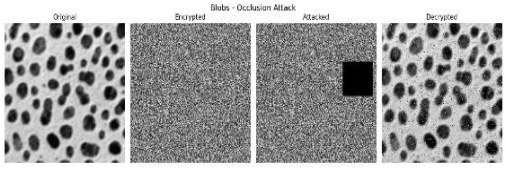
Image	Global	Local
Baboon	7.999765	7.737285
Cameraman	7.997331	7.175586
Earth	7.999889	7.737838
Blobs	7.997381	7.174168

3.11. Noise and occlusion attack analysis

Table 10 displays visual results of this analysis. In the noise attack scenario, the addition of salt-and-pepper noise introduces visible distortion in the ciphertext; however, the decrypted images still preserve the main structural and visual features of the original images. Similarly, under occlusion attacks, where portions of the ciphertext are removed, the decrypted images remain recognizable, with distortion confined to the affected regions. The quantitative results further support these observations. The PSNR values range from approximately 18.9 dB to 20.8 dB under both attack conditions, indicating moderate degradation while maintaining perceptual visibility of image content. The corresponding MSE values remain within a consistent range across different test images, suggesting stable robustness independent of image characteristics [6], [9].

These results demonstrate that the proposed scheme effectively limits error propagation through its permutation–diffusion structure, achieving a practical balance between security and robustness. Consequently, the method is suitable for real-world image transmission scenarios where noise and data loss are unavoidable, consistent with findings in [1], [9], [31], [34].

Table 10. Noise and occlusion attack analysis

Image	Noise attack	Occlusion attack
Baboon		
	MSE = 539.7175 / PSNR = 20.8091 dB	MSE = 583.2725 / PSNR = 20.4721 dB
Cameraman		
	MSE = 633.9344/ PSNR = 20.1104 dB	MSE = 739.4059/ PSNR = 19.4420 dB
Earth		
	MSE = 833.2309 / PSNR = 18.9231 dB	MSE = 809.8518 / PSNR = 19.0467 dB
Blobs		
	MSE = 607.1531/ PSNR = 20.2978 dB	MSE = 692.9781/ PSNR = 19.7236 dB

3.12. Runtime analysis

The runtime analysis in Table 11 confirms the linear computational behavior of the proposed scheme. Encryption and decryption times increase proportionally with image size, which is consistent with the theoretical complexity of $O(M \times N \times C)$. For instance, the 749×768 RGB earth image requires 7.84 s for encryption, whereas smaller 256×256 grayscale and RGB images require less than 0.30 s. The proximity between encryption and decryption times further demonstrates algorithmic symmetry and implementation efficiency. Compared with recently reported hybrid chaotic schemes that incorporate high-dimensional maps or multi-stage diffusion structures often incurring higher computational overhead [1], [4], [8], [35] the proposed dyadic–tent with SHA-256 whitening achieves competitive runtime while maintaining strong security metrics. This balance between security performance and computational cost is particularly important for lightweight and IoT-oriented applications, where excessive structural complexity may hinder practical deployment [5]. Overall, the results indicate that the proposed secret key mechanism and encryption framework are not only secure but also computationally feasible for real-world image transmission systems.

Table 11. Runtime measurement of the encryption and decryption algorithm for grayscale and RGB images, time is measured in seconds

No	Image	Image size	Color mode	Encryption time (s)	Decryption time (s)
1	Baboon	512×512	RGB	2.8742	2.9117
2	Cameraman	256×256	Grayscale	0.2807	0.2688
3	Earth	749×768	RGB	7.8354	6.8025
4	Blobs	256×254	RGB	0.2528	0.2592
	Averages			2.8148	2.5424

3.13. Discussion

The experimental results consistently demonstrate that the proposed hybrid dyadic–tent encryption scheme achieves strong security performance while maintaining computational efficiency. Statistical analyses show near-uniform histograms, entropy values approaching the ideal 8-bit limit, and negligible adjacent pixel correlations, confirming effective confusion and diffusion in accordance with Shannon's cryptographic principles [10], [20], [32], [33]. Differential attack evaluation further yields NPCR values above 99.6% and UACI values centred around the theoretical benchmark (~33%), in both plaintext and secret-key domains. This confirms not only strong diffusion capability but also high key sensitivity, indicating that the secret key structure is suitable and secure for encryption applications [1], [6], [8], [35]. Autocorrelation analysis reveals that SHA-256 whitening significantly suppresses residual dependencies in the raw chaotic sequence, mitigating finite-precision effects and enhancing resistance to statistical cryptanalysis. Robustness tests under noise and occlusion attacks preserve essential visual structures, with PSNR values around 19–21 dB, demonstrating acceptable reconstruction stability. Moreover, runtime measurements confirm linear time complexity $O(M \times N \times C)$ and practical execution times, supporting feasibility for lightweight and resource-constrained environments compared to more complex hyperchaotic designs [4], [29], [34], [36].

Overall, the findings validate that the tightly coupled dyadic–tent composition with integrated SHA-256 whitening provides a balanced trade-off between randomness quality, differential resistance, and computational practicality, positioning the proposed scheme as a secure and lightweight alternative within contemporary chaos-based image encryption research.

– Comparison with other schemes

Single-map chaotic schemes based on logistic and hénon maps are computationally efficient but are known to exhibit finite-precision degradation and residual statistical correlations when implemented digitally [11], [37]–[39]. Hybrid 1D schemes such as logistic–tent combinations improve diffusion and randomness but typically rely on loose map concatenation without explicitly suppressing autocorrelation artifacts [2], [3], [10]. Recent multi-dimensional and hyperchaotic approaches further increase dynamical complexity and key space [1], [4], [9], [29], [31], [35], yet often incur higher computational overhead and structural complexity, limiting suitability for lightweight IoT environments [8].

The proposed dyadic–tent encryption framework tightly couples two one-dimensional chaotic maps with block-level SHA-256 whitening, yielding substantial statistical enhancement while preserving computational efficiency. Specifically, whitening reduces the maximum absolute autocorrelation from 0.049 to 0.00032, driving the keystream behavior close to ideal randomness, while entropy values approach the theoretical 8-bit limit and differential metrics exceed NPCR > 99.6% with UACI near theoretical expectations. At the same time, the algorithm maintains linear time complexity $O(M \times N \times C)$ and operates with a single chaotic state variable and constant auxiliary memory. Unlike hyperchaotic or multi-layer architectures that incur increased computational and memory overhead [1], [4], the proposed design integrates chaotic generation, whitening, permutation, and dual diffusion within a compact and streamlined structure. These characteristics suggest potential suitability for IoT environments [5], [35], indicating practical deployability without sacrificing statistical robustness or security performance. Table 12 gives a brief comparison of the proposed hybrid dyadic-tent with other maps.

Table 12. Comparison table between different maps

Criterion	Logistic	Hénon	Logistic-tent hybrid	Multi-D/hyperchaotic	Proposed hybrid dyadic-tent + SHA256
Representative works	[33]	[34]	[2], [3]	[1], [4]	This study
Dimensionality	1D	2D	1D hybrid	≥ 3D	1D hybrid (tightly coupled)
Whitening layer	No	No	Rare	Sometimes	Yes-integrated SHA-256
Finite-precision mitigation	Weak	Weak	Moderate	Strong	Strong (150 × AC reduction)
Entropy performance	< 8	~ 8	~ 8	~ 8	≈ 8 (near ideal)
NPCR / UACI	High	High	High	High	High (plaintext and key domains)
Computational overhead	Low	Moderate	Low-moderate	High	Low (linear O(L))
Suitability for IoT	High	Moderate	Moderate	Limited	High
Overall position	Lightweight but weaker randomness	Improved complexity	Improved diffusion	High security, heavy cost	Balanced security + lightweight design

4. CONCLUSION

This paper introduces and analyzes a new hybrid dyadic–tent chaotic map, defined through functional composition, and demonstrates its application within a lightweight image encryption scheme enhanced by SHA-256 whitening. The primary novelty of this work lies in the introduction of this newly defined one-dimensional chaotic map, whose dynamics can be analytically characterized via a closed-form Lyapunov exponent, as well as in its systematic integration with cryptographic whitening to achieve statistically robust keystream generation. The experimental results show that the proposed framework provides strong statistical security. This includes entropy values that are close to the theoretical limit, very little pixel correlation, NPCR values that are higher than 99.6%, and effective suppression of keystream autocorrelation. Furthermore, the algorithm used preserves linear time complexity $O(M \times N \times C)$ while maintaining a compact one-dimensional structure, providing a practical balance between security strength and computational efficiency for lightweight image encryption applications.

Despite these encouraging results, several limitations should be acknowledged. First, the proposed encryption scheme is validated through software-based simulations using a finite set of benchmark grayscale and RGB images, and no hardware or real-time implementation is considered. Second, the security evaluation focuses primarily on statistical, differential, and key-sensitivity analyses; formal cryptographic proofs and resistance against side-channel attacks are beyond the scope of this study. In addition, although the scheme is designed for lightweight image encryption, direct performance comparisons with standardized block ciphers such as AES were not conducted, as the objective is not to replace conventional cryptosystems but to provide an efficient alternative for resource-constrained multimedia environments.

Finally, while the newly proposed chaotic map exhibits robust chaotic behavior when enhanced through hybridization and SHA-256 whitening, its digital implementation may still be influenced by finite-precision effects inherent in floating-point arithmetic. Future work will focus on hardware implementation on field-programmable gate array (FPGA) and IoT platforms, extended evaluation on larger and more diverse datasets, formal security analysis under advanced attack models, and further exploration of adaptive chaotic parameter strategies to enhance robustness without increasing structural complexity.

FUNDING INFORMATION

Authors state that they personally funded the project.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Anymore Majere	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
Hiento Suharja		✓				✓		✓	✓	✓	✓	✓		✓
Suryadi MT	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The Authors state no conflict of interest.

DATA AVAILABILITY

Available from the corresponding author, AM, upon reasonable request.

REFERENCES

[1] Y. H. Huang, Q. L. Zhang, and Y. B. Zhao, "Color image encryption algorithm based on hybrid chaos and layered strategies," *Journal of Information Security and Applications*, vol. 89, p. 103921, Mar. 2025, doi: 10.1016/j.jisa.2024.103921.
[2] M. Jiang and H. Yang, "Image Encryption Using a New Hybrid Chaotic Map and Spiral Transformation," *Entropy*, vol. 25, no.

11, p. 1516, Nov. 2023, doi: 10.3390/e25111516.
[3] R. Munir, "Combining Two Chaos Maps and Determining Selective Methods for MSB Bits in a Digital Image Encryption Algorithm," *Journal of Multimedia Trend and Technology*, vol. 3, no. 3, pp. 166–175, Dec. 2024, doi: 10.35671/jmtt.v3i3.63.
[4] A. Panwar, G. Biban, R. Chugh, A. Tassaddiq, and R. Alharbi, "An efficient image encryption model based on 6D hyperchaotic system and symmetric matrix for color and gray images," *Heliyon*, vol. 10, no. 11, p. e31618, Jun. 2024, doi: 10.1016/j.heliyon.2024.e31618.
[5] S. A. Ansari and S. Ali, "A systematic review of lightweight cryptographic schemes for security and privacy in IoT," *Discover Computing*, vol. 28, no. 1, p. 266, Nov. 2025, doi: 10.1007/s10791-025-09755-3.
[6] B. Zhang and L. Liu, "Chaos-Based Image Encryption: Review, Application, and Challenges," *Mathematics*, vol. 11, no. 11, p. 2585, Jun. 2023, doi: 10.3390/math11112585.
[7] M. Yesilyurt and Y. Yalman, "Security threats on mobile devices and their effects: Estimations for the future," *International Journal of Security and its Applications*, vol. 10, no. 2, pp. 13–26, Feb. 2016, doi: 10.14257/ijsia.2016.10.2.02.
[8] M. T. Elkandoz and W. Alexan, "Image encryption based on a combination of multiple chaotic maps," *Multimedia Tools and Applications*, vol. 81, no. 18, pp. 25497–25518, Jul. 2022, doi: 10.1007/s11042-022-12595-8.
[9] H. Wen, Y. Lin, S. Kang, X. Zhang, and K. Zou, "Secure image encryption algorithm using chaos-based block permutation and weighted bit planes chain diffusion," *iScience*, vol. 27, no. 1, p. 108610, Jan. 2024, doi: 10.1016/j.isci.2023.108610.
[10] D. Sweetania, M. T. Suryadi, and S. Madenda, "Development of a New Chaotic Function-based Algorithm for Encrypting Digital Images," *International Journal of Advanced Computer Science and Applications*, vol. 15, no. 4, pp. 264–269, 2024, doi: 10.14569/IJACSA.2024.0150427.
[11] V. Patidar, N. K. Pareek, and K. K. Sud, "A new substitution-diffusion based image cipher using chaotic standard and logistic maps," *Communications in Nonlinear Science and Numerical Simulation*, vol. 14, no. 7, pp. 3056–3075, Jul. 2009, doi: 10.1016/j.cnsns.2008.11.005.
[12] M. Alawida, "A novel chaos-based permutation for image encryption," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 6, p. 101595, Jun. 2023, doi: 10.1016/j.jksuci.2023.101595.
[13] I. Yasser, F. Khalifa, M. A. Mohamed, and A. S. Samrah, "A New Image Encryption Scheme Based on Hybrid Chaotic Maps," *Complexity*, vol. 2020, pp. 1–23, Jul. 2020, doi: 10.1155/2020/9597619.
[14] C. Wang and L. Song, "An image encryption scheme based on chaotic system and compressed sensing for multiple application scenarios," *Information Sciences*, vol. 642, p. 119166, Sep. 2023, doi: 10.1016/j.ins.2023.119166.
[15] H. Wang, D. Xiao, X. Chen, and H. Huang, "Cryptanalysis and enhancements of image encryption using combination of the 1D chaotic map," *Signal Processing*, vol. 144, pp. 444–452, Mar. 2018, doi: 10.1016/j.sigpro.2017.11.005.
[16] E. Güvenoğlu, "An image encryption algorithm based on multi-layered chaotic maps and its security analysis," *Connection Science*, vol. 36, no. 1, Dec. 2024, doi: 10.1080/09540091.2024.2312108.
[17] A. H. Khaleel and I. Q. Abduljaleel, "Chaotic Image Cryptography Systems: A Review," *Samarra Journal of Pure and Applied Science*, vol. 3, no. 2, pp. 129–143, Sep. 2021, doi: 10.54153/sjpas.2021.v3i2.244.
[18] M. J. Jaber, Z. J. Jaber, and A. J. Obaid, "An efficient hybrid chaotic map-based encryption technique for multiple image security systems," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 5, pp. 1507–1522, 2024, doi: 10.47974/JDMSC-1934.
[19] L. A. Baxter, "Chaos, Fractals, and Noise: Stochastic Aspects of Dynamics, Second Edition, 1994, by Andrzej Lasota and Michael C. Mackey, Applied Mathematical Sciences, vol. 97 (New York: Springer-Verlag), xiv + 472 pp.," *Probability in the Engineering and Informational Sciences*, vol. 10, no. 2, pp. 311–313, Apr. 1996, doi: 10.1017/s0269964800004368.
[20] M. Mudrika, S. Mt, and S. Madenda, "New chaos function of composition function Gauss map and dyadic transformation map for digital image encryption," *ITM Web of Conferences*, vol. 61, p. 01004, Jan. 2024, doi: 10.1051/itmconf/20246101004.
[21] R. L. Devaney, *An introduction to chaotic dynamical systems: Second Edition*. CRC Press, 2018. doi: 10.4324/9780429502309.
[22] R. L. Devaney, "An introduction to chaotic dynamical systems," *Acta Applicandae Mathematica*, vol. 19, no. 2, pp. 204–205, May 1990, doi: 10.1007/bf00049580..
[23] U. Shahid, S. Kanwal, M. Bano, S. Inam, M. E. M. Abdalla, and Z. A. Shaikh, "Blockchain driven medical image encryption employing chaotic tent map in cloud computing," *Scientific Reports*, vol. 15, no. 1, p. 6236, Feb. 2025, doi: 10.1038/s41598-025-90502-5.
[24] N. Khalil, A. Sarhan, and M. A. M. Alshewimy, "An efficient color/grayscale image encryption scheme based on hybrid chaotic maps," *Optics and Laser Technology*, vol. 143, p. 107326, Nov. 2021, doi: 10.1016/j.optlastec.2021.107326.
[25] S. Ang, "randomness_testsuite: Python implementation of NIST's statistical test suite for random and pseudorandom number generators for cryptographic applications," *GitHub repository*, 2021. [Online]. Available: https://github.com/stevenang/randomness_testsuite. (accessed May 14, 2025).
[26] R. Saidi, N. Cherrid, T. Bentahar, H. Mayache, and A. Bentahar, "Number of pixel change rate and unified average changing intensity for sensitivity analysis of encrypted inSAR interferogram," *Ingenierie des Systemes d'Information*, vol. 25, no. 5, pp. 601–607, Nov. 2020, doi: 10.18280/ISI.250507.
[27] C. Fu, G. Y. Zhang, M. Zhu, J. X. Chen, and W. M. Lei, "A fast chaos-based colour image encryption algorithm using a hash function," *Informatica (Netherlands)*, vol. 29, no. 4, pp. 651–673, Jan. 2018, doi: 10.15388/Informatica.2018.186.
[28] L. E. Bassham *et al.*, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Gaithersburg, MD, 2010. doi: 10.6028/NIST.SP.800-22r1a.
[29] M. Riaz *et al.*, "Secure and Fast Image Encryption Algorithm Based on Modified Logistic Map," *Information (Switzerland)*, vol. 15, no. 3, p. 172, Mar. 2024, doi: 10.3390/info15030172.
[30] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International Journal of Bifurcation and Chaos*, vol. 16, no. 8, pp. 2129–2151, Aug. 2006, doi: 10.1142/S0218127406015970.
[31] M. Gabr, R. Elias, K. M. Hosny, G. A. Papakostas, and W. Alexan, "Image Encryption via Base-n PRNGs and Parallel Base-n S-Boxes," *IEEE Access*, vol. 11, pp. 85002–85030, 2023, doi: 10.1109/ACCESS.2023.3301460.
[32] J. A. Vargas Valencia, M. A. Londoño-Arboleda, H. D. Salinas Jiménez, C. A. Marín Arango, and L. F. Duque Gómez, "Image Encryption Using Chaotic Box Partition–Permutation and Modular Diffusion with PBKDF2 Key Derivation," *Journal of Cybersecurity and Privacy*, vol. 6, no. 1, p. 21, Jan. 2026, doi: 10.3390/jcp6010021.
[33] S. A. S. Almola, H. A. Younis, and R. S. Khudeyer, "A Robust Image Encryption Framework Using Deep Feature Extraction and AES Key Optimization," *Cryptography*, vol. 10, no. 2, p. 16, Mar. 2026, doi: 10.3390/cryptography10020016.
[34] W. Alexan, E. A. Maher, E. Mamdouh, M. Youssef, and N. Ehab, "A chaos-based augmented image encryption scheme for satellite images using Fredkin logic," *Scientific Reports*, vol. 15, no. 1, p. 37345, Oct. 2025, doi: 10.1038/s41598-025-22008-z.
[35] A. N. Latifa, C. A. Sari, E. H. Rachmawanto, and M. K. Sarker, "Multi-Level Secure Image Cryptosystem Using Logistic Map

Chaos: Entropy, Correlation, and 3D Histogram Validation," *Jurnal Masyarakat Informatika*, vol. 16, no. 2, pp. 247–267, Nov. 2025, doi: 10.14710/jmasif.16.2.74537.
[36] J. Arif *et al.*, "A Novel Chaotic Permutation-Substitution Image Encryption Scheme Based on Logistic Map and Random Substitution," *IEEE Access*, vol. 10, pp. 12966–12982, 2022, doi: 10.1109/ACCESS.2022.3146792.
[37] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Image and Vision Computing*, vol. 24, no. 9, pp. 926–934, Sep. 2006, doi: 10.1016/j.imavis.2006.02.021.
[38] G. Alvarez and S. Li, "Breaking an encryption scheme based on chaotic baker map," *Physics Letters, Section A: General, Atomic and Solid State Physics*, vol. 352, no. 1–2, pp. 78–82, Mar. 2006, doi: 10.1016/j.physleta.2005.11.055.
[39] S. Zhu, C. Zhu, and W. Wang, "A new image encryption algorithm based on chaos and secure hash SHA-256," *Entropy*, vol. 20, no. 9, p. 716, Sep. 2018, doi: 10.3390/e20090716.

BIOGRAPHIES OF AUTHORS

Anymore Majere is a graduate student pursuing a Master's degree in Mathematics at Universitas Indonesia, with a focus on mathematical modeling and its applications in epidemiology and security systems. She holds a Bachelor of Science in Mathematics and Statistics from the Zimbabwe Open University (2023). In addition to her academic work, she serves as a crime investigation officer with the Zimbabwe Republic Police. Her research interests include cryptography, dynamical systems, data science, and computational modeling. She presented her work at the IndoMS International Conference on Mathematics and Applications (IICMA). In this study, she contributed to the design of the hybrid chaotic model, implementation of the encryption algorithm, and experimental evaluation. She can be contacted at email: anymoremajere2@gmail.com, anymore.majere@ui.ac.id.

Hiento Suharja received his B.Sc. degree in Industrial Technology from Atma Jaya Catholic University, Jakarta, and is currently pursuing an M.Sc. degree in Mathematics at the University of Indonesia (2024). Alongside his postgraduate studies, he serves as a member of the Teaching, Learning, and Curriculum team at Citra Kasih School, where he actively contributes to advancing educational quality and supporting effective learning processes. His academic and professional interests have led him to focus on malaria modelling, reflecting his passion for applying mathematical approaches to real-world health challenges. He can be contacted at email: hiento.suharja@citrakasih.sch.id, hiento.suharja@ui.ac.id.

Suryadi MT received the B.Sc. degree in Mathematics from the Faculty of Mathematics and Natural Sciences, Universitas Indonesia, Indonesia, in 1990, the M.Sc. degree in Informatics Engineering from the Bandung Institute of Technology, Indonesia, in 1998, and the D.Phil. degree from the Department of Electrical and Computer Engineering, Universitas Indonesia, in 2013. He is currently a Professor in the field of Data Security Science at the Department of Mathematics, Faculty of Mathematics and Natural Sciences, Universitas Indonesia. Currently he is also the head of the research center for cyber-information security and intelligent transportation systems at the Department of Mathematics, Faculty of Mathematics and Natural Sciences, Universitas Indonesia. He is the author or coauthor of more than 55 papers published in prominent international journals and conference proceedings, has written three books, and has contributed a chapter to a book. His current research interests include information security, cryptography, and computational mathematics. He can be contacted at email: yadi.mt@sci.ui.ac.id.