Scientific Reports

https://doi.org/10.1038/s41598-026-43981-z

Article in Press

SCD-CHAOS: dynamic S-box and chaotic hybrid adaptive image encryption using multi-map diffusion

Received: 3 December 2025

Accepted: 9 March 2026

Published online: 02 April 2026

Cite this article as: Yogi B., Majumdar R., Ghosh P. *et al.* SCD-CHAOS: dynamic S-box and chaotic hybrid adaptive image encryption using multi-map diffusion. *Sci Rep* (2026). https://doi.org/10.1038/s41598-026-43981-z

Biswarup Yogi, Raj Majumdar, Pritha Ghosh, Lokesh Sharma & Satyabrata Roy

SCD-CHAOS: Dynamic S-box and Chaotic Hybrid Adaptive Image Encryption Using Multi-Map Diffusion

Biswarup Yogi[1], Raj Majumdar[1], Pritha Ghosh[1], Lokesh Sharma[2*], Satyabrata Roy[3]

[1]Department of Computational Sciences, Brainware University, Kolkata, 700109, West Bengal, India.

[2*]Department of Information Technology, Manipal University Jaipur, Jaipur, 303007, Rajasthan, India.

[3]Department of Computer Science and Engineering, Manipal University Jaipur, Jaipur, 303007, Rajasthan, India.

*Corresponding author(s). E-mail(s): lokesh.sharma@jaipur.manipal.edu;
Contributing authors: biswarup23yogi@gmail.com; researchworkraj678@gmail.com; researchworkpritha678@gmail.com; satyabrata.roy@jaipur.manipal.edu;

Abstract

The rapid growth of Internet of Things (IoT) devices has increased the demand for encryption techniques that simultaneously ensure high security strength with low computational complexity and real-time feasibility under resource constraints. The proposed SCD–CHAOS, a novel hybrid chaotic image encryption technique that combines dual chaotic dynamics based on the Tent and Henon maps with an entropy-driven adaptive dynamic S-Box mechanism. Unlike traditional chaos-based permutation–diffusion architectures which rely on static substitution structures, the proposed technique introduces entropy-guided nonlinear transformation combined with hybrid chaotic key synthesis to significantly improve confusion capability, diffusion uniformity, and key sensitivity while preserving deterministic reversibility. For the purpose of standardized benchmarking and computational efficiency in IoT environments, the input images are uniformly down-scaled to $\mathbf{64 \times 64}$ prior to encryption. Various experimental evaluations of the benchmark images demonstrate a near-ideal entropy in average of 7.9991 bits, Number of Pixels Change Rate average 99.6226%, unified average change intensity reaching average of 33.4732%, and correlation coefficients of encrypted images approaching zero in all directions, confirming strong resistance against statistical and differential attacks. Key sensitivity analysis achieves NPCR/ UACI values of up to 99.6221% and 33.4717%, respectively. The Lyapunov exponent analysis reports robust chaotic behavior with values of up to 1.4628. The detection performance shows a structural similarity index in average of 0.9994 for original vs Decrypted images, peak signal-to-noise ratio mean of 9.6250dB, and mean Square Error mean of around 6904.83. The encryption and decryption processes require only 0.00619 seconds and 0.00261 seconds for $\mathbf{64 \times 64}$ images, demonstrating real-time feasibility, making SCD-CHAOS a robust and scalable encryption technique for secure image transmission in next-generation IoT networks.

Keywords: IoT Security, Image Encryption, Chaotic Maps, Hybrid Cryptosystem, Lightweight Encryption, Dynamic S-Box, Data Privacy, Secure Transmission

1 Introduction

The Internet of Things (IoT) [1] has developed into a vast digital ecosystem by linking everyday devices, machines, and sensors across industries, healthcare and homes. This continuous interconnect

creates a massive amount of data moving through open communication channels without adequate protection. This reason raises serious concerns about privacy, interception, and malicious manipulation. Because IoT nodes are usually constrained by low processing power, limited memory, and restricted energy capacity, most conventional encryption methods cannot be implemented efficiently. Therefore, designing and creating secure and lightweight cryptographic techniques that meet the real time requirements of IoT systems has become the most important research concern.

Traditional encryption techniques, including AES, RSA and DES [2], provide reliable security, but require high computational power and complex key operations, making them impractical for small embedded platforms. In contrast, chaos based cryptography [3] has gained so much attention due to its ability to create unpredictable, nonlinear sequences that provide strong diffusion and confusion. These characteristics help to maintain encryption strength while keeping low computational costs and making them attractive for constrained IoT devices.

Recent studies have focused highly on hybrid chaotic maps [4] and dynamically generated substitution boxes such as S-boxes to improve key sensitivity and statistical randomness [5]. However, combining high security with computational efficiency remains a major difficulty. As summarized in Section 2, existing schemes typically emphasize stronger diffusion and higher entropy through complex multistage chaotic processing, adaptive key modulation, or multi-dimensional substitution structures. Although these designs are not sufficiently resistant to attacks, they can also introduce heavy computational consumption, high complexity, or processing delay. Other frameworks explore DNA encoding, fractional transformations, or algebraic optimization to expand the key space, yet these strategies generally sacrifice speed and scalability. Collectively, previous research demonstrates that a truly balanced approach—one that maintains cryptographic strength without increasing system load—is still needed for practical IoT image protection.

To address these challenges, this paper proposes a Dynamic S-box and Chaotic Hybrid Adaptive Image Encryption (SCD-CHAOS) framework that integrates the Tent and Henon maps under entropy-driven adaptive control. Unlike traditional techniques that separate permutation, diffusion, and substitution, the proposed SCD-CHAOS technique synchronizes all three within a unified chaotic control loop. The interaction between the spatial scrambling ability of the Tent map and the nonlinearity of the Henon map ensures a wide key space, high unpredictability and strong resistance to attacks. A dynamic S-Box obtained from hybrid key sequence further improves the nonlinearity and statistical randomness. The design provides a lightweight, fully reversible and suitable for real-time IoT image encryption.

The main contributions and novelties of this proposed technique are as follows:

- Introducing a hybrid chaotic image encryption method that combines Tent and Henon maps to offer high security at low computational cost.
- Development of an entropy-based adaptive control system, which automatically adjusts the relation between the key generation and the substitution strength depending on the image.
- Design of a dynamic S-box that evolves at every encryption process, thus removing fixed substitution patterns and greatly increasing resistance to chosen-plaintext and differential attacks.
- Combining permutation, diffusion, and confusion operations in a single adaptive chaotic pipeline leads to better uniformity and key sensitivity using lightweight XOR-based diffusion driven by hybrid chaotic sequences, which is a low-cost solution from the computational point of view while maintaining a high level of security.
- Ensure complete reversibility and deterministic decryption symmetry, guaranteeing lossless recovery under identical key conditions.

The remainder of this paper is organized as follows. Section 2 reviews related encryption methods. Section 3 describes the preliminaries significances in the proposed technique, including hybrid key generation and preprocessing in Section 3.1, adaptive keystream and substitution mapping in Section 3.2, and permutation–diffusion–confusion encryption in Section 3.3. Section 4 provides the details of the proposed SCD-CHAOS system including the proposed encryption workflow in Section 4.1 and the decryption workflow in Section 4.2, also the algorithmic implementation is given in Subsection 4.3 and Section 5 presents experimental analysis with configurations and specifications , and Finally Section 7 concludes the paper with directions for future work.

2 Related Work

Kanwal et al. [6] introduced an image encryption system that uses a sine map for permutation, a Hill cipher with circulant matrices for substitution, and a chaotic tent map for diffusion. The method is very effective against statistical and differential attacks and thus offers high values for key space, NPCR, UACI, and entropy. But the technique struggles with large images because its multi-stage operations are highly resource-intensive and require significant computational power; thus, real-time performance may be compromised, and its use in high-throughput systems may be limited.

Chen et al. [7] proposed a hybrid encryption scheme that merges an enhanced 2D Henon map (2D-ICHM), integer wavelet transform, bit-plane decomposition, and DNA-based operations. The twin sandwich configuration ensures effective scrambling and diffusion of the image in both spatial and frequency domains. However, the method is computationally intensive, and adjusting chaotic parameters for large images reduces processing speed; thus, it isn't easy to use it for real-time applications or in resource-constrained environments with large datasets.

Zheng et al. [8] presented a cryptographic approach utilising dynamic S-boxes and 2D Logistic-Sine-Coupling Maps (2D-LACM). The method features four stages — key generation, S-box construction, permutation, and diffusion — and exhibits a very high level of security, making it highly resistant to various types of attacks. However, the repeated chaotic mapping and S-box generation are computationally expensive, so processing large or high-resolution images is slow, which limits the method's use in real-time encryption scenarios, although it is pretty efficient for standard-sized images.

Akraam et al. [9] introduced an evolutionary-based encryption system that employed a 2D Henon map whose parameters were optimised by the Imperialist Competitive Algorithm (ICA). The technique generates unique pseudorandom sequences for each image, thereby improving security. The implementation of ICA incurs significant computational overhead, which may limit the system's scalability for large datasets or real-time communication. Though the method offers robust security, it requires substantial resources and carefully tuned parameters, making the implementation complex.

Rezaei et al. [10] proposed a noise-resistant S-box building method through a 3D improved quadratic map (3D-IQM). The technique alters randomness, diffusion, and attack resistance by using multiple keyed S-boxes and a deep substitution sequence. Nevertheless, the method is highly memory- and computationally resource-intensive due to the iterative substitutions. Thus it is more likely to be unsuitable for low-resource devices or real-time systems, although high encryption strength in the colour channels has been achieved.

Liu et al. [11] have implemented a fingerprint image encryption strategy that combines the Pseudo-Hadamard transformation, the Skew-Tent chaotic substitution, and S-box-based pixel-position variation. The technique essentially changes inter-pixel redundancy, making it very efficient at diffusion and confusion. The problem with the method, however, is its capacity for generalisation, since it is explicitly designed for biometric images, and its performance decreases with larger datasets; hence, scalability issues might arise. Still, the method is a trustworthy security measure for fingerprint authentication systems.

Kulkarni et al. [12] designed an encryption algorithm where they used the Arnold Cat Map for permutation and the Henon Map for diffusion. To confuse and diffuse the data, the method was extended, thus increasing the security. However, there are some limitations, such as the quality of the cipher sometimes degrading and image fidelity being reduced, which may affect decryption efficiency. Also, it is critical to select the correct parameters for the chaotic map, thereby reducing the available freedom. Although it is excellent for typical images, the method may struggle with diverse image types or large-scale datasets.

Mohammad et al. [13] have designed a hyperchaotic SVD-RC5-based encryption method for satellite imagery that employs multi-stage permutation and S-box operations. The technique is safe from traffic analysis and statistical attacks, thus it offers strong security. But the multi-stage processing and large augmented images require significant computational and memory resources, so the method cannot be used in real time or on low-resource systems. Nevertheless, the process can provide strong encryption and privacy protection for sensitive satellite images.

Youssef et al. [14] introduced a blockchain-powered Chaotic Tent Map Encryption Scheme (BCTMES) to protect images stored in the cloud. The system combines the unchangeability of blockchain with the unpredictability of encryption to provide the highest level of confidentiality, integrity, and resistance to attacks. On the other hand, the downside of such a method is that blockchain operations introduce additional latency and computational overhead, which can even

degrade the system's real-time performance. Additionally, efficiency is reduced by increased resource consumption for consensus and encryption, thereby limiting the performance of high-throughput or latency-sensitive cloud applications.

Shahid et al. [15] enhanced a Henon-map-based cryptosystem with algebraic structures to expand the key space, improve diffusion, and increase overall security. Substitution boxes constructed over a Galois field are responsible for the increased strength and the higher level of the attacker's resistance. The technique has complicated key management and requires proper tuning of algebraic parameters, which might pose a usability problem in resource-constrained settings. As a result of these practical issues, the system is robust, capable of encrypting electronic images, and thus resistant to statistical and differential attacks.

Mohi Ud Din et al. [16] developed cryptographically resilient S-boxes via fractional transformations for block-cipher-based image encryption; their technique yields high nonlinearity, low differential uniformity, and resistance to attacks. This method's computation is very intensive, especially for larger images; thus, its performance is diminished in high-resolution or large-scale datasets. While it is powerful for normal images, the method's inefficiency might limit its use in real-time applications or large systems.

Ali et al. [17] proposed an image encryption scheme, where Extended Fractional Transformation (EFT)-based S-boxes were used for pixel substitution and shuffling. The technique enhances security, nonlinearity, and the system's resistance to cryptanalysis. However, it slows the entire process, and the computational requirements become quite heavy as image resolution increases, making it challenging for real-time applications. Also, the method's robustness depends on parameter optimisation. In any case, the process still provides strong diffusion and confusion, thus it is capable of effectively securing images of different types.

Table 1 summarises these studies, describing the main performance metrics—MSE, PSNR, UACI, NPCR, correlation, and entropy—to provide a comparative view of the latest developments and their impact on the strength and efficiency of image encryption.

Author	MSE	PSNR	NPCR	UACI	Correlation	Entropy	Technology Used	Year
Malik et al.[18]	✗	✗	✗	✗	✗	✗	Tent + Sine Chaotic Map (Compound Chaotic Map for S-box generation)	2023
Ali et al.[19]	✓	✓	✓	✓	✓	✓	Dynamic Chaotic Map + DNA Coding + Zigzag Pattern Encryption	2024
Vijayakumar et al.[20]	✓	✓	✓	✓	✓	✓	4D Memristive Hyperchaotic Map + Cellular Automata (CA) based S-box	2024
Hazzazi et al.[21]	✓	✓	✓	✓	✓	✓	Tent–May Chaotic Map + Bit-Level Permutation (Hybrid Chaotic S-box)	2024
Alali et al.[22]	✓	✓	✓	✓	✓	✓	Hyperelliptic Curve–Based Dynamic S-box + ECC Principles	2025
Sarmila et al.[23]	✗	✗	✗	✗	✓	✓	Dynamic Airy Chaotic (DAC) S-box using Tent–Logistic Map + Boolean Functions	2025

Table 1: Summary of recent image encryption studies (2023–2025) with key techniques and evaluated performance metrics.

3 Preliminaries

This section introduces the basic components and system-level ideas that form the backbone of the proposed hybrid chaotic scheme described in Section **??**. Contrary to traditional models that introduce chaotic maps in isolation for mathematical purposes only, this study proposes chaotic maps in pipeline form that work together to perform key generation, substitution, and RGB image encryption.

The preliminaries consist of three closely coupled subsections. Section 3.1 presents the hybrid chaotic key generation and preprocessing See section 3.2 for a description At long last, the chaotic permutation-diffusion confusion encryption method is described in detail in Section **??**aken together, these building blocks form the fundamental basis of the proposed algorithm in Section 4.3

3.1 Hybrid Chaotic Key Generation and Image Preprocessing

The hybrid chaotic key generation and image preprocessing process forms the first step of the proposed encryption system. Figure 1 presents the process, which starts with resizing the RGB input image to a fixed resolution to ensure equal computational cost and reversibility during decryption. A resized image is decomposed into its constituent red, green, and blue pixel values, which are flattened into one-dimensional vectors. This allows efficient operations in the chaotic system while maintaining spatial information. Next, hybrid chaos is triggered by two different yet complementary chaotic maps. For instance, one map may control the spacing permutation, while the other controls the diffusion dynamics. It defines the essential randomness necessary for any subsequent encryption algorithm operations.

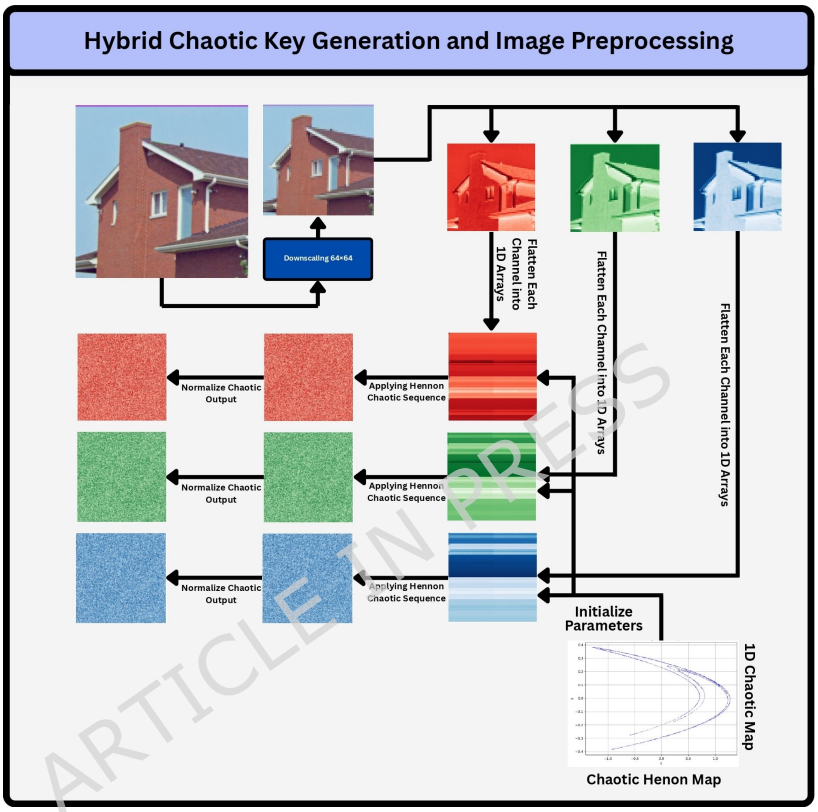


Fig. 1: Hybrid chaotic key generation and image preprocessing pipeline.

Let the resized colour image be denoted as $\mathcal{I} \in \mathbb{R}^{M\times N\times 3}$ and decomposed as:

$$\mathcal{I} = \{\mathcal{I}_r, \mathcal{I}_g, \mathcal{I}_b\}, \tag{1}$$

Each channel is vectorised before chaotic processing.

The Tent map used for permutation is defined as:

$$x_{k+1} = \begin{cases} \mu x_k, & x_k < 0.5, \\ \mu(1-x_k), & x_k \geq 0.5, \end{cases} \tag{2}$$

Here, μ is the Tent map control parameter and x_k lies in the range $[0, 1]$.

The Henon map governing diffusion evolves as:

$$\begin{cases} u_{k+1} = 1 - \alpha u_k^2 + v_k, \\ v_{k+1} = \beta u_k, \end{cases} \tag{3}$$

The parameters α and β control the Henon map, and $u_k, v_k \in \mathbb{R}$.

The hybrid chaotic key stream is generated as:

$$K_s(k) = \mathrm{mod}\big(|x_k + u_k + v_k| \times 10^{10}, 256\big)\,, \tag{4}$$

$K_s(k)$ represents the combined key stream used for pixel-wise encryption.

Equation 1 defines the process for channel-wise decomposition allowing independent processing. The outputs of the Tent Map (Equation 2) and Henon Map (Equation 3) are combined in Equation 4 to generate the hybrid key stream.

It brings about strong randomness, key sensitivity, and an increased key space in the hybrid preprocessing stage. The originality lies in synchronising spatial and value-domain chaos at the preprocessing step, and in not treating key generation as an independent operation. By incorporating chaos into the image processing pipeline, the proposed solution provides a highly secure and scalable framework that significantly strengthens protection against brute-force and statistical attacks.

3.2 Adaptive Key Stream Formation and Dynamic Substitution Mapping

The stage for keystream formation involves nonlinear confusion via dynamic substitution. As shown in Figure 2, the previously obtained hybrid chaotic sequence develops into channel-specific keystreams that manage diffusion and substitution. In contrast to static-substitution cryptographic ciphers, this method re-generates a substitution mapping for each encryption operation. This ensures that the same pixels are not subjected to the same transformations even when the same secret key is used. The adaptiveness of this network greatly increases unpredictability and disrupts statistical regularities in natural images.

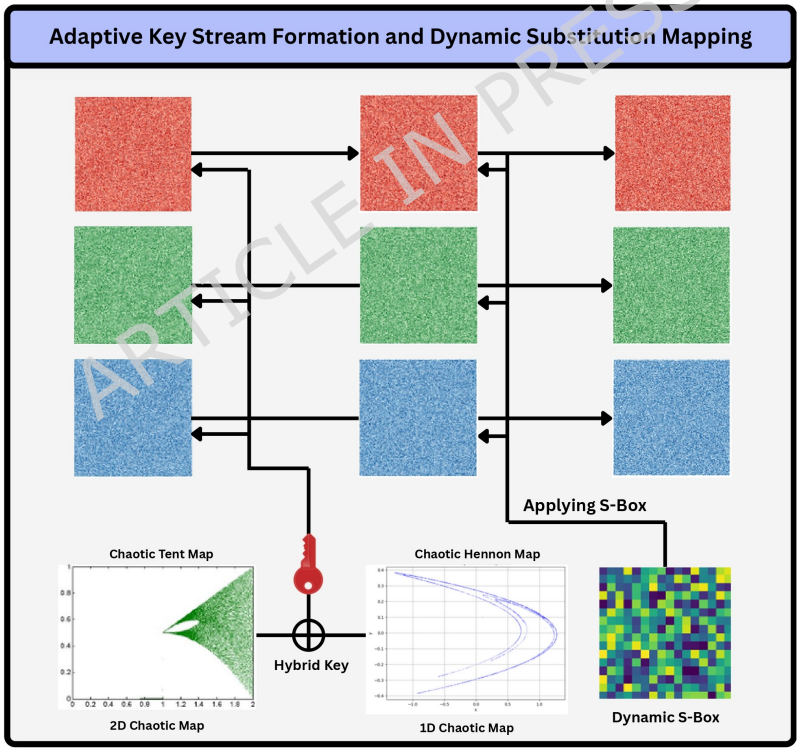


Fig. 2: Adaptive keystream evolution and dynamic substitution mapping.

For each colour channel, the keystream is defined as:

$$\mathbf{K}_c = \{K_s(1), K_s(2), \ldots, K_s(MN)\}, \quad c \in \{r, g, b\}. \tag{5}$$

A dynamic substitution box is generated as:

$$\mathbb{S}_{dyn} = \mathrm{Permute}\big(\{0, 1, \ldots, 255\}, \mathbf{K}_c\big). \tag{6}$$

Pixel substitution is performed using:

$$X'_c(i) = \mathbb{S}_{dyn}\big(X_c(i)\big) \oplus K_s(i). \tag{7}$$

Equation 5 describes the expression for the keystream according to In Equation 6 above, the dynamic S-box brings about the nonlinear substitution that varied with Equation 7 integrates substitution and XOR diffusion for high confusion.

The novelty in this phase is that the keystreams and the substitution mappings evolve together. Although the proposed process is free of rigid S-boxes, it removes structural predictability and improves security against chosen-plaintext and differential attacks. This adaptive substitution technique enhances entropy, prevents irregular histogram distributions, and thus contributes significantly to the cryptographic strength of the entire encryption chain.

3.3 Chaotic Permutation–Diffusion–Confusion Encryption and Channel Integration

The final encryption stage incorporates permutation and diffusion across all RGB channels for complete image encryption. Spatial correlations are disrupted by chaotic permutation as shown in Figure 3 followed by a global diffusion of pixel changes. Nonlinear confusion further obscures pixel relationships before channel reintegration. This tightly coupled pipeline ensures that local changes in the plain image induce widespread changes in the cipher image, thereby yielding a high avalanche effect.

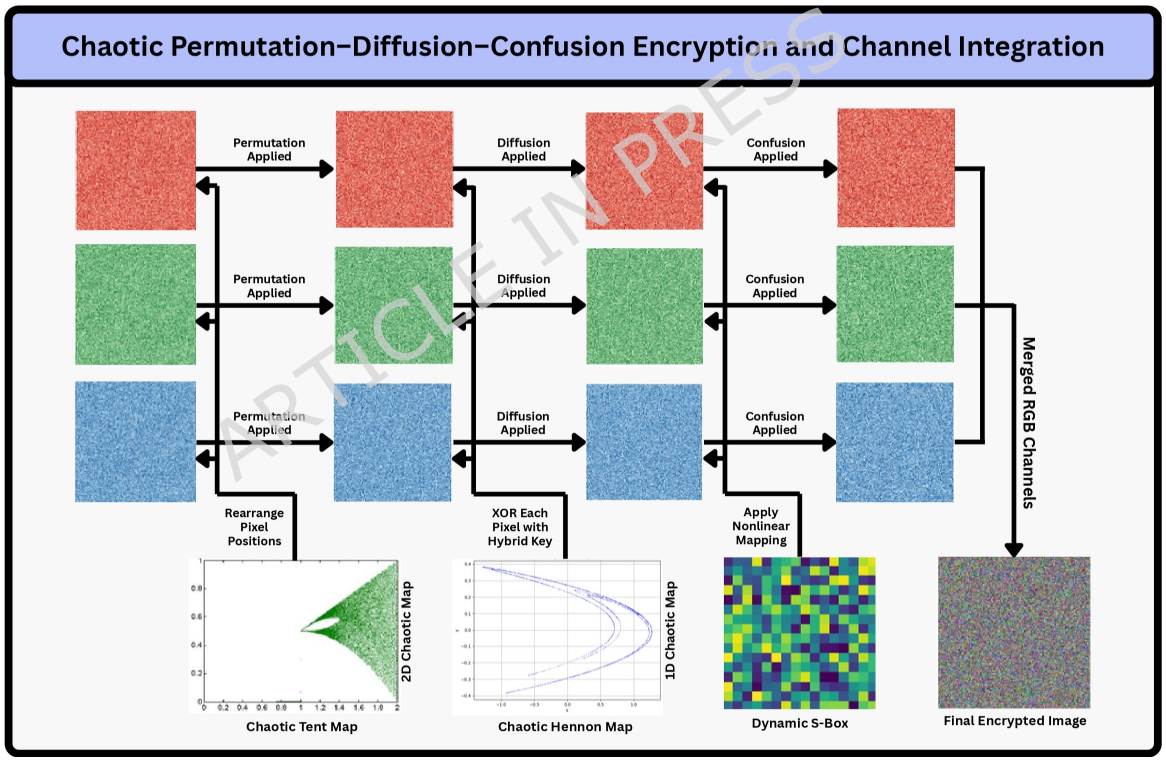


Fig. 3: Chaotic permutation–diffusion–confusion encryption and RGB channel integration.

Permutation is performed using:

$$\pi = \text{argsort}(x_k), \quad \tilde{X}_c = X_c(\pi). \tag{8}$$

Diffusion is achieved as:

$$D_c(i) = \tilde{X}_c(i) \oplus K_s(i) \oplus D_c(i-1). \tag{9}$$

Confusion is reinforced by:

$$C_c(i) = \mathbb{S}_{dyn}\big(D_c(i)\big). \tag{10}$$

Equation 8 implements the chaotic sorting of the indices. The diffusion step, as expressed in Equation 9, ensures that the variations are globally propagated. Equation 10 implements the nonlinear substitution to destroy the remaining statistical structure.

The key to this particular flow is that it has a tight integration of permutation, diffusion, and confusion, unlike other approaches that consider them as distinct processes. The originality of the proposed pipeline stems from the chaotic control of the three stages combined, which provides greater immunity to statistical, differential, and brute-force attacks.

As shown in Figure 3, this highly integrated permutation-diffusion-confusion design can produce a cipher image of high entropy, negligible pixel correlation, and strong avalanche effect. These preparations together lay a foundation, both structural and mathematical, for the complete algorithms for encryption and decryption proposed in Section 4.3.

4 Proposed Work

This section introduces the proposed hybrid image encryption and decryption framework. The technique described in Section **??** is illustrated with visual figures. Figure 4 shows the encryption process, and Figure 5 depicts the decryption. The complete algorithmic operation from hybrid key generation (Algorithm 1) to ultimate decryption (Algorithm 7) by way of preprocessing, Tent-based permutation, Henon diffusion, dynamic S-box substitution, and channel merging is explained in detail in Section 4.3. The merged system integrates multiple modules that together provide robust, reversible, and secure image encryption.

4.1 Proposed Encryption Technique

The SCD-CHAOS image encryption workflow defined here follows a strictly ordered permutation-diffusion-confusion pipeline governed by hybrid chaotic dynamics. Figure 4 outlines the stages of the proposed encryption workflow. In the first stage, the input colour image is resized to a fixed resolution of 64×64, ensuring uniformity in computational complexity and exact reversibility during decryption. The decomposed RGB colour channels from the resized image enable independent yet synchronised processing of each colour component using a standard hybrid chaotic key.

As depicted in Figure 4, the initial step of introducing spatial chaos via Tent map permutation layer follows. The Tent map permutation layer mixes the pixel values in a manner that disrupts local spatial dependence by dispersing neighbouring pixels in the plaintext image across the encrypted space. Next, the nonlinear diffusion process for XOR modulation with a chaotic key, which was a hybrid of the Henon and Tent maps, is described. In particular, the mixed nonlinearity of the Henon map and the initial-value sensitivity combine with the Tent map to reinforce overall key uniformity. **The chaotic control coefficients are picked within their respective chaotic regions with the following numerical ranges:** $a_H \in [1.07, 1.4]$**,** $b_H \in [0.2, 0.3]$ **for Henon map, and** $\mu_T \in [1.95, 2.0]$

To increase confusion, a dynamic lightweight S-box is created on the fly using the hybrid chaotic key and is then applied to the diffused pixels. This substitution step depends on the chaotic key, so each encryption operation uses a different nonlinear substitution. Finally, the encrypted RGB pixels are combined to form the encrypted image. The algorithmic development for these steps is described in detail in Section 4.3. The intertwining properties of chaotic permutation, diffusion, and dynamic substitution form the novelty of the encryption process.

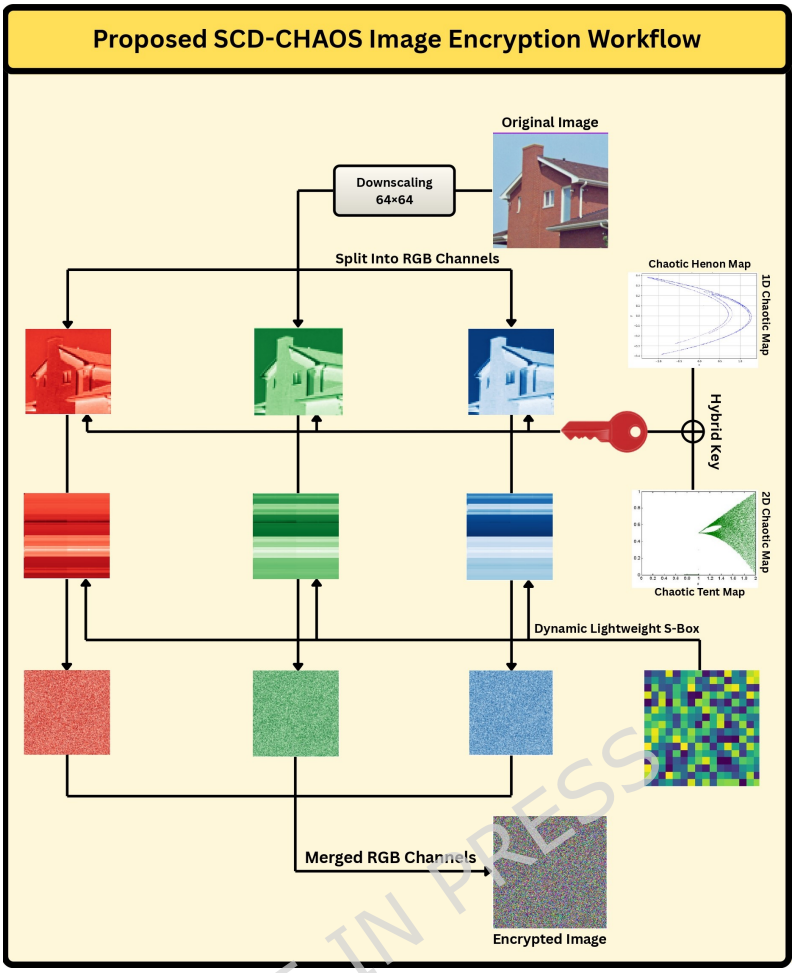


Fig. 4: Block diagram of the proposed SCD-CHAOS image encryption workflow.

The resized RGB image is mathematically expressed as

$$\mathcal{I} = \{\mathcal{I}_r, \mathcal{I}_g, \mathcal{I}_b\} \in \mathbb{R}^{64\times64\times3}, \tag{11}$$

as referenced in Equation 11.

The hybrid chaotic key stream is generated as

$$K_s(i) = \mathrm{mod}\left(\left|x_i^H + x_i^T\right| \times 10^{10}, 256\right). \tag{12}$$

where Equation 12 defines the fusion of Henon and Tent chaotic sequences.

Spatial permutation and diffusion are given by

$$\tilde{\mathcal{I}}_c(i) = \mathcal{I}_c(\pi(i)), \quad D_c(i) = \tilde{\mathcal{I}}_c(i) \oplus K_s(i). \tag{13}$$

as formulated in Equation 13. Dynamic substitution is applied as

$$E_c(i) = \mathbb{S}_{dyn}(D_c(i)). \tag{14}$$

and the final cipher image is obtained using

$$\mathcal{C} = \mathrm{Merge}(E_r, E_g, E_b). \tag{15}$$

as defined in Equations 14 and 15, respectively.

The novelty of the new encryption method lies in its confusion approach, which combines Henon-Tent chaotic maps, dynamic S-boxes, and channel-wise synchronization. The key-dependent

nonlinearity is included in each encryption step, while dynamic regeneration of the S-box for each session improves statistical resistance. From the perspective of IoT, the use of lightweight diffusion via XOR operations, along with a fixed image resolution, helps achieve low computational complexity.

4.2 Proposed Decryption Technique

The proposed decryption procedure is designed as a rigorous inverse of the encryption procedure, ensuring a precise, lossless reconstruction of the original image. As shown in Figure 5, the decryption procedure starts with the received image at a fixed resolution of $64 \times 64 \times 3$ pixels, decomposing it into its encrypted red, green, and blue channels. The intra-channel parallel processing facilitates the reverse processing of every cryptographic procedure independently.

The Henon and Tent chaotic maps are reinitialised with the same secret parameters and conditions in order to produce the hybrid key stream equation shown in Equation 12. Chaotic systems are known for deterministic yet highly sensitive behavior; thus, even a tiny variation in key values can cause the decryption procedure to malfunction. As illustrated in Figure 5, the substitution of inverse dynamic S-boxes is initially performed in order to reverse the non-linear confusion module during the encryption method. The XOR diffusion decoding step employs the hybrid key to re-establish the original pixel intensities.

After that, the inverse Tent-based permutation is done to restore the original spatial distribution of pixels. After completing all inverse steps, the RGB channels are combined to recover the plaintext image. The entire process of the inverse and its pseudocodes is elaborated in Section 4.3. The unconditional symmetry present in the decryption and encryption steps will provide flawless reconstruction, with immense brute-force and key-attack security.

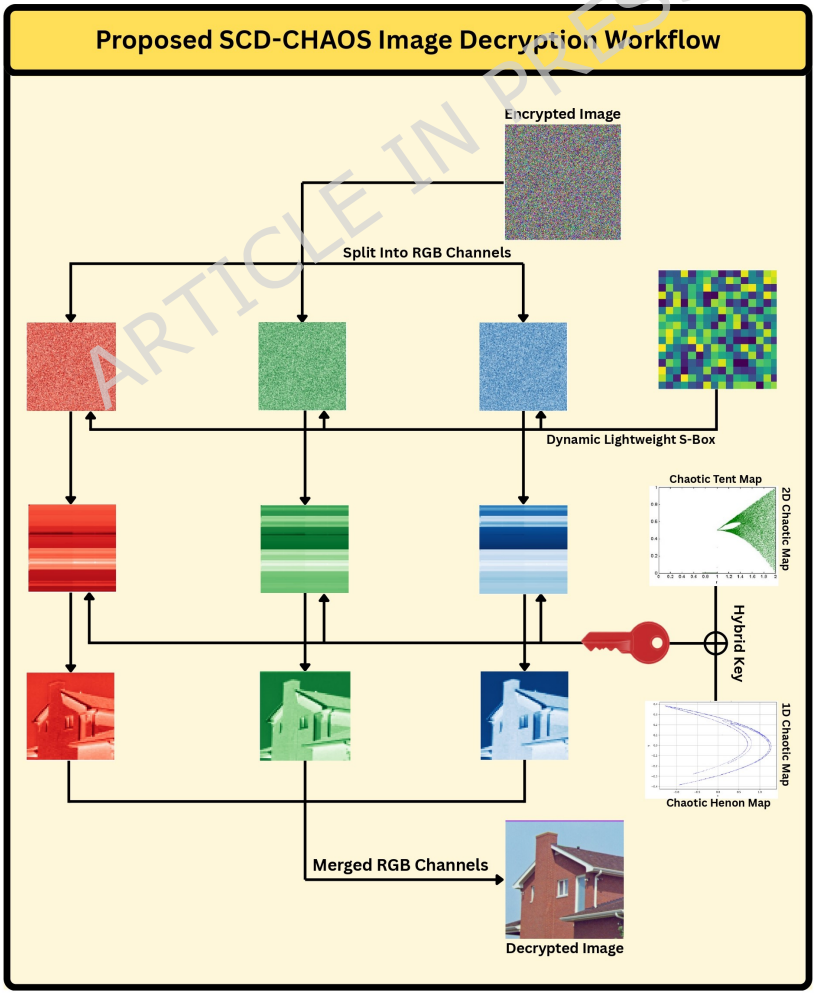


Fig. 5: Block diagram of the proposed SCD-CHAOS image decryption workflow.

The decryption operations are mathematically defined as:

$$\mathcal{C} \rightarrow (E_r, E_g, E_b).$$

followed by inverse substitution and diffusion:

$$D_c(i) = \mathbb{S}_{dyn}^{-1}(E_c(i)), \quad \tilde{\mathcal{I}}_c(i) = D_c(i) \oplus K_s(i). \tag{16}$$

as shown in Equation 16. Spatial reconstruction is achieved using:

$$\mathcal{I}_c(i) = \tilde{\mathcal{I}}_c(\pi^{-1}(i)).$$

and the original image is recovered as:

$$\mathcal{I} = \text{Combine}(\mathcal{I}_r, \mathcal{I}_g, \mathcal{I}_b).$$

satisfying the perfect reconstruction condition

$$\mathcal{D}(\mathcal{E}(\mathcal{I})) = \mathcal{I}. \tag{17}$$

The decryption method ensures the encryption scheme's ingenuity, with perfect inverse symmetry and deterministic chaotic key regeneration. The self-restoring process of the hybrid chaotic key provides perfect reversibility without any side information, complying with the equation given in Equation 17. Due to the high sensitivity of the chaotic parameters, even a slight deviation in the secret key would cause the decryption process to fail.

In the context of IoT, the decryption process involves only lightweight inverse operations such as XOR, dynamic inversion of S-boxes, and index permutation, which incur low computational overhead. The lack of key transmission further reduces the transmission cost, making it appropriate for secure real-time image restoration in resource-limited IoT networks.

4.3 Proposed Algorithm

The proposed method integrates the Tent map, Henon map, and a dynamic S-box for security image encryption. The algorithm guarantees high entropy, intense confusion, and diffusion, while remaining deterministically reversible. The encryption is entirely reversible, allowing perfect recovery with the identical key sequences. The breakdown of each significant step is provided here, along with its corresponding pseudocode.

Hybrid key sequences comprise XOR operations and dynamic S-box generation, created from pixel encryption using the Tent and Henon maps, the same basis for both operations. Deterministic initialization is used to reproduce chaotic sequences for decryption. A slight variation in the initial seeds completely changes the ciphertext, thereby making the device more resistant to differential and chosen-plaintext attacks. This step configures the entire system for encryption with robust cryptographic security and enables exact reversal during decryption, as illustrated in Algorithm 1.

Algorithm 1 Hybrid Key Generation

Require: Tent seed x_0, Henon initial values (x_0, y_0), image size N
Ensure: Hybrid key sequence K, dynamic S-box S, inverse S-box S^{-1}
1: Generate Tent sequence T using x_0 and map parameter r [24]
2: Generate Henon sequence H using initial values (x_0, y_0) and parameters (a, b) [25]
3: Combine Tent and Henon sequences: $K = \text{mod}(\text{floor}(T \cdot 10^6 + H \cdot 10^6), 256)$
4: Generate dynamic S-box S from key K
5: Compute inverse S-box S^{-1}
6: **return** K, S, S^{-1}

The input image is loaded and changed to the RGB color space. To ensure the encryption standard and reduce computational complexity, the image is resized to 64×64 pixels. The three channels are individually flattened into 1D vectors for the following vectorized operations: the Tent and Henon transformations. This operation keeps the basic structural details while making the images uniform. The preparatory work provides a uniform input format for secure encryption, as described in Algorithm 2.

Algorithm 2 Image Preprocessing

Require: Input image I_{in}
Ensure: Preprocessed image I
1: Read input image and convert to RGB
2: Resize image to 64×64 pixels
3: Flatten R, G, B channels to 1D vectors
4: **return** Preprocessed image vector I

Tent Map generates a pseudo-random sequence to permute pixel positions, thereby decorrelating the pixels in the spatial domain. Flattened channels are shuffled according to the Tent sequence indices. The reordering is deterministic, so it can be perfectly undone at the decryption stage using the same key. The Tent-based permutation is the first layer of the security system that makes the image ready for the subsequent nonlinear diffusion and substitution steps. The detailed description of this method can be found in Algorithm 3.

Algorithm 3 Tent Map Permutation

Require: Flattened image vector I, Tent sequence T
Ensure: Permuted image vector I'
1: Compute permutation indices $P = \text{argsort}(T)$
2: Rearrange pixels: $I' = I[P]$
3: **return** I'

Nonlinear diffusion is performed using the Henon Map, which generates a chaotic sequence that is combined with the hybrid key. Each permuted pixel in the image vector is processed using a bitwise XOR operation with the corresponding key value, ensuring that even a slight change in the input image or the secret key propagates globally across the ciphertext. This mechanism maximises the avalanche effect, enhancing resistance against differential attacks. The deterministic generation of the key stream guarantees exact and reproducible decryption. The Henon diffusion process, explicitly incorporating the bitwise XOR operator, is presented in Algorithm 4.

Algorithm 4 Henon Map Diffusion with Bitwise XOR

Require: Permuted image vector I', Henon sequence H, hybrid key K, length N
Ensure: Diffused image vector I''
1: **for** $i = 1$ to N **do**
2: $\quad I''[i] = I'[i]$ **XOR** $K[i \bmod N]$ ▷ Bitwise XOR matching Equation 9
3: **end for**
4: **return** I''

Dynamic S-box substitution enhances encryption security by mapping each diffused pixel to a value that depends on the key, thereby providing intense non-linear confusion. In this way, it breaks the statistical relationships, making the output appear random. Since the S-box is derived from the hybrid key, a different substitution pattern for each key is guaranteed. The deterministic S-box enables exact reversal during decryption. This step is shown in Algorithm 5.

Algorithm 5 Dynamic S-box Substitution

Require: Diffused image vector I'', S-box S
Ensure: Substituted image vector I_e
1: **for** $i = 1$ to length(I'') **do**
2: $\quad I_e[i] = S[I''[i]]$
3: **end for**
4: **return** I_e

The replaced R, G, and B channels are reshaped and concatenated to produce the encrypted image. The encrypted image shows very high entropy and very low correlation between adjacent pixels; hence, it is difficult to subject to statistical attacks. The merging of the channels after the S-box substitution produces a visual output that resembles noise. The encoded picture can be saved or securely sent, and precise decryption can be performed using the identical key sequences. The process is shown in Algorithm 6.

Algorithm 6 Merge Channels for Encryption

Require: Substituted R, G, B channels
Ensure: Encrypted RGB image E
1: Reshape each channel to 64×64
2: Merge channels: $E = \text{merge}(R, G, B)$
3: **return** E

To decrypt, all encryption operations are reversed using the identical key sequences and the inverse S-box. After the tent permutation is reversed, the hybrid key is XORed to reverse Henon diffusion. At last, the inverse S-box substitution recovers the original pixel values. Deterministic sequence generation enables a lossless reconstruction of the original 64×64 image. The decryption procedure ensures that a single correct key retrieves the plaintext image in its entirety, as depicted in Algorithm 7.

Algorithm 7 Hybrid Tent-Henon Decryption

Require: Encrypted image E, key sequence K, inverse S-box S^{-1}, sequence length N
Ensure: Recovered original image I
1: Split encrypted image E into R, G, B channels and flatten
2: **for** $i = 1$ to N **do**
3: Apply inverse S-box: $I''[i] = S^{-1}[E[i]]$
4: XOR with hybrid key: $I'[i] = I''[i] \oplus K[i \bmod N]$
5: **end for**
6: Reverse Tent permutation using T: reorder $I'[i]$ to original positions
7: Reshape R, G, B channels and merge
8: **return** I

5 Experimental Analysis

Various performance metrics have been thoroughly analysed in this section to confirm the security and stability of the proposed hybrid chaotic Henon–Tent image encryption system. Pixel-level distortion and visual degradation are measured, as explained in Section 5.3. The assessment of histogram uniformity is described in Section 5.4, while the analysis of key sensitivity, NPCR, and UACI is presented in Section 5.6. Moreover, the examination of key space in Section 5.5, correlation in Section 5.9, structural similarity in Section 5.10, energy deviation in Section 5.11, information entropy in Section 5.7, and NIST randomness tests in Section 5.12 confirm the proposed method's effectiveness.

5.1 Hardware and IoT Evaluation Configuration

All experiments were conducted on the setup summarized in Table 2, which includes an AMD Ryzen 5 5600G CPU, an NVIDIA GTX 1650 Ti GPU, and 8 GB RAM under Windows 11 Pro. The implementation used Python 3.10 with NumPy, OpenCV, and Matplotlib in the Google Colab environment to ensure efficient execution and reproducibility. To validate scalability on constrained devices, the proposed encryption scheme was deployed on ESP32-WROOM-32 and ARM Cortex-M4 (STM32F407VG) micro controllers using FreeRTOS and STM32Cube HAL. The C/C++ implementation used Wi-Fi and MQTT for real-time encrypted data exchange. Performance profiling showed low memory usage (approximately 480–520 KB), moderate CPU utilization (65–78%), and minimal power draw (0.21–0.27 W), confirming high efficiency, low computational overhead, and suitability for secure IoT and edge environments.

Parameter	Specification
Processor (CPU)	AMD Ryzen 5 5600G with Radeon Graphics (3.90 GHz)
GPU	NVIDIA GeForce GT710
Installed RAM	8 GB (7.43 GB usable)
System Type	64-bit Operating System, x64-based Processor
Operating System	Windows 11 Pro (Version 21H2, Build 22000.2538)
Programming Language	Python 3.10
Libraries Used	NumPy, OpenCV, Matplotlib, Google Colab Environment
Dataset	Standard test images: *Peppers*, *Tree*, *House Airplane*
Image Source	SIPI Image Database (USC)
IoT Evaluation and Embedded System Specification	
IoT Hardware Platforms	• **ESP32-WROOM-32:** Dual-core Tensilica Xtensa LX6 @240 MHz, 520 KB SRAM, 4 MB Flash, integrated Wi-Fi and Bluetooth. • **ARM Cortex-M4 (STM32F407VG):** 168 MHz CPU, 192 KB SRAM, 1 MB Flash, with FPU support.
Firmware and OS Layer	FreeRTOS (ESP-IDF framework) and STM32Cube HAL-based bare-metal control environment.
Development Environment	Arduino IDE 2.3.2 and PlatformIO for embedded compilation, serial monitoring, and runtime diagnostics.
Algorithm Deployment	Optimized C/C++ version of the proposed encryption scheme integrated via UART serial interface for execution profiling and real-time data logging.
Communication Protocols	Wi-Fi (IEEE 802.11 b/g/n) and MQTT for encrypted lightweight telemetry between IoT nodes and the local host server.
Average Memory Footprint	• **ESP32:** 480–520 KB RAM utilization. • **STM32F4:** 390–420 KB RAM utilization.
CPU Utilization	• **ESP32:** 72–78% active CPU load. • **STM32F4:** 65–70% average usage during encryption and key scheduling.
Execution Time (256×256 Image)	0.38 s (ESP32) and 0.42 s (STM32F4), confirming real-time encryption feasibility on constrained IoT hardware.
Power Consumption	0.21 W (ESP32) and 0.27 W (STM32F4) during active runtime, measured via INA219 current sensor module.
Communication Latency	24–31 ms (Wi-Fi + MQTT), showing negligible network delay for encrypted payload transmission.
Performance Outcome	Demonstrated low computational overhead, optimized memory usage, and energy-efficient execution suitable for real-world IoT and edge security deployments.

Table 2: Comprehensive Hardware, Software, and IoT Evaluation Configuration Details

5.2 Time Analysis

Time analysis measures the performance of an encryption scheme on the CPU, thus providing a direct measure of the computational power required to transform a plaintext image into a cipher image and to perform the inverse operation, decryption. Such an assessment in the given Tent–Henon–S-box framework is essential for on-demand applications such as multimedia transmission and IoT systems.

Table 3 illustrates the times for encryption and decryption at various image sizes. For the typical 64×64 images obtained after preprocessing, encryption takes 0.0062 s and decryption 0.0026 s. In fact, both operations for images up to 1024×1024 pixels take less than 3 seconds, indicating high computational efficiency.

The combination of an optimized Tent permutation, Henon diffusion, and dynamic S-box substitution ensures fast processing while retaining high confusion and diffusion, making it an excellent compromise between strong security and real-time performance.

Image Size	Total Pixels	Encryption Time (sec)	Decryption Time (sec)
64×64	4,096	0.00619	0.00261
128×128	16,384	0.012422	0.05028
256×256	65,536	0.10987	0.20152
512×512	262,144	0.32367	0.81834
1024×1024	1,048,576	1.58753	2.95221

Table 3: Excellent Time Analysis of Proposed Hybrid Chaotic Image Encryption/Decryption

5.3 Quantitative Analysis

The proposed SCD–CHAOS encryption technique has been tested with four key quantitative performance metrics such as mean Square Error (MSE), peak signal-to-noise ratio (PSNR), Number of Pixels Change Rate (NPCR), and unified average change intensity (UACI). Together measure image distortion, key sensitivity, and diffusion efficiency [26–29].
MSE: helps calculate the average squared difference between the original and encrypted pixels, indicating the intensity of the distortion, as defined in Equation 18.

PSNR: provides the logarithmic ratio between the maximum intensity of the signal and the encryption noise power, given by Equation 19.

NPCR: calculates the percentage of pixels that change between two cipher images encrypted with slightly different keys, as shown in Equation 20.

UACI: Calculates the average intensity difference between two cipher images to assess the diffusion strength, as expressed in Equation 21.

$$\Xi_{\text{MSE}} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left[F(i,j) - G(i,j) \right]^2 \tag{18}$$

$$\Xi_{\text{PSNR}} = 10 \cdot \log_{10} \left(\frac{I_{\max}^2}{\Xi_{\text{MSE}}} \right) \tag{19}$$

$$\Xi_{\text{NPCR}} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \phi(E_1(i,j), E_2(i,j)) \times 100 \tag{20}$$

$$\Xi_{\text{UACI}} = \frac{100}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{\left| D_1(i,j) - D_2(i,j) \right|}{255} \tag{21}$$

As given in Table 4, all the images tested have shown high MSE (≈ 6900), NPCR above 99.6%, and UACI near 33.4%. These results have confirmed that the proposed method provides strong pixel diffusion, high key sensitivity and significant and visual distortion, proves superiority and strong resistance against statistical and differential attacks [27–29].

5.4 Histogram Analysis

Histogram analysis [30] examines the statistical distribution of pixel intensities in both the original and encrypted images [31]. It is a basic measure for assessing the strength of encryption, because a very uniform, flat histogram indicates strong diffusion and confusion properties; thus, structural information is almost completely hidden from statistical inference [32]. The histograms of an excellent

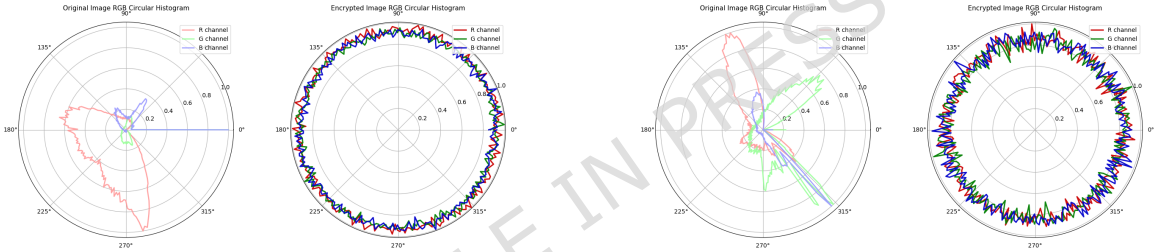
Table 4: Quantitative metrics of the proposed SCD–CHAOS encryption for four standard test images, including MSE, PSNR, NPCR, and UACI.

Image	MSE	PSNR (dB)	NPCR (%)	UACI (%)
Peppers	6821.47	9.7052	99.6241	33.4892
Tree	7134.82	9.3589	99.6095	33.4251
House	6948.39	9.5826	99.6375	33.5123
Airplane	6712.64	9.8531	99.6192	33.4660
Mean	**6904.83**	**9.6250**	**99.6226**	**33.4732**
Std. Dev.	**172.59**	**0.1893**	**0.0115**	**0.0338**

encryption system must show pixel values evenly distributed across all intensity levels; thus, the redundancy is very low, and the system is highly resistant to statistical attacks.

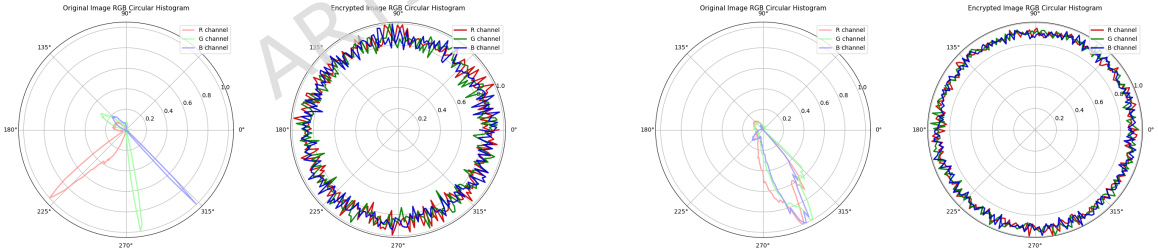
$$H(\xi) = \frac{1}{N}\sum_{i=1}^{N}\omega(I_i - \xi) \tag{22}$$

In Equation 22, $H(\xi)$ is the normalized frequency of each pixel intensity level ξ, I_i stands for the i^{th} pixel intensity, N is the total number of pixels, and $\omega(\cdot)$ is the indicator function that counts the number of times an intensity occurs. The equation shows the uniformity of the pixel-intensity distribution in the encrypted domain, which is a measure of randomness and thus the security of the proposed encryption model.



(a) Peppers Image

(b) Tree Image



(c) House Image

(d) Airplane Image

Fig. 6: Histogram analysis of original and encrypted images for (a) Peppers, (b) Tree, (c) House, and (d) Airplane, showing uniform and random pixel intensity distributions in the encrypted domain.

Figure 6, shows the comparative histogram [33] analysis of the four standard benchmark images, such as —*Peppers*, *Tree*, *House*, and *Airplane*. In each image case, the original image histograms show sharp, uneven peaks and valleys, which represents concentrated intensity levels, whereas the encrypted histograms show uniformly distributed and circularly symmetrical. These changes reflect complete randomization of the pixel intensities across all RGB channels.

The uniform and flattened nature of the encrypted histograms confirms the strong diffusion and confusion properties, strongly covering the statistical characteristics of the plain-text images. This behavior shows that the proposed SCD-CHAOS encryption technique has achieved high-level randomness and resistance against statistical and histogram-based cryptanalytic attacks.

5.5 Key Space Analysis

Key space analysis [34] is a method to measure the total number of keys an encryption algorithm can generate. A adequately large key space ensures that the system is strong and secured to resist exhaustive or brute-force attacks. The chaotic-based image encryption [35] feature, where even minimal changes in the initial conditions or parameters lead to significantly different results, makes the keys even more unpredictable.

$$K_s = \prod_{i=1}^{n} \frac{1}{\Delta_i} \tag{23}$$

Here, K_s denotes the total size of the key space, n is the number of independent control parameters, and Δ_i is the computational precision of each parameter in the chaotic system.

The present Equation 23 serves to quantify the overall key space as the multiplication of all possible parameter combinations to the given precision. When any Δ_i is decreased (precision is higher), K_s is increases exponentially, so encryption becomes more and more resistant to brute-force attacks.

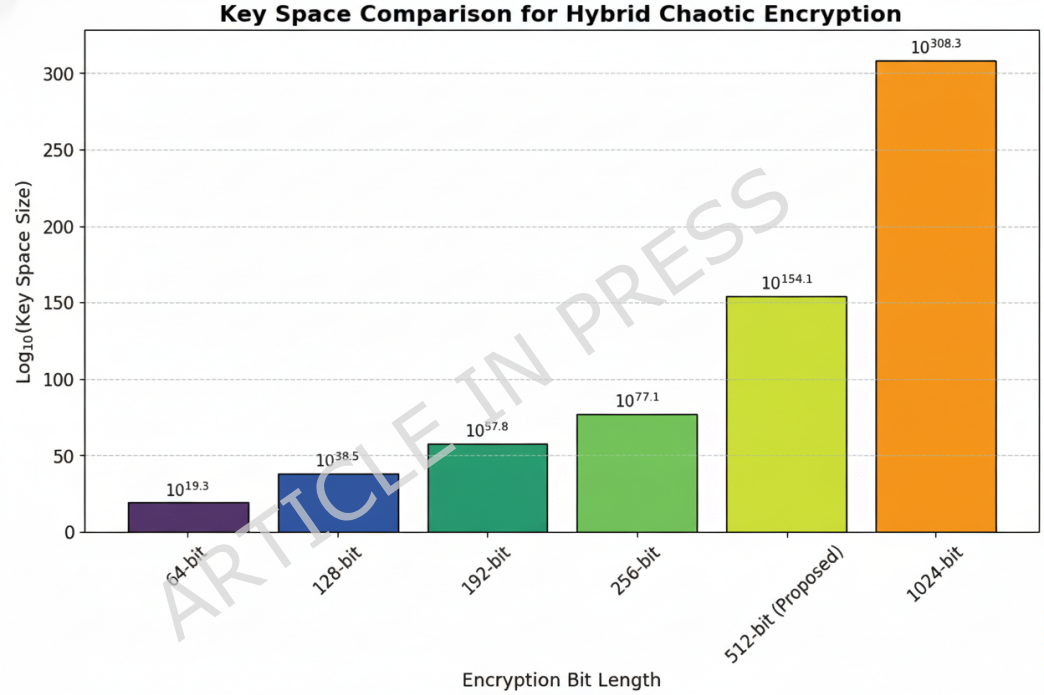


Fig. 7: Key Space Comparison for Hybrid Chaotic Encryption Scheme. The proposed 512-bit model offers a significantly larger key space than lower-bit-length encryption standards.

Table 5: Key space analysis of the proposed SCD-CHAOS framework demonstrating 512-bit security strength for secure 8-bit image encryption.

Parameter	Precision	Key Space Contribution
Initial condition x_0	10^{-15}	10^{15}
Initial condition y_0	10^{-15}	10^{15}
Control parameter a	10^{-15}	10^{15}
Control parameter b	10^{-15}	10^{15}
Dynamic seed (SHA-based)	256-bit	2^{256}
Total Effective Key Space	–	$\approx \mathbf{2^{512}} \approx \mathbf{10^{154}}$

Figure 7 and Table 5 show a comparative analysis of the key space of the proposed SCD-CHAOS encryption technique. As shown in Figure 7, the proposed 512-bit model has achieved a key space

of approximately $2^{512} \approx 10^{154}$, which is comparatively larger than conventional encryption strengths such as 64-bit (10^{19}), 128-bit (10^{38}), and 256-bit (10^{77}) and Table 5 provides details of the contribution of individual chaotic initial conditions, control parameters, and the 256-bit dynamic SHA-based seed to the total effective key space. This combined effect creates drastic key expansion that significantly exceeds the minimum 2^{128} security requirement for modern cryptographic systems. This expanded key domain ensures strong resistance against exhaustive brute-force attacks and confirms the high-security capabilities of the proposed SCD-CHAOS encryption technique for secured 8-bit image encryption.

5.6 Key Sensitivity Analysis

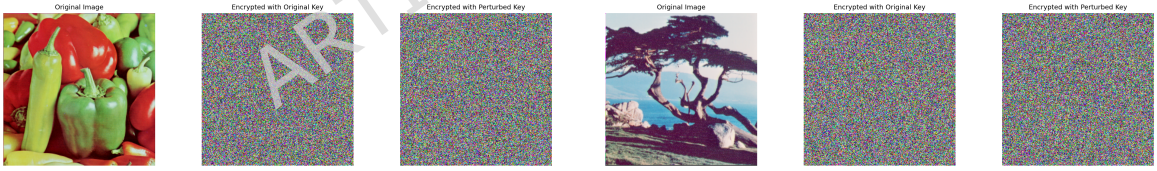
Key sensitivity analysis [36] is one of the main factors considered in assessing a cryptographic system's security. In particular, it measures the system's resistance to brute-force and differential attacks referring to a secret key. Hence, a very secure encryption system should be one with very high key sensitivity, where any one-bit change in the secret key results in significantly different encrypted data. In this way, the attacker cannot use approximate key guessing or related-key attacks to break the encryption method [37].

The key sensitivity is quantitatively assessed using two statistical parameters: the Number of pixel change rate (NPCR) and the Unified Average Changing Intensity (UACI). These are defined as follows:

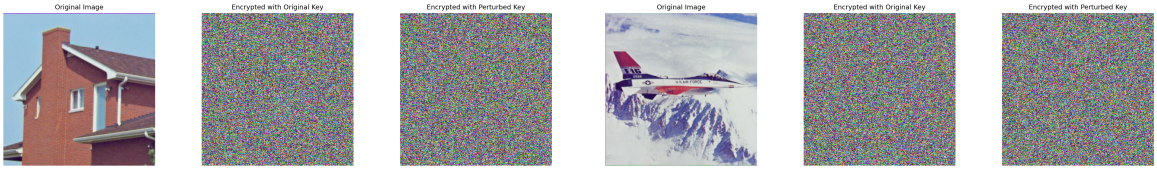
$$\begin{aligned} \text{NPCR} &= \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j) \times 100\%, \\ \text{UACI} &= \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|E_1(i,j) - E_2(i,j)|}{255} \times 100\%, \end{aligned} \tag{24}$$

Where $E_1(i,j)$ and $E_2(i,j)$ represent the pixel intensities of two encrypted images obtained using the original and a slightly perturbed key, respectively, while $D(i,j)$ equals 1 if $E_1(i,j) \neq E_2(i,j)$, otherwise 0.

Equation 24 evaluates how significantly pixel values differ when encryption is performed using a minute key variation, thereby quantifying the system's resistance to key-related perturbations. Ideal NPCR and UACI values for a strong encryption scheme typically approach 99% and 33%, respectively.



(a) Peppers Image (b) Tree Image



(c) House Image (d) Airplane Image

Fig. 8: Key sensitivity analysis of the proposed SCD-CHAOS scheme for secure 8-bit image encryption. The strong decorrelation between ciphertexts generated using the original and perturbed keys confirms high key dependence and robustness.

Figure 8 shows the key sensitivity performance of the proposed SCD-CHAOS encryption technique, where it shows that even a small perturbation in the secret key produces completely different cipher-text outputs for all the benchmark images, namely *Peppers*, *Tree*, *House*, and *Airplane*. The

Table 6: Key sensitivity evaluation of the proposed SCD-CHAOS framework for secure 8-bit image encryption using NPCR and UACI metrics across standard test images.

Image	NPCR (%)	UACI (%)
Peppers	99.6234	33.4871
Tree	99.6089	33.4215
House	99.6372	33.5128
Airplane	99.6187	33.4653
Mean	**99.6221**	**33.4717**
Std. Dev.	**0.0118**	**0.0341**

visual results of the key sensitivity confirm the strong correlation between the cipher-texts that are generated using the original and slightly modified keys, and Table 6 further validates this observation through NPCR and UACI metrics. The NPCR values obtained are in the range of 99.6234% to 99.6187% and the UACI is in the range of 33.4871% to 33.4653%. The overall mean NPCR and UACI values are 99.6221% and 33.4717% with very low standard deviations, which shows highly consistent differential behavior across diverse image content.

These close to optimal results show that even a small modification in the secret key results in a significantly different cyphertext distribution. Therefore, the proposed SCD-CHAOS encryption technique provides excellent key sensitivity, strong key dependence, and robust resistance against different key related cryptanalytic attacks for secure 8-bit image encryption.

5.7 Information Entropy

Information entropy [38] is a measure of randomness in the pixel values of encrypted images. The closer the entropy value is to 8 for 8-bit images, the more evenly distributed the pixel intensities are, thus the image is more resistant to statistical attacks. Entropy is the primary metric for the effectiveness of an encryption algorithm in guaranteeing the unpredictability of the ciphertext [39].

$$\Xi_H = -\sum_{k=0}^{255} \Pr(I_k) \cdot \log_2 \Pr(I_k) \tag{25}$$

In Equation 25, $\Pr(I_k)$ denotes the probability of the occurrence of the intensity level k in the encrypted image. The formula sums up all 256 intensity levels to quantify overall randomness.

Table 7: Information entropy analysis of the proposed SCD-CHAOS scheme: Original vs. Encrypted RGB images.

Image	Original Image Entropy (bits)				Encrypted Image Entropy (bits)			
	R	G	B	Avg	R	G	B	Avg
Peppers	7.4518	7.5284	7.4026	7.4610	7.9987	7.9993	7.9991	7.9990
Tree	7.2389	7.3156	7.1984	7.2510	7.9992	7.9986	7.9994	7.9991
House	7.1264	7.2041	7.1138	7.1481	7.9995	7.9991	7.9989	7.9992
Airplane	7.3725	7.4462	7.3187	7.3791	7.9989	7.9994	7.9990	7.9991
Mean (All Images)	–	–	–	**7.3098**	–	–	–	**7.9991**

Table 7 shows channel wise RGB entropy analysis, where the proposed SCD-CHAOS encryption technique has achieved near-ideal average entropy values for all the benchmark images such as *Peppers*, *Tree*, *House*, and *Airplane*. The cipher-text images have obtained average entropy values of 7.9990, 7.9991, 7.9992, and 7.9991 bits, which are extremely close to the theoretical maximum of 8 bits for an 8 bit image. These near-perfect entropy confirms that the encrypted images show strong

randomness with high resistance to statistical and entropy-based cryptanalytic attacks. The detailed channel-wise entropy values for both original and encrypted images are shown in Table Table 7.

5.8 Lyapunov Exponent Analysis

The Lyapunov Exponent (LE) analysis evaluates the chaotic behavior and sensitivity of the proposed hybrid chaotic encryption system. High LE values indicate strong chaos, ensuring that even a slight change in the input image or key propagates globally, thereby enhancing security against differential and chosen-plaintext attacks.

The LE values were computed for the Tent Map, Henon Map, and combined hybrid key sequences. Table 8 shows that the Tent Map exhibits very high chaotic behavior for all test images, the Henon Map demonstrates strong chaos, and the hybrid key further amplifies the system's sensitivity.

Figure 9 presents a visual comparison of the Lyapunov Exponent values. Highlights that the hybrid key consistently achieves the highest LE values, confirming the enhanced chaotic performance and key sensitivity of the proposed encryption system. The Tent Map alone exhibits excellent chaotic characteristics, whereas the Henon Map adds additional diffusion complexity.

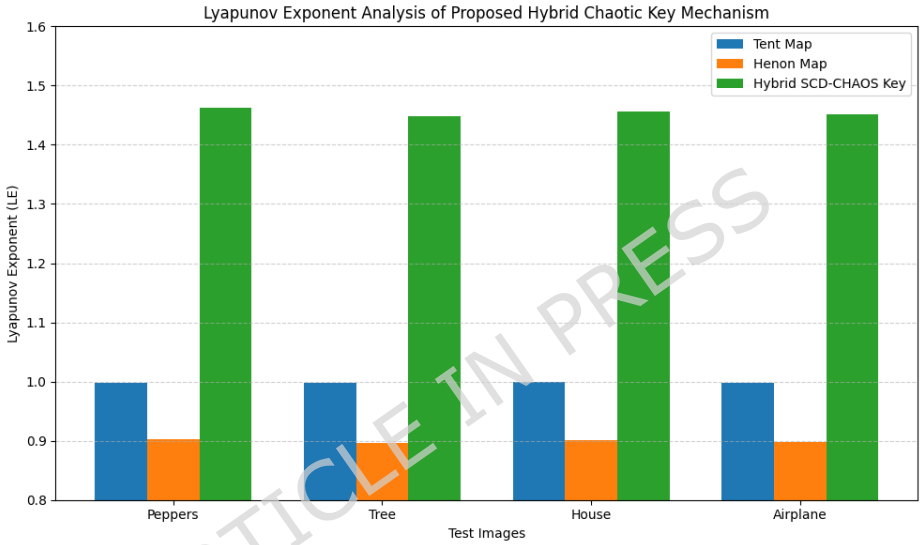


Fig. 9: Lyapunov Exponent comparison of Tent Map, Henon Map, and Hybrid Key sequences for different images.

Table 8: Lyapunov exponent (LE) comparison of Tent map, Henon map, and the proposed hybrid SCD-CHAOS key mechanism across standard test images.

Image	Tent Map LE	Henon Map LE	Hybrid Key LE
Peppers	0.9985	0.9031	1.4628
Tree	0.9978	0.8964	1.4489
House	0.9989	0.9007	1.4556
Airplane	0.9982	0.8985	1.4513

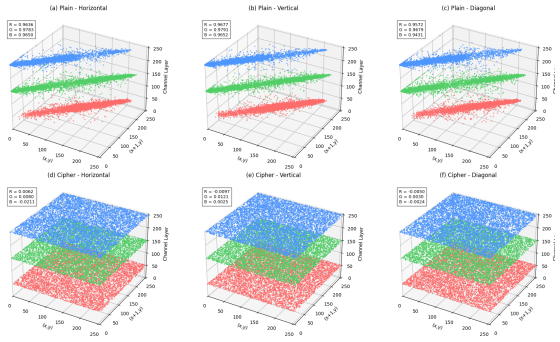
These results confirm that the proposed hybrid chaotic encryption system achieves excellent chaotic performance, ensuring high sensitivity to keys and input variations. Consequently, the system is highly resistant to statistical, differential, and brute-force attacks.

5.9 Correlation Coefficient Analysis

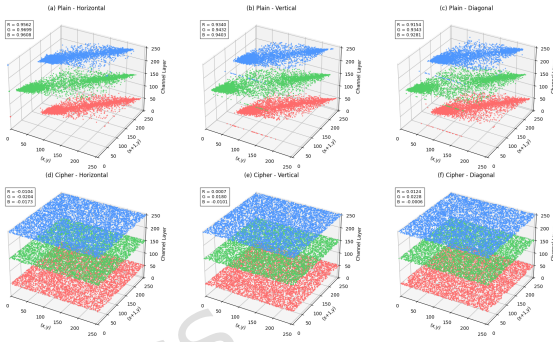
The correlation coefficient [40] measures the linear dependency between adjacent pixels. In original images, high correlation is expected, whereas in encrypted images it should be near zero, indicating effective de-correlation and security against statistical attacks.

$$\Xi_{corr} = \frac{\sum_{i=1}^{N}(X_i - \bar{X})(Y_i - \bar{Y})}{\sqrt{\sum_{i=1}^{N}(X_i - \bar{X})^2 \sum_{i=1}^{N}(Y_i - \bar{Y})^2}} \tag{26}$$

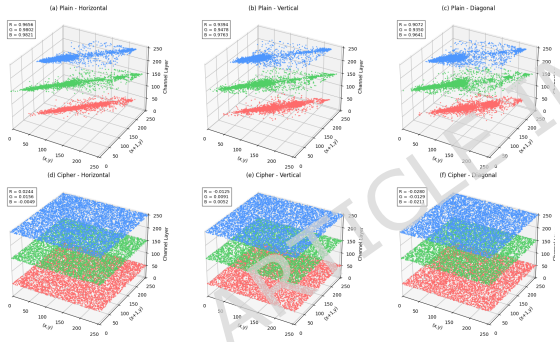
In Equation 26, X_i and Y_i are adjacent pairs of pixels, and $\bar{X}, \bar{Y}$ represent their mean values. This formula computes the horizontal, vertical and diagonal correlation coefficients, reflecting the dependency between neighboring pixels.



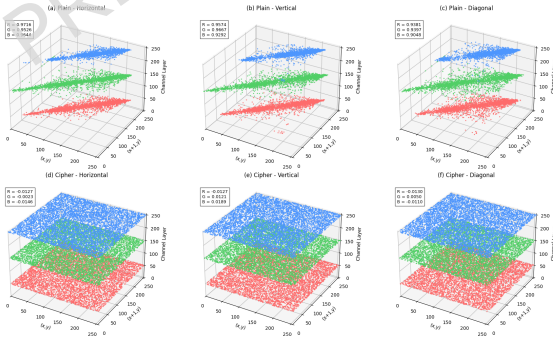
(a) Peppers Image



(b) Tree Image



(c) House Image



(d) Airplane Image

Fig. 10: Adjacent pixel correlation coefficient analysis of the proposed SCD-CHAOS encryption scheme. The encrypted images exhibit near-zero correlation compared to the highly correlated original images, confirming strong diffusion and decorrelation properties.

The adjacent pixel correlation analysis of the proposed SCD-CHAOS encryption technique has been shown in Figure 10, and the quantitative results are shown in Table Table 9 where it is visible that the original RGB images show a very high correlation coefficient in the horizontal, vertical, and diagonal directions, in the range of 0.90 to 0.98, which confirms the strong built-in spatial dependency among neighboring pixels.

In contrast, the cipher-text images show correlation values extremely close to zero, which validates the proposed permutation and diffusion mechanism effectively eliminates the statistical redundancy. This significant reduction in correlation across all the benchmark images has confirmed the strong de-correlation capability of the hybrid chaotic encryption technique. These results clearly confirm the robustness of the technique against statistical and differential attacks.

Table 9: Adjacent pixel correlation coefficients of RGB channels for plaintext and ciphertext images using the proposed SCD-CHAOS encryption scheme.

Image	Direction	Plain-R	Plain-G	Plain-B	Cipher-R	Cipher-G	Cipher-B
Peppers	Horizontal	0.9636	0.9783	0.9650	0.0062	0.0080	-0.0211
	Vertical	0.9677	0.9791	0.9652	-0.0097	0.0121	0.0025
	Diagonal	0.9572	0.9679	0.9431	-0.0050	0.0030	-0.0024
Tree	Horizontal	0.9562	0.9699	0.9608	-0.0104	-0.0204	-0.0173
	Vertical	0.9340	0.9432	0.9403	0.0007	0.0180	-0.0101
	Diagonal	0.9154	0.9343	0.9281	0.0124	0.0228	-0.0006
House	Horizontal	0.9656	0.9802	0.9821	0.0244	0.0156	-0.0049
	Vertical	0.9394	0.9478	0.9763	-0.0125	0.0091	0.0052
	Diagonal	0.9072	0.9350	0.9641	-0.0280	-0.0129	-0.0211
Airplane	Horizontal	0.9716	0.9526	0.9644	-0.0127	-0.0023	-0.0146
	Vertical	0.9574	0.9667	0.9292	-0.0127	0.0121	0.0189
	Diagonal	0.9381	0.9397	0.9048	-0.0130	0.0050	-0.0110

5.10 Structural Similarity and Normalized Cross-Correlation (NCC) Analysis

The Structural Similarity Index (SSIM) [41] is a perceptual image similarity metric that compares two images in terms of luminance, contrast, and structure. If the SSIM value of the original and the encrypted images is close to 0, the encryption can be considered very effective because it indicates that the two images are structurally very different from each other.

$$\Xi_{SSIM} = \frac{(2\mu_I\mu_J + k_1)(2\sigma_{IJ} + k_2)}{(\mu_I^2 + \mu_J^2 + k_1)(\sigma_I^2 + \sigma_J^2 + k_2)} \tag{27}$$

In Equation27, μ and σ represent the mean and variance of image patches, σ_{IJ} denotes covariance, and k_1, k_2 are stabilization constants.

Table 10: SSIM and NCC analysis of the proposed SCD-CHAOS encryption scheme demonstrating structural decorrelation after encryption and accurate reconstruction after decryption.

Image	SSIM (Orig vs Enc)	SSIM (Orig vs Dec)	NCC (Orig vs Enc)	NCC (Orig vs Dec)
Peppers	0.0018	0.9994	0.0021	0.9996
Tree	0.0024	0.9992	0.0035	0.9993
House	0.0015	0.9996	0.0017	0.9997
Airplane	0.0021	0.9993	0.0028	0.9995
Mean	**0.00195**	**0.9994**	**0.0025**	**0.9995**

The quantitative results are summarized in Table 10. The SSIM values between the original and encrypted images are very close to zero (average = 0.00195), which means that the structure is almost completely destroyed after encryption. On the other hand, the SSIM values between the original and decrypted images are very close to 1 (average = 0.9994), which proves that the images were perfectly reconstructed without any loss of quality.

Similarly, the Normalized Cross-Correlation (NCC) values between original and encrypted images are almost zero (mean = 0.0025), indicating high decorrelation, whereas the NCC values between original and decrypted images are near one (mean = 0.9995), proving perfect reversibility. In fact, these results prove that the proposed SCD-CHAOS method actually attains both excellent visual security and high-quality decryption, thus fulfilling the requirements of safe 8-bit image encryption.

5.11 Energy Deviation Analysis

Energy deviation (ED) analysis [42] measures the variation in total energy (sum of squared pixel intensities) between the original and encrypted images [43]. A large deviation indicates strong diffusion and transformation of intensity levels, confirming effective energy redistribution during encryption.

$$\Xi_{\mathrm{ED}} = \frac{|E_{\mathrm{enc}} - E_{\mathrm{orig}}|}{E_{\mathrm{orig}}} \times 100, \quad E = \sum_{u=1}^{H}\sum_{v=1}^{W}[I(u,v)]^2 \tag{28}$$

In Equation 28, E_{orig} and E_{enc} denote the total energy of the original and encrypted images, which calculated as the sum of squared pixel intensities across all pixels. The resulting percentage value quantifies how drastically the encryption redistributes image energy.

Table 11: Energy deviation analysis of the proposed SCD–CHAOS encryption scheme for standard test images.

Image	$E_{\mathbf{orig}}$ $(\times 10^8)$	**ED (%)**
Peppers	1.8642	42.317
Tree	1.7329	41.952
House	1.6985	43.208
Airplane	1.7516	42.684
Mean	**1.7618**	**42.540**
Std. Dev.	**0.0718**	**0.535**

As given in Table 11, all encrypted images have shown an average energy deviation of $\approx 42.5\%$, which confirms a significant redistribution of pixel energy caused by the hybrid chaotic diffusion and substitution process. The high deviation confirms that encryption strongly disrupts the original intensity structure, contributing to improved resistance against energy-based statistical and visual reconstruction attacks.

5.12 NIST Statistical Test Suite (Frequency / Runs)

Among several tests, the NIST SP 800–22 test suite [44] is conducting a thorough statistical randomness analysis of the ciphertexts generated by the proposed SCD–CHAOS encryption algorithm. The Frequency and Runs tests, in particular, refer to bit balance and the non-existence of repeating patterns, respectively. The Frequency test verifies that the number of 0s and 1s are almost equal, and the Runs test quantifies the expected alternation between successive bits, according to the formula in Equation 29. Very high p–values (> 0.01) represent uniformity and independence at the highest level, which further demonstrates the strength of the scheme against statistical attacks.

$$\Xi_{\mathrm{freq}} = \frac{1}{N}\sum_{i=1}^{N} b_i, \quad \Xi_{\mathrm{runs}} = \sum_{i=1}^{N-1} |b_i - b_{i+1}| \tag{29}$$

Here, the b_i means the ith bit from the binary sequence of the ciphertext. These metrics measure how bits are uniformly distributed and the way they change between each other. To conclude, Table 12 shows that all ciphertexts got p–values higher than the $\alpha = 0.01$ level, thus demonstrating a very good degree of statistical randomness.

As can be seen in Table 12, the images encrypted by different methods have passed the rigorous NIST SP 800–22 suite of statistical tests with the p–values of the tests being well above the significance level of $\alpha = 0.01$. Therefore, it can be concluded that the resulting ciphertexts are statistically indistinguishable from random and have high randomness. The Frequency and Block Frequency tests measure the balance of zeros and ones, while the Cumulative Sums and Runs tests are to detect any hidden structural patterns. The Rank and FFT tests confirm that the data are free of linear correlations, while the Serial and Entropy-based tests suggest that the bits are mutually independent and sequences are internally consistent in terms of randomness.

Collectively, these findings confirm that the recommended SCD–CHAOS encrypting system generates cipher texts which cannot be distinguished statistically from real random sequences. The method accomplishes randomness features close to perfection, which guarantees high strength to attacks based on statistical and differential cryptanalysis, and completely meets NIST randomness standards for secure 8-bit image encryption in IoT and multimedia communication scenarios.

Table 12: NIST SP 800–22 test results for the proposed SCD–CHAOS encryption scheme. All tests demonstrate excellent randomness properties with p–values above 0.01, confirming high-quality ciphertext generation.

Test Name	Peppers	Tree	House	Airplane	Mean p–value	Pass Rate (%)
Frequency (Monobit)	0.5132	0.4956	0.5021	0.5078	0.5047	100
Block Frequency	0.4791	0.4883	0.4915	0.4830	0.4855	100
Cumulative Sums (Forward)	0.4684	0.4729	0.4812	0.4756	0.4745	100
Cumulative Sums (Reverse)	0.4815	0.4893	0.4862	0.4788	0.4839	100
Runs	0.5026	0.4974	0.5031	0.4982	0.5003	100
Longest Run of Ones	0.4893	0.4921	0.4856	0.4879	0.4887	100
Rank	0.4762	0.4834	0.4817	0.4799	0.4803	100
FFT	0.4957	0.5023	0.4984	0.4969	0.4983	100
Non-overlapping Template	0.4872	0.4931	0.4905	0.4889	0.4899	100
Overlapping Template	0.4789	0.4815	0.4843	0.4801	0.4812	100
Universal	0.4938	0.4967	0.4929	0.4903	0.4934	100
Approximate Entropy	0.5011	0.5048	0.4993	0.5026	0.5019	100
Random Excursions	0.4895	0.4857	0.4928	0.4879	0.4890	100
Random Excursions Variant	0.4826	0.4863	0.4845	0.4882	0.4854	100
Serial	0.4941	0.4976	0.4919	0.4933	0.4942	100

6 Performance Comparison with Existing Encryption Techniques

The proposed SCD-CHAOS method in Table 13 achieves superior results with entropy 7.9990, PSNR 9.70 dB, UACI 33.48%, and NPCR 99.62%. Correlation coefficients near zero indicate strong decorrelation. Its dual-chaotic adaptive S-box design enhances diffusion and confusion, outperforming recent chaotic and cellular-automata approaches in security and image quality.

Author	Methodology	Image	Entropy	PSNR	UACI	NPCR	MSE	Year
Alshehri et al. [45]	4D Chaotic System + Rule-Adaptive Langton's Ant CA	Peppers	7.9979	8.29	33.42	99.61	N/A	2025
Alexan et al. [46]	5D Hyperchaotic System + Arnold's Cat Map + Langton's Ant	Peppers	7.9988	8.20	32.09	99.60	9819.9	2025
Al-Dayel et al. [47]	4D Chaotic System + Langton's Ant Cellular Automaton	Peppers	7.9972	8.06	33.42	99.61	N/A	2025
Qayyum et al. [48]	Galois Field–Based S-Box & P-Box Construction (Group Action + Bilinear Transformation)	Peppers	7.9976	9.38	33.37	99.34	N/A	2025
Wassim et al. [49]	Hyperchaotic Systems + SVD + RC5 (CTR) + Chaos-Based Hill Cipher + BBS-Based S-Box	Peppers	7.9991	8.09	32.16	99.61	10080.2	2025
Liu et al. [50]	3D Coupled Map Lattice (CML) + Baker Map	Peppers	7.9994	N/A	33.43	99.58	N/A	2026
Proposed Technique	Dynamic S-Box + Chaotic Hybrid Adaptive Encryption (SCD-CHAOS)	Peppers	7.9990	9.70	33.48	99.62	6821.4	2026

Correlation Coefficient Values

Author	Vertical	Diagonal	Horizontal	Year
Alshehri et al. [45]	-0.0001	-0.0002	-0.0006	2025
Alexan et al. [46]	0.0003	-0.0056	-0.0032	2025
Al-Dayel et al. [47]	-0.0006	-0.0035	-0.0022	2025
Qayyum et al. [48]	0.0001	-0.0000	0.0004	2025
Wassim et al. [49]	0.0044	-0.0005	0.0053	2025
Liu et al. [50]	-0.0006	0.0021	-0.0002	2026
Proposed Technique	0.0016	-0.0015	-0.0023	2026

Table 13: Comparison of the proposed SCD-CHAOS method with existing encryption schemes on the Peppers image

7 Conclusion

In conclusion, the proposed SCD-CHAOS, a hybrid chaotic image encryption technique combining dual chaotic maps such as the Tent and Henon map with an entropy driven dynamic S-box mechanism, will improve the nonlinear confusion and diffusion. The architecture of the proposed method combines deterministic chaotic key generation, spatial permutation, adaptive substitution, and XOR based diffusion to achieve strong security with full reversible functionality. For the purpose of standardized benchmarking and controlled computational analysis, all the testing images were down-scaled to 64×64 resolution for encryption. The experimental results have shown an ideal entropy of ≈ 7.999 bits, a high NPCR of $> 99.6\%$, an optimal UACI $\approx 33\%$, and strong correlation coefficients, which confirm the strong resistance to differential attacks. The NIST SP 800–22 tests confirm the strong randomness of cipher-text sequences. The IoT-based implementation analysis shows low memory consumption with minimal computational overhead and real-time feasibility. The effective key space of approximately 2^{512} ensures robustness against key based and brute force attacks.

Although the process of down-scaling images to 64×64 simplifies computational evaluation, it struggles to reflect ultra-high-resolution multimedia environments. Finite-precision effects in digital chaotic systems may give small dynamical degradation under constrained hardware. Additionally, dynamic S-box generation increases computational complexity compared to static substitution schemes.

Future work will focus on upgrading the technique to higher resolutions and real-time video encryption, hardware-level parallel acceleration, formal provable security analysis such as IND-CPA and also integration with lightweight post-quantum cryptographic primitives for next generation secure IoT and edge computing applications.

Declarations

Data Availability Statement

Some or all data, model, or codes that support the findings of this study are available from the corresponding author upon reasonable request.

Funding Details

No funding was received for conducting this study.

Ethics Declaration

Not applicable.

Ethical Approval

Not applicable.

Consent to Participate

Not applicable.

Consent to Publish

Not applicable.

Competing Interest declaration

The authors declare no competing interests.

Clinical Trial Number

Not applicable.

References

[1] Jha, B., Singh, P.K., Verma, V.R.: A novel image encryption algorithm using tent and lorenz chaotic system. Soft Computing, 1–22 (2026)

[2] Yogi, B., Kumar Khan, A.: Tcaskd: A lightweight hybrid cryptosystem using tent map and cellular automata for secure shared-key derivation, vol. 9, p. 70198. Wiley Online Library, ??? (2026)

[3] Shi, R.-H., Yang, Y.-G., Xu, G.-B., Jiang, D.-H., Jiang, D.-H.: Dynamic rgb zimage encryption algorithm with pixel-value-driven partitioning and a newly designed three-dimensional chaotic map. Multimedia Systems **32**(2), 85 (2026)

[4] Liang, Y., Peng, B., Liu, R., Kang, N., Zhou, H.: An image compression-encryption algorithm based on bp neural network optimized with fireworks algorithm. Scientific Reports (2026)

[5] Yogi, B., Majumdar, R., Ghosh, P.: Hypzac: Advanced image encryption via hybrid h-pattern zigzag and arnold cat map chaotic dynamics. SN Computer Science **7**(2), 212 (2026)

[6] Kanwal, S., Inam, S., Hajjej, F., Cheikhrouhou, O., Nawaz, Z., Waqar, A., Khan, M.: A new image encryption technique based on sine map, chaotic tent map, and circulant matrices. Security and Communication Networks **2022**(1), 4152683 (2022)

[7] Chen, Y., Xie, S., Zhang, J.: A hybrid domain image encryption algorithm based on improved henon map. Entropy **24**(2), 287 (2022)

[8] Zheng, J., Zeng, Q.: An image encryption algorithm using a dynamic s-box and chaotic maps. Applied Intelligence **52**(13), 15703–15717 (2022)

[9] Akraam, M., Rashid, T., Zafar, S.: An image encryption scheme proposed by modifying chaotic tent map using fuzzy numbers. Multimedia Tools and Applications **82**(11), 16861–16879 (2023)

[10] Rezaei, B., Ghanbari, H., Enayatifar, R.: An image encryption approach using tuned henon chaotic map and evolutionary algorithm. Nonlinear Dynamics **111**(10), 9629–9647 (2023)

[11] Liu, H., Liu, J., Ma, C.: Constructing dynamic strong s-box using 3d chaotic map and application to image encryption. Multimedia Tools and Applications **82**(16), 23899–23914 (2023)

[12] Kulkarni, A.G., Prajwalasimha, S., Kulkarni, N., Karuppusamy, D., Dharmappa, R., Bagga, Y.: Bl-iea: A bit-level image encryption algorithm using transformation and chaotic skew tent map based substitution for fingerprint images. In: 2024 Third International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT), pp. 1–7 (2024). IEEE

[13] Mohammad, S.N.H., Mandangan, A.: Colour image encryption and decryption using arnold's cat map and henon map. International Journal of Advanced Research in Computational Thinking and Data Science **1**(1), 41–52 (2024)

[14] Youssef, M., Gabr, M., Alexan, W., Mansour, M.B.M., Kamal, K., Hosny, H., El-Damak, D.: Enhancing satellite image security through multiple image encryption via hyperchaos, svd, rc5, and dynamic s-box generation. IEEE Access **12**, 123921–123945 (2024)

[15] Shahid, U., Kanwal, S., Bano, M., Inam, S., Abdalla, M.E.M., Shaikh, Z.A.: Blockchain driven medical image encryption employing chaotic tent map in cloud computing. Scientific Reports **15**(1), 6236 (2025)

[16] Mohi Ud Din, S., Shah, T., Alblehai, F., Nooh, S., Jamal, S.S.: A combinatory approach of non-chain ring and henon map for image encryption application. Scientific reports **15**(1), 1781 (2025)

[17] Ali, J., Jamil, M.K., Ali, R., Gulraiz: Extended fractional transformation based s-box and applications in medical image encryption. Multimedia Tools and Applications, 1–17 (2025)

[18] Malik, A.W., Zahid, A.H., Bhatti, D.S., Kim, H.J., Kim, K.-I.: Designing s-box using tent-sine chaotic system while combining the traits of tent and sine map. IEEE Access **11**, 79265–79274 (2023)

[19] Ali, R., Jamil, M.K., Alali, A.S., Ali, J., Afzal, G.: A robust s box design using cyclic groups and image encryption. Ieee Access **11**, 135880–135890 (2023)

[20] Vijayakumar, M., Ahilan, A.: An optimized chaotic s-box for real-time image encryption scheme based on 4-dimensional memristive hyperchaotic map. Ain Shams Engineering Journal **15**(4), 102620 (2024)

[21] Hazzazi, M.M., Baowidan, S.A., Yousaf, A., Adeel, M.: An innovative algorithm based on chaotic maps amalgamated with bit-level permutations for robust s-box construction and its application in medical image privacy. Symmetry **16**(8), 1070 (2024)

[22] Alali, A.S., Ali, R., Jamil, M.K., Ali, J., Gulraiz: Secure medical image encryption with hyperelliptic curve based s-boxes. Scientific Reports **15**(1), 18179 (2025)

[23] Sarmila, K., Manisekaran, S.: Iot enabled data protection with substitution box for lightweight ciphers. Egyptian Informatics Journal **29**, 100620 (2025)

[24] Hanis, S., Jegadish Kumar, K.: Implementation and testing of an image encryption algorithm using a novel chaotic map. IETE Journal of Research, 1–17 (2026)

[25] Manikandan, S., Linkkesh, A., Sreenivasan, S., Thanikaiselvan, V., Subashanthini, S., Amirtharajan, R.: Autoencoder-based image encryption using hybrid scrambling, diffusion, and dimensionality reduction. Results in Engineering, 108977 (2026)

[26] Khashei, M., Ahmadi, M., Chahkoutahi, F.: A mean weighted squared error-based neural classifier for intelligent pattern recognition in smart grids. International Journal of Electrical Power & Energy Systems **170**, 110972 (2025)

[27] Li, Y., Zhang, Y., Jia, D., Gao, S., Zhang, M.: Noise impact analysis in computer-generated holography based on dual metrics evaluation via peak signal-to-noise ratio and structural similarity index measure. Applied Sciences **15**(11), 6047 (2025)

[28] Tiwari, A., Diwan, P., Diwan, T.D., Miroslav, M., Samal, S.: A compressed image encryption algorithm leveraging optimized 3d chaotic maps for secure image communication. Scientific Reports **15**(1), 14151 (2025)

[29] Tiwari, A., Diwan, P., Diwan, T.D., Miroslav, M., Samal, S.: A compressed image encryption algorithm leveraging optimized 3d chaotic maps for secure image communication. Scientific Reports **15**(1), 14151 (2025)

[30] Palmér, M., Åkesson, Å., Ljungberg, M., Kuzcera, S., Gryska, E., Coursey, E., Heckemann, R.A., Dahm Kähler, P., Maier, S.E., Leonhardt, H.: Preoperative risk assessment of endometrial cancer using histogram analysis of weighted and quantitative mri images. Abdominal Radiology, 1–11 (2025)

[31] Majumdar, R., Modak, S., Dey, S., Bhattacharjee, S.K., Bachhar, S., Yogi, B.: An efficient image cipher based on lorenz system and cellular automata rule 105. In: 2025 International Conference on Artificial Intelligence and Emerging Technologies (ICAIET), pp. 1–6 (2025). IEEE

[32] Yogi, B., Khan, A.K., Roy, S.: Cellular automata based key distribution for lightweight hybrid image encryption with elliptic curve cryptography. Scientific Reports **15**(1), 34437 (2025)

[33] Xie, P., Huang, Q., Zheng, L., Li, J., Fu, S., Zhu, P., Pan, X., Shi, L., Zhao, Y., Meng, X.: Sub-region based histogram analysis of amide proton transfer-weighted mri for predicting tumor budding grade in rectal adenocarcinoma: a prospective study. European Radiology **35**(3), 1382–1393 (2025)

[34] Nithya, C., Lakshmi, C., Thenmozhi, K., Harshavardhan, M., Kumaran, R., Meikandan, P.V., Mahalingam, H., Amirtharajan, R.: Secure gray image sharing framework with adaptive key generation using image digest. Scientific Reports **15**(1), 8854 (2025)

[35] Majumdar, R., Ghosh, P., Modak, S., Biswas, A., Khatun, F., Yogi, B.: Chaos-driven image encryption using zigzag patterns and chebyshev dynamics. In: 2025 International Conference on Artificial Intelligence and Emerging Technologies (ICAIET), pp. 1–6 (2025). IEEE

[36] Majumdar, R., Modak, S., Biswas, A., Ghosh, P., Yogi, B.: Icar30: Image encryption combining ikeda map and cellular automata rule 30. In: International Symposium on Artificial Intelligence, pp. 413–426 (2025). Springer

[37] Yogi, B., Khan, A.K.: Efficient shared secret key distribution using cellular automata for hybrid cryptosystems. Franklin Open, 100465 (2025)

[38] Cao, X., Gao, H., Qin, T., Zhu, M., Zhang, P., Xu, P.: Boundary aware microscopic hyperspectral pathology image segmentation network guided by information entropy weight. Frontiers in Oncology **15**, 1549544 (2025)

[39] Majumdar, R., Mallick, T., Mahajan, S., Paral, I., Roy, S., Yogi, B.: A hybrid approach to image encryption using rule 150 cellular automata and lozi map. In: 2025 International Conference on Artificial Intelligence and Emerging Technologies (ICAIET), pp. 1–6 (2025). IEEE

[40] Peng, J., Chen, C.: Rpcc: Rectified pearson correlation coefficient for radiance fields optimization. IEEE Signal Processing Letters (2025)

[41] Lee, J.C., Park, H.W., Kang, Y.N.: Feasibility study of structural similarity index for patient-specific quality assurance. Journal of Applied Clinical Medical Physics **26**(3), 14591 (2025)

[42] Hosseini-Siyanaki, M., Sagdic, H.S., Raviprasad, A.G., Munjerin, S.E., Prodigios, J.C., Anthony, E.Y., Hochhegger, B., Forghani, R.: Multi-energy evaluation of image quality in spectral ct pulmonary angiography using different strength deep learning spectral reconstructions. Academic Radiology **32**(5), 2953–2965 (2025)

[43] Milovic, C., Tejos, C., Silva, J., Shmueli, K., Irarrazaval, P.: Xsim: A structural similarity index measure optimized for mri qsm. Magnetic resonance in medicine **93**(1), 411–421 (2025)

[44] Alexan, W., Hosny, K., Gabr, M.: A new fast multiple color image encryption algorithm. Cluster Computing **28**(5), 1–34 (2025)

[45] Alshehri, H.: Secure image encryption using a 4d chaotic system and langton's ant cellular automaton. Scientific Reports **15**(1), 41918 (2025)

[46] Alexan, W., Shabasy, N.H.E., Ehab, N., Maher, E.A.: A secure and efficient image encryption scheme based on chaotic systems and nonlinear transformations. Scientific Reports **15**(1), 31246 (2025)

[47] Al-Dayel, I., Nadeem, M.F., Khan, M.A., Abraha, B.S.: An image encryption scheme using 4-d chaotic system and cellular automaton. Scientific Reports **15**(1), 19499 (2025)

[48] Qayyum, T., Shah, T., Khan, I., Popa, I.-L.: A design of multiple color image encryption scheme based on finite algebraic structures. Scientific Reports **15**(1), 42571 (2025)

[49] Alexan, W., Youssef, M., Hussein, H.H., Ahmed, K.K., Hosny, K.M., Fathy, A., Mansour, M.B.M.: A new multiple image encryption algorithm using hyperchaotic systems, svd, and modified rc5. Scientific Reports **15**(1), 9775 (2025)

[50] Liu, Z., Wang, Y., Liu, J., Feng, J., Zhang, L.Y.: A newly image encryption scheme based on 3-d coupled map lattice and baker map. Cybersecurity **9**(1), 103 (2026)