RESEARCH PAPER

Lightweight Adaptive Chaotic Image Encryption with Dual-Diffusion Mechanism for Secure Medical IoT Applications

Madan Mishra[1*], Rakesh Kumar[2]

[1]Department of Computer Science and Engineering, Madan Mohan Malaviya University of Technology, Gorakhpur (U.P.), India, 273010. Email: mmadan.lko74@gmail.com (Corresponding Author)
[2]Department of Computer Science and Engineering, Madan Mohan Malaviya University of Technology, Gorakhpur (U.P.), India, 273010. Email: rkcs@mmmut.ac.in
***Corresponding author: Madan Mishra, Department of Computer Science and Engineering, Madan Mohan Malaviya University of Technology, Gorakhpur (U.P.), India, 273010**
Email: mmadan.lko74@gmail.com

Received: 28th May, 2026; **Revised:** 10th June, 2026; **Accepted:** 14th June, 2026; **Available Online:** 16th June, 2026

ABSTRACT

Background

In this research article, a chaos and encryption-based framework for resource-constrained environments is proposed, combining the advantages of dynamic S-boxes and a two-way diffusion strategy to increase both security and computational efficiency (lightweighting). The framework utilizes a hybrid chaotic system (sine and logistic maps) with plaintext-dependent feedback to enhance sensitivity and unpredictability.

Objective

A unified architecture is developed, and the framework's operation with specific chaotic configurations (Logistic, Sine, Henon, Hybrid, Enhanced Hybrid, Logistic-Sine, and Hyperchaotic maps) is compared in terms of security and operational aspects to validate the developed methodology and framework.

Materials and Methods

Experiments using standard benchmark images from various medical and standard image datasets yielded nearly ideal entropy values of 8 (approx. 7.996-7.998), indicating high unpredictability and even pixel distribution. The proposed scheme withstood strong differential attacks with NPCR around 99.5% and UACI around 33%, demonstrating strong effective diffusion. The method has balanced bit uniformity, a low correlation coefficient (approx. 0), suitable key sensitivity (approx. 99.6%), and robustness against various statistical and cryptanalytic attacks. The cryptographic framework stands against known-plaintext/chosen-plaintext attacks to provide strong structural security, along with decrypted images from different datasets, with no information.

Results

Moreover, in addition to conventional security assessment, the suggested methodology places paramount importance on comprehensive performance analysis, examining its relevance to energy-aware cryptography design. Based on experiments in this framework, lightweight and hybrid chaotic configurations provide a similar degree of security to complex hyperchaotic configurations while consuming less energy and achieving higher throughput. From the results, hybrid-based solutions strike a better balance among energy consumption, security, and computational complexity, and a performance-energy analysis indicates that lightweight chaotic maps are best suited for high-throughput, real-time applications with lower energy consumption.

Conclusion

The proposed framework is a good fit for medical Internet of Things (IoT) platforms, embedded healthcare devices, and real-time image transmission applications.

Keywords: Image Encryption, Chaos Theory, Lightweight Cryptography, NPCR, UACI, IoT Security.

How to cite this article: Mishra M, Kumar R. Lightweight Adaptive Chaotic Image Encryption with Dual-Diffusion Mechanism for Secure Medical IoT Applications. Int J Drug Deliv Technol. 2026;16(60s):925-945. DOI: 10.25258/ijddt.16.60s.105

Source of support: Nil.
Conflict of interest: None

1. Introduction

1.1 Background

Due to the advancement in digital photographic technology and networked multimedia, a huge amount of medical visual data is delivered and stored across a widespread range of application fields, such as telemedicine applications [1], intelligent surveillance [2], remote sensing [3], and Smart City platforms for real-time visual information in a public secure network of insecure networks. Confidentiality, data integrity, and privacy are difficult to protect from the public. Therefore, secure and efficient image encryption systems have become an important topic and attracted much attention in modern information security.

Medical images or scans and X-ray reports have statistical characteristics distinct from those of text data, including large volume, strong spatial correlation between neighbouring pixels, and redundancy. This means traditional encryption schemes like DES [5] and AES [4] can only provide poor performance when applied to medical images across different data sets. In [4,5], it is shown that DES and AES can provide robust cryptographic security. Still, neither is suitable for the varied structural features of medical images and incurs higher computational costs and reduced efficiency in real-time applications and limited-resource environments. The strong correlation [6] between neighbouring pixels in an image further degrades the performance of traditional block ciphers unless additional preprocessing or transformations are used.

Lately, various chaos-based cryptography methods have been proposed to overcome those difficulties mentioned above [7]. This is due to many important characteristics of chaotic systems that support a secure encryption scheme [8], such as sensitivity to initial conditions, deterministic pseudo-randomness, and ergodic behaviour. The sensitive nature [9] means that even tiny changes in the initial values can make a dramatic difference in the encryption result, thereby increasing security and making the key sensitive [10]. The second characteristic, pseudo-randomness, enables the generation of a chaotic sequence for keystream or permutation indices; in addition, ergodicity helps provide a uniform distribution, making the encrypted medical images statistically unpredictable.

These advantages could not prevent the current medical images encryption systems [11]. Some of those encryption systems used low-dimensional Chaotic map (LDCM) encryption schemes, which could be vulnerable to brute-force attacks by reducing the key space size [11, 12, 13, 14, 15]. On the contrary, others that rely on insufficient coupling within the chaotic system generation with the plaintext data [12, 16] could be hacked using chosen-plaintext and known-plaintext attacks [13]. High-dimensional Chaotic maps or hyperchaotic encryption algorithms increase security but also computational complexity and power consumption, which are not suitable for lightweight systems and devices [12]. The insufficient design of the chaos-based diffusion model could yield unstable or inadequate differential measurements, such as NPCR and UACI, indicating that the system is susceptible to differential attacks [15].

This study introduces a lightweight, adaptive chaotic image encryption approach to mitigate the challenges of medical image encryption by harmonizing security with computational efficiency. The proposed scheme, which uses a hybrid chaotic system as described in Reference [16], combines the logistic and sine maps' nonlinear dynamics as discussed in Reference [17], but with feedback from the plaintext, thereby making the chaotic sequence adaptive to the plaintext and making it more resilient to chosen plaintext and differential attacks as in Reference [18]. To enhance security further, a chaos-driven S-box, which uses a dynamic replacement strategy as noted in Reference [19], brings more confusion in encryption and a dual-direction diffusion mechanism [20], having forward and backward phases to ensure that a slight change in the plaintext spreads throughout the entire ciphertext and yields complete avalanche and diffusion effects. One other noticeable characteristic of the proposed framework, its lightweight structure, means it avoids using high dimensional chaotic models, as discussed in Reference [21], transform domain processing similar to Reference [22] and large-scale matrix operations, similar to Reference [23], instead employing scalar arithmetic operations and low dimensional chaos generation to reduce time and power consumption for real-time medical applications and resource constrained medical Internet of things, IoT environment.

All test performed to measure the performance and security for medical image encrypted by the proposed encryption technique, in the area of Information Entropy [24], Number of Pixels Change Rate (NPCR) [25], Unified Average Changing Intensity (UACI) [25], Correlation coefficients [26],

Lyapunov exponent [27] and National Institute of Standards and Technology (NIST) based Randomness tests [28], showed a close to ideal result value for entropy, resistance to differential attacks, robust statistical randomness and reasonable processing cost.

1.2 Hybrid Chaotic Adaptive System

To achieve the desired outcome, we introduce a Hybrid Chaotic Adaptive system, defined by the following equations.

$$x_{n+1} = (rx_n(1 - x_n) + \beta \sin(\pi y_n) + f_n) \bmod 1 \quad (1)$$

$$y_{n+1} = (\mu \sin(\pi y_n) + \gamma x_n + f_n) \bmod 1 \quad)$$

In the equations

- $x_n, y_n \rightarrow$ State variables in $[0, 1]$
- $rx_n(1 - x_n) \rightarrow$ Logistic map (chaotic backbone)
- $\sin(\pi y_n) \rightarrow$ Nonlinear trigonometric perturbation
- $\beta, \gamma \rightarrow$ Coupling strengths
- $\mu \rightarrow$ Controls sine-map dynamics
- $f_n \rightarrow$ External/feedback forcing (can be plaintext dependent)
- mod 1 → Keeps values bounded, enhances randomness.

We investigate the two-dimensional chaotic map using logistic and trigonometric nonlinearities and external forcing. Modular operation between the two state variables establishes the 'closed loop' mutual excitation, and hence the trajectory of the system will be constrained rather than unbounded compared with those classical one-dimensional ones. Hence, we may change its behaviour from a predictable fixed cycle to full chaos; the key space will be larger, along with multiple parameters, and may bring advantages for lightweight image encryption and coding. The trajectories of each state variable are uniformly distributed, sensitive, and unpredictable. The phase diagrams exhibit complex, weird attractors with ergodic properties, while the bifurcation displays vast, fully developed chaotic regions with small, predictable windows. Hence, it may apply to encryption, especially to image encryption.

1.2.1 Bifurcation Diagram of Proposed System

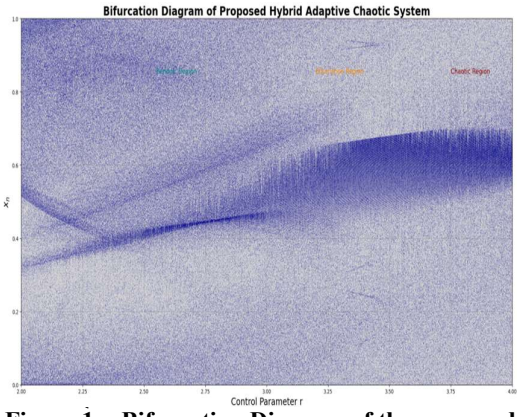


Figure 1a: Bifurcation Diagram of the proposed Hybrid Adaptive Chaotic System

The bifurcation diagram (Figure 1a) illustrates that as the control parameter r (the r value ranging from 2.0 to 4.0), is increased, it moves from weakly ordered dynamics to fully well-developed chaotic mode, for example; when r ≈2.0 to 2.3 values, then the trajectory show low (small) spreading/diffusion, indicates weak chaos or quasi-periodic behaviour of system and for the r ≈2.3 values to 3.0 values it shows some diffusion along with trajectories of systems, it means diffusion increases in bifurcating branches, shows onset of bifurcation and nonlinear instabilities, so, when for the r ≈3.0 to 3.4 value it shows dense bifurcating branches with multilayer orbit of systems, it indicates high nonlinear bifurcating branches, shows chaotic mode operation occurs and for the r ≈3.4 to 4.0 value it clearly indicates fully well-established chaotic mode of operation of system. It means it enhances sensitivity, as indicated by higher density and randomness along the trajectories/orbits, which is advantageous for encryption techniques, cryptographic security, and the analysis of systems with higher diffusion values. So, we will see its effect in some cases.

1.2.1.1 Impact of forcing term f_n on Bifurcation Diagram

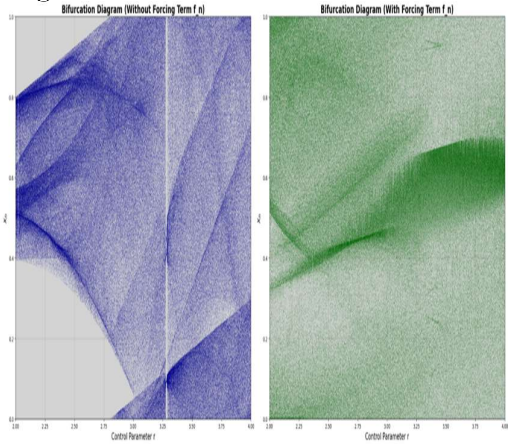


Figure1b: Bifurcation Diagram of the proposed Hybrid Adaptive Chaotic System

As can be seen in the bifurcation analysis of Figure 1b, while the open-loop critical bifurcation figures remain consistent, the plaintext-dependent forcing term f_n dramatically shifts the chaotic system's nonlinearity; the bifurcation values that describe the transition from steady state to period-doubling and chaotic behaviour change under the influence of f_n. Furthermore, the chaotic bands vary in their orbital density, attractor edge position, and chaotic windows, thereby demonstrating that the forcing term dictates the phase-space evolution. Moreover, the fact that f_n explicitly depends on the plaintext introduces a time-varying dynamic perturbation. It thus improves state-space mixing and diffusion characteristics, as well as data sensitivity. The system's complexity is further increased because even small changes to the plaintext lead to different results in the chaotic sequences and ciphertext. This all reinforces the system's cryptographic capability, improving robustness against cryptanalytic attacks.

1.2.1.2 Phase diagram of the proposed system with forcing and without forcing term

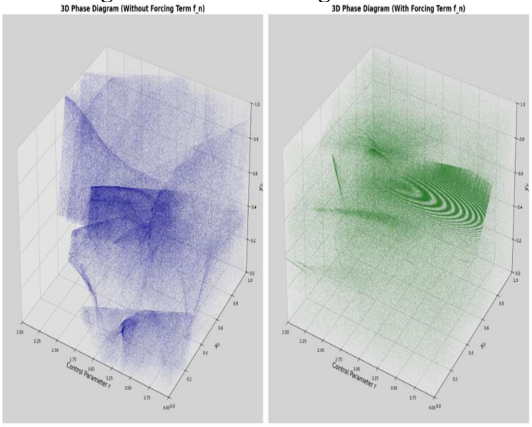


Figure 2: Phase diagram of the proposed Hybrid Adaptive Chaotic System without(Figure 2a) and with a forcing term (Figure 2b)

The three-dimensional phase diagrams Figure 2 shows that the plaintext-dependent forcing term influences the level of chaos generated by the system. Figure 2 presents a phase diagram without and with (Figure 2a and 2b respectively) a plaintext forcing term. The phase diagram without the forcing term shows the trajectory of the chaotic function (plaintext), which appears dispersed and irregular, indicating ill-structured, less controlled behaviour. In contrast, the phase diagram with plaintext as forcing depicts a spiral-like, well-defined attractor and thus, enhanced chaotic dynamics through nonlinear couplings and strongly deterministic chaotic behaviour. With the introduction of the plaintext as a fuzzy forcing term, a more organized and predictable state or structure (a well-defined attractor with a densely evolved trajectory) is observed. The fuzzy forcing will enhance complexity and sensitivity to changes in the slightest fluctuations, improve state-space mixing, and further shape the chaotic attractor while simultaneously bounding the chaotic evolution. This implies the presence of a fuzzy mechanism that increases and makes determinism predictable within the system, potentially driven by the structure of the fuzzy plaintext term itself, which influences chaotic system dynamics and enriches diffusion, sensitivity, and unpredictability in secured cryptographic and image encryption applications.

Contributions of the proposed method can be summarised as follows:

(i) An adaptive hybrid chaotic system has been designed with a plaintext-dependent feedback mechanism.

(ii) For confusion, a dynamic chaos-based S -box has been devised and used.

(iii) To improve avalanche characteristics, a dual-direction diffusion mechanism has been implemented.

(iv) An energy-efficient, lightweight encryption framework has been developed with heightened security ideal for its application in IoT-based solutions.

The remainder of this paper is organized as follows: Section II reviews related work on chaos-based image encryption. Section III explores the proposed methodology, and Section IV contains the security analysis of the proposed cryptosystem. Performance evaluation and experimental results are discussed in Section V. Section VI concludes and outlines directions for future research.

2. Related Work

Medical image encryption via chaos is becoming a hot research topic [29], with considerable growth. Early methods moved from basic one-dimensional chaotic systems [29] toward more elaborate, combined approaches [30], hyperchaotic setups [31], and adaptive designs [32]. Initially, researchers relied on common chaotic functions such as the logistic, sine, and tent maps [33]. These generated pseudorandom sequences were primarily used for permutation and diffusion; they were effective at reducing pixel correlations and achieving decent entropy. However, these earlier efforts ran into several security issues: they had a limited key space, relatively low complexity, and often could not withstand differential or statistical attacks [29].

Faced with the drawbacks and shortcomings of current methods, recent investigations have aimed to bolster the resilience of chaotic encryption systems [34]. This involves implementing structural and algorithmic enhancements. A prevalent strategy among the many available techniques is to employ hybrid chaotic systems [35]. These introduce greater complexity and greater unpredictability by merging two or more distinct chaotic maps. For instance, researchers have commonly employed modified

skew-tent [36] and sine-chaotic hybrid systems [36] to increase their defence against diverse types of assaults. Independently, multi-chaotic systems, built by integrating various maps such as the Henon [37], logistic [38], or sine maps, are frequently used to craft a ciphertext that achieves a uniform distribution, effectively resembling noise.

Another significant advancement appears in hyperchaotic and multidimensional chaotic systems [39]. These systems offer greater degrees of freedom and exhibit more intricate dynamics than their one-dimensional counterparts [40]. Recent research has proposed new two-dimensional and multi-scroll chaotic systems exhibiting robust chaotic behaviour. This robustness is supported by evidence from Lyapunov exponents, bifurcation analyses, and entropy measurements [41]. While these systems markedly enhance sensitivity to the key and improve overall security, they often incur increased computational overhead. This elevates the complexity, potentially making them less practical for resource-constrained applications.

Meanwhile, some researchers [42] have started implementing plaintext dependency in chaotic systems in an attempt to be resistant against modern cryptographic attacks by linking the generation of a chaotic sequence to image data, so that effects dependent mechanisms in chaotic systems have been employed [42] where the chaotic sequence is somehow generated from the input image to ensure the butterfly effect. For example, a chaos-based block permutation and bit-level diffusion scheme [43] with plaintext feedback is a robust cipher against chosen-plaintext and known-plaintext attacks, i.e., plaintext and ciphertext are interdependent in a cycle; however, an adaptive mechanism has made significant progress in applying real-world chaos-based encryption.

Simultaneously, efforts have also been devoted to performance optimization and computational efficiency [44] when dealing with large-scale image data and real-world applications, for instance, by using a parallel encryption framework or a bit-plane approach to improve throughput while maintaining security. For example, a parallel chaotic encryption technique that operates on multiple bit planes simultaneously has shown significant speedups without compromising encryption quality, and multi-image encryption techniques that effectively leverage parallel processing architectures have improved computational efficiency in high-volume data environments.

The relevance of IoT and embedded systems has also made energy efficiency and lightweight cryptography areas of growing research interest. Therefore, the intention to reduce expenses by reducing processing and computational power in lightweight chaos-based encryption has spurred new research in the field. Recently, some lightweight chaotic encryption schemes have been proposed for IoT, healthcare, and wearables, meaning they can provide good encryption results with low energy consumption, along with fast processing times. The proposed hybrid lightweight cryptographic designs based on chaos and simple mathematical operations exhibit good NPCA and UACI along with low resource consumption. Furthermore, the advent of lightweight cryptography standards, such as the NIST Lightweight Cryptography Initiative, signals an increasing need for power-efficient cryptographic algorithms in resource-constrained environments. These standards focus on aspects such as power consumption, memory footprint, and throughput, emphasizing the need for cryptographic systems that offer a good trade-off between security and efficiency.

These provide crucial guidance in gauging the pragmatic feasibility and relevance of modern lightweight encryption schemes, including those based on chaos. Recent works have focused on coupling chaos-based encryption with emerging technologies such as artificial intelligence (AI), machine learning (ML), and neural networks [48]. These hybrid approaches aim to dynamically adjust parameters, improve S-box design, and enhance resistance to advanced attacks, thereby improving the system's overall robustness. AI-assisted chaos-based frameworks have been proposed to adapt chaos system parameters based on, say, image characteristics [49], thereby enhancing security and efficiency. However, overall, these come at the expense of additional computational overhead, which might limit their usability in lightweight environments. The choice of an appropriate trade-off among security strength, computational efficiency, and energy consumption is yet to be established, since high-dimensional chaotic maps that provide a high security regime are generally computationally heavy, and lightweight schemes, which show low complexity, tend to be less reliable. On top of that, achieving similar differential behaviours (e.g., NPCR, UACI) and developing new attacks based on deep learning algorithms remain open research questions from a defensive point of view.

3. Proposed Methodology

3.1 Notation and Preliminaries

Let the grayscale input image be $P \in \{0,1,\dots,255\}^{H\times W}$ with total pixels $N = H \times W$, and let K denote the secret key. The image is flattened into a 1D sequence.

Let:

- $P \in \{0,1,\dots,255\}^{H\times W}$: grayscale input image
- $N = H \times W$: total number of pixels
- K: user secret key
- $H(K)$: hash of key using SHA-256
- C: encrypted image

Flatten:

$P \rightarrow \mathrm{p} = \{p_1, p_2, \ldots, p_N\}$
(3)
.

3.2 Key Scheduling Mechanism

The key is hashed using a Hash Key H. The secret key K is transformed using a secure hash function H(SHA-256) to generate a fixed-length hash value h, which is subsequently used to derive the initial conditions and control parameters of the chaotic system, ensuring high key sensitivity and security.

$\mathrm{h} = \mathrm{H(K)}$
(4)

The initial conditions of the chaotic system are derived from the hashed key to ensure strong key sensitivity and randomness. Specifically, the first two components of the hash value are normalized and used to initialize the system as

$x_0 = \frac{h_1}{255} + \delta, y_0 = \frac{h_2}{255} + \delta$
(5)

where h_1 and $h_2$represent byte values extracted from the hash output h. The division by 255 maps these values into the interval $(0, 1)$, which is suitable for chaotic map initialization. A small positive constant $\delta > 0$ is added to avoid degenerate cases such as fixed points or zero states that may weaken chaotic behavior. This formulation ensures that even a slight variation in the secret key produces significantly different initial conditions, thereby enhancing the unpredictability and security of the proposed cryptosystem.$\delta > 0$ is a small perturbation constant introduced to avoid fixed points and degenerate dynamics, while $r = 3.99$ and $\mu = 0.99$ Are control parameters selected to ensure strong chaotic behavior in the system?

- $\delta > 0$ avoids fixed points.
- control parameters:

$$r = 3.99, \mu = 0.99$$

The control parameters of the chaotic system are derived from the hash output to ensure randomness and key dependence. Specifically, the parameters are defined as

$\beta = \frac{h_3}{255}, \gamma = \frac{h_4}{255}$
(6)

where h_3 and h_4 are byte values extracted from the hash sequence h. The normalization by 255 maps these values into the interval $(0, 1)$, which is essential for maintaining stable yet chaotic system dynamics. By linking $\beta$and γ directly to the hashed key, the system ensures that even minor variations in the input key led to significant changes in the control parameters, thereby altering the chaotic trajectories. This strengthens key sensitivity, increases unpredictability, and enhances resistance against brute-force and statistical attacks.

3.3 Adaptive Hybrid Chaotic System

The system evolves as:

$x_{n+1} = (rx_n(1 - x_n) + \beta \sin(\pi y_n) + f_n) \bmod 1$
(7)

$y_{n+1} = (\mu \sin(\pi y_n) + \gamma x_n + f_n) \bmod 1$ (8)

Equations (7) and (8) define the evolution of the proposed adaptive hybrid chaotic system, where the next states x_{n+1} and $y_{n+1}$are generated by combining logistic and sine map dynamics with cross-coupling and plaintext feedback. The term $rx_n(1 - x_n)$ensures strong nonlinearity from the logistic map, while $\sin(\pi y_n)$ introduces additional chaotic behavior from the sine map. The parameters β and γ control the coupling strength between the two state variables, enhancing system complexity. The inclusion of the plaintext-dependent feedback term f_n makes the system adaptive, ensuring that the chaotic sequence varies with the input image, thereby improving resistance against chosen-plaintext and differential attacks. Finally, the modulo operation confines the outputs within the interval. $(0, 1)$, maintaining bounded chaotic dynamics.

Plaintext Feedback Term

$f_n = \frac{P_{(n \bmod N)}}{255}$
(9)

Equation (9) defines the plaintext-dependent feedback term that enhances the adaptivity of the chaotic system.p_n represents the pixel values of the flattened image and N is the total number of pixels. The modulo operation $(n \bmod N)$ ensures cyclic access to pixel values, thereby keeping the feedback term well-defined across all iterations. Dividing by 255 normalizes the pixel intensity to the specified range. $(0, 1)$, making it compatible with the chaotic system. By incorporating f_n into the system equations, the chaotic sequence becomes directly dependent on the plaintext, thereby introducing strong plaintext sensitivity and significantly improving resistance to chosen plaintext and differential attacks. This introduces plaintext sensitivity and resistance to chosen-plaintext attacks. It gives the output sequence.

$s_n = (x_n + y_n + x_n y_n) \bmod 1$
(10)

In the above equation (10), the output sequence s_n is generated by combining the current chaotic states $x_n$and y_n along with their nonlinear interaction term $x_n y_n$, which increases complexity and randomness. The modulo one operation ensures that the resulting values remain within the interval. $(0, 1)$. This formulation enhances the statistical properties of the sequence, making it suitable for cryptographic

applications such as permutation, substitution, and key stream generation.

3.4 Chaotic Sequence Partitioning

Generate total sequence:

$s =$

$\{s_1, s_2, \ldots, s_{256+} \quad\}$

(11)

Equation (11) defines the complete sequence. $s = \{s_1, s_2, \ldots, s_{256+2N}\}$generated from the chaotic system. It serves as the master key stream, large enough to support all encryption stages—substitution, permutation, and diffusion.

Partition:

- S-box sequence:

$s^{(1)} = \{s_1, \ldots, s_{256}\}$

(12)

In equation (12), the first 256 elements of the chaotic sequence are extracted to form the S-box sequence. These values are used to construct a substitution box, enabling nonlinear transformations of pixel values and enhancing confusion in the encryption process.

- Permutation sequence:

$s^{(2)} = \{s_{257}, \ldots, s_{256+N}\}$

(13)

In equation (13) above, the next N Elements are used to generate the permutation sequence. This sequence determines how pixel positions are shuffled, effectively scrambling the image's spatial arrangement and increasing security by introducing confusion.

- Diffusion key:

$s^{(3)} = \{s_{256+N+1}, \ldots, s_{256+2N}\}$

(14)

In equation (14) above, the final N Elements form the diffusion key. These values are used to modify pixel intensities so that small changes in the plaintext propagate widely in the ciphertext, ensuring strong diffusion and resistance to differential attacks.

3.5 Dynamic S-box Construction

A dynamic substitution box S is generated using the Fisher–Yates shuffle*:*

$S = \pi(\{0,1,2, \ldots, 255\})$

(15)

The equation (15) represents that the S-box, S is obtained by applying a permutation function π to the ordered set of all possible 8-bit values. In other words, it rearranges the elements. 0 to 255 into a new, unique order, ensuring a one-to-one (bijective) mapping between input and output values. This property guarantees that every input byte maps to a unique output byte, enabling both secure substitution and correct decryption.

where the permutation index is:

$j = \lfloor (s_i \times 10^6) mod\ (i+1) \rfloor$

(16)

The index in equation (16) maps the chaotic value. $s_i \in (0,1)$into an integer in the range $[0, i]$, which is used in the Fisher–Yates shuffle to swap elements. By deriving j from a chaos-based sequence, the permutation becomes key-dependent and highly unpredictable, ensuring strong randomness while preserving bijectivity (no repeated indices), thereby enhancing confusion and nonlinearity in the S-box construction.

The Inverse S-box S^{-1}satisfies:

$S^{-1}(S(i)) = i$

(17)

In equation (17), applying. S followed by S^{-1}returns the original value, ensuring lossless decryption and confirming that the S-box is bijective (invertible).

3.6 Permutation Stage

Defines permutation index:

$\sigma = \text{argsort}(s^{(2)})$

(18)

This step, as given in equation (18), generates a permutation index. σ from the chaotic sequence $s^{(2)}$. The argsort operation returns the indices that sort the sequence in ascending order, producing a pseudo-random permutation pattern used to rearrange pixel positions.

$p'_i = p_{\sigma_i}$

(19)

The next step involves constructing a Permuted vector, as given by equation (19). Using the permutation index σ, the original pixel vector p is rearranged to form the permuted vector p'. Each element p'_itakes the value of the original pixel at position σ_i, effectively scrambling the image structure for enhanced security.

3.7 Substitution Stage

$u_i =$

$S(p'_i)$

(20)

The next step, shown by equation (20), applies the S-box transformation to each element of the permuted vector. p'. For every index i, the pixel value $p'_i$is replaced by its corresponding S-box output u_i. This nonlinear substitution increases confusion by altering pixel intensities in a key-dependent and seemingly irreversible manner, thereby strengthening resistance to statistical and brute-force attacks.

3.8 Key Stream Generation

$\boldsymbol{k_i = \lfloor s_i^{(3)} \times 255 \rfloor}$

(21)

The next step. to convert the resulting $\boldsymbol{s_i^{(3)}}$(typically in the range (0,1)) into an integer key $\boldsymbol{k_i}$. k_i in the range 0 to 255. The multiplication by 255 scales the value to the grayscale pixel range, and the floor operation ensures an integer output. These keys are then used during the diffusion stage to modify pixel

values, helping to spread small changes across the ciphertext and strengthen security.

3.9 Dual Diffusion Mechanism

Forward Diffusion

$$c_1 = (u_1 + k_1) \bmod 256 \quad (22)$$

In the next step, given by equation (22). The first cipher element is generated by combining the substituted pixel $u_1$with the diffusion key k_1. The modulo 256 operation ensures the result stays within the valid 8-bit pixel range (0–255). This initializes the diffusion process.

$$c_i = (u_i + k_i + c_{i-1}) \bmod 256, i > 1 \quad (23)$$

Each subsequent cipher value depends not only on the current substituted pixel. $u_i$and key k_i, but also on the previous cipher value c_{i-1}. This creates a chaining effect, where a small change in the input propagates through all following elements, achieving strong diffusion and resistance to differential attacks.

Backward Diffusion

$$C_N = c_N \oplus k_N \quad (24)$$

For Backward diffusion, as shown in equation (24), the final ciphertext element C_N is obtained by XORing the last forward-diffused value $c_N$with the key k_N. This starts the backward diffusion stage and adds a layer of key-dependent mixing.

$$C_i = c_i \oplus k_i \oplus C_{i+1}, i = N-1, \ldots, 1 \quad (25)$$

In the further step, each preceding ciphertext element C_i is computed using the current forward-diffused value c_i, the key k_i, and the next ciphertext value C_{i+1} as shown in equation (25). This reverse chaining ensures that changes in any part of the sequence influence earlier elements as well, providing bidirectional diffusion and stronger security.

3.10 Decryption Process

The Decryption process is done by following the reverse steps:

1. Reverse backward diffusion
2. Reverse forward diffusion
3. Apply inverse S-box.
4. Apply inverse permutation.

After applying the reverse steps, we get the original image.

3.11 Algorithm Pseudocode

The pseudo code for the encryption algorithm is as follows

Algorithm 1: Encryption

Input: Image P, Key K

Output: Cipher image C

1: Compute hash h = SHA-256(K)
2: Extract parameters x0, y0, β, γ
3: Generate chaotic sequences of length (256 + 2N)
4: Partition s into:
  s1 → S-box
  s2 → permutation
  s3 → keystream

5: Construct S-box S using Fisher-Yates shuffle and then get inverse S^{-1}

6: Flatten image P → p

7: Permutation:
  σ = argsort(s2)
  p' = p[σ]

8: Substitution:
  u[i] = S(p'[i])

9: Key stream:
  k[i] = floor(s3[i] * 255)

10: Forward diffusion:
  c[1] = (u[1] + k[1]) mod 256
  for i = 2 to N:
    c[i] = (u[i] + k[i] + c[i-1]) mod 256

11: Backward diffusion:
  C[N] = c[N] XOR k[N]
  for i = N-1 down to 1:
    C[i] = c[i] XOR k[i] XOR C[i+1]

12: Reshape C → image

The pseudo code for the decryption algorithm is as follows

Algorithm 2: Image Decryption

Input:

- Cipher image C
- Permutation index π
- Inverse S-box S^{-1}
- Chaotic sequence $\{s_i\}$

Output:

- Recovered image I

Step 1: Initialization

1. Flatten cipher image:

flat ← reshape(C)

2. Compute key stream:

$k_i = \lfloor s_{256+N+i} \times 255 \rfloor$

Step 2: Reverse Diffusion

3. Initialize array c
4. Last element:

$c_N = flat_N \oplus k_N$

5. For $i = N-1$ down to 1:

$c_i = flat_i \oplus k_i \oplus flat_{i+1}$

Step 3: Reverse Forward Diffusion

6. Initialize array u

7. First element:

$u_1 = (c_1 - k_1) mod 256$

8. For $i = 2$ to N:

$u_i = (c_i - k_i - c_{i-1}) mod 256$

Step 4: Inverse Substitution

9. Apply inverse S-box:

$p'_i = S^{-1}(u_i)$

Step 5: Inverse Permutation

10. Initialize output array P
11. For all i:

$P_{\pi(i)} = p'_i$

Step 6: Reshape

12. Reshape P into image:

$I = \text{reshape}(P, H, W)$

End Algorithm

3.12 The detailed flow diagram of the encryption/decryption algorithm

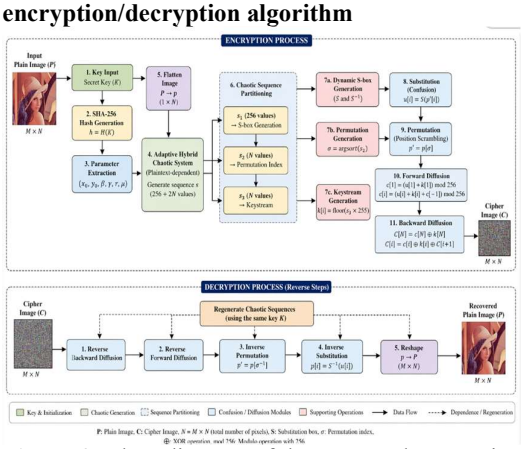


Figure 3: Flow diagram of the proposed encryption and Decryption algorithm

3.13 Theoretical Properties

3.13.1 Bijectivity

- **S-box: permutation:** A permutation-based S-box maps each input value uniquely to another value, ensuring a one-to-one correspondence. This guarantees the existence of an inverse S-box, enabling exact recovery of the original data during decryption.
- **diffusion: reversible operations:** Diffusion uses reversible operations such as modular addition and XOR, which can be inverted during decryption. These operations ensure strong pixel dependency while preserving lossless reconstruction of the plaintext.

3.13.2 Sensitivity

- **From chaos:**

$\frac{d(x_n)}{dx_0} \to \infty$ (26)

The expression $\frac{dx_n}{dx_0} \to \infty$ represents the sensitivity to initial conditions, a fundamental property of chaos. It indicates that an infinitesimally small change in the initial value. x_0 leads to exponentially diverging trajectories as n increases.

This behaviour implies that two identical starting points will evolve into completely different states over time, making long-term prediction impossible. In cryptography, this property ensures high key sensitivity and unpredictability, strengthening security.

- **Key sensitivity:** The exponential divergence of nearby initial values means even a tiny change in the key produces a completely different chaotic sequence. This ensures high key sensitivity, where small key variations lead to drastically different ciphertext outputs.

3.13.3 Confusion & Diffusion

- **Confusion by using S-box:** The S-box introduces nonlinearity by mapping input pixels to different output values in a complex, key-dependent manner. This obscures the relationship between plaintext and ciphertext, making statistical and analytical attacks difficult.
- **Diffusion by dual chain:** The dual diffusion chain (forward and backward) spreads pixel influence across the entire image in both directions. This ensures that a small change in the plaintext affects all cipher pixels, achieving a strong avalanche effect.

3.13.4 Space Complexity Analysis:

Let $N = H \times W$ be the number of pixels.

The proposed algorithm requires memory for storing intermediate sequences and arrays generated during encryption. The major space components are:

- Input image P: $O(N)$
- Flattened vector p, permuted vector p', substituted vector u: $O(N)$each
- Chaotic sequence $s$of length $(256+2N)$: $O(N)$
- Keystream k: $O(N)$
- Diffusion arrays c, C: $O(N)$
- Permutation indices σ: $O(N)$
- S-box and inverse S-box: $O(256) \approx O(1)$

Total Space Complexity

$S(N) = O(N)$ (27)

Suitability for IOT/Lightweight Cryptography

Since, the encryption mechanism only involves modular addition, XOR, and S-boxes (which are all less hardware-intensive and readily implemented digitally), it is well-suited to lightweight hardware

implementation. Also, its linear structure, like backward-forward diffusion blocks, offers an easy way to pipeline in FPGAs, providing a single pass for stream ciphering. Additionally, it consumes only O(N) memory because it does not involve floating-point arithmetic or require large transformation matrices. Also, the sorting part, which runs in O(N log N), will be replaced by another linear-time permutation method, such as index mapping or Fisher-Yates Shuffle, if it turns out to be hardware-expensive.

4. RESULTS AND DISCUSSION

A. Experimental Setup

We propose a lightweight chaotic cryptographic algorithm for colour images and evaluate it on multiple grayscale images, using standard datasets such as the Vegetable, Lena, and Baboon images. Additionally, we are using custom datasets, such as the PanNuke Dataset and the RSNA Bone Age Dataset on Kaggle. We have resized all the images and encrypted them with all seven proposed chaotic configurations, namely Logistic, Sine, Henon, Hybrid, Enhanced Hybrid, Logistic-Sine, and Hyperchaotic maps. The seven distinct chaotic configurations have been utilized for this purpose and compared in terms of evaluation performance. To evaluate performance and parameters such as entropy, NPCR, UACI, the correlation coefficient, the sensitivity of the keys, sensitivity to the plain text, differential attack resistance, and KPA, the standard image cryptographic metrics were used, as well as energy, throughput, and Execution time.

4.1 Key Space Analysis of the Proposed Method

Let the secret key be denoted as $K \in \{0,1\}^L$, where $L$is the key length. In the proposed scheme, the key is processed using the cryptographic hash function SHA-256, producing a fixed-length hash:

$$h = H(K) \in \{0,1\}^{256}$$

Thus, the effective key space is:

$$| \mathcal{K} | = 2^{256}$$

Since the hash output is partitioned into byte sequences:

$$h = (h_1, h_2, h_3, h_4, \dots)$$

The initial conditions and control parameters are derived as:

$$x_0 = \frac{h_1}{255} + \delta, y_0 = \frac{h_2}{255} + \delta \;\; \beta = \frac{h_3}{255}, \gamma = \frac{h_4}{255}$$

where $h_i \in \{0,1,\dots,255\}$and $\delta > 0$.
Since the mapping from h to parameters $(x_0, y_0, \beta, \gamma)$is deterministic and injective over finite precision, the entropy of the system remains:

$$H(K) = 256 \text{ bits}$$

Hence, the effective key space is not reduced by parameter extraction. Therefore, the key space is sufficiently large (2^{256}), making brute-force attacks infeasible.

4.2 Information Entropy of Different Images from the Dataset in the Proposed Method

$$iH = -\sum p_i \log_2 p_i$$

(28)

The entropy expression in equation (28) measures the randomness of the encrypted image by quantifying the uncertainty in pixel intensity distribution. In the proposed methodology, the dynamic S-box and chaotic permutation–diffusion process ensure that pixel probabilities p_i, i.e., p_i become uniform, maximizing entropy. As a result, the cipher images achieve entropy values close to the ideal value of 8, indicating strong confusion and diffusion properties. This high entropy confirms that the encryption scheme effectively eliminates statistical patterns, making it resistant to entropy-based and statistical attacks.

4.3 Differential Attack Analysis on different images from the data in the proposed method

Table 1: The Entropy, NPCR, and UACI of various images from the dataset

Sno	Image from the dataset	Entropy	NPCR	UACI
1	Lena.png	7.99723219262636	99.623107910156625	33.52211148131127
2	Vegetable.png	7.99758530385 9784	NPCR: 99.5971679687 5	UACI: 33.6050 1756855 086
3	Baboon.png	7.99718634985 9262	NPCR: 99.5681762695 3125	UACI: 33.4117 2162224 2645
4	Cancer_cells.jpg	7.99753279580 4469	NPCR: 99.6124267578 125	UACI: 33.6198 9339192 7086
5	Ankle.jpg	7.99744329828 1562	NPCR: 99.6154785156 25	UACI: 33.5269 5839077 819

As indicated in Table 1, the proposed encryption technique achieves high efficiency in terms of statistical security and diffusion capability. Entropy values are close to the ideal value of 8 for all images. Thus, this shows minimal information revelation and an even distribution of pixels. Moreover

differential attack has also confirmed good robustness as NPCR values are higher than 99.5 which confirms good modifications in the cipher image upon small changes in the plain images and with similar pattern UACI values higher than almost 33 per cent for the average difference between the intensity of cipher images which reveals robust diffusion and stronger avalanche effect respectively along with strong confusion-diffusion as among the different chaotic configurations hybrid and enhanced hybrid chaos had showed more robust performance with more stability over a different dataset against statistical and differential attack.

4.4 Chosen Plain Text Attack analysis on different images from the data in the proposed method.

Structured images, including all-zero, all-maximum, gradient, and checkerboard patterns, were fed into the system to assess its resilience against chosen-plaintext attacks, as illustrated in Table 2. Even though these plaintexts were predictable, the resulting ciphertexts showed entropy values close to ideal (around 7.999) and minimal correlation coefficients. No discernible patterns were visible in the encrypted images. This strongly suggests the proposed method does a solid job of removing structural information. This outcome is attributed to the plaintext-dependent chaotic feedback combined with a dual-diffusion mechanism, which ensures that even carefully controlled inputs yield statistically random outputs. Consequently, the scheme proves robust against attacks involving chosen plaintexts. You can find the CPA test outcomes for these varied images presented in Table 2.

Table 2: CPA Test results on different images from the data in the proposed method

Sno.	Image Type	Entropy	Correlation
1	Zero Image	Entropy: 7.9976	Correlation: 0.000433
2	Max Image	Entropy: 7.9973	Correlation: 0.000436
3	Gradient Image	Entropy: 7.9975	Correlation: 0.002600
4	Gradient Image	Entropy: 7.9969	Correlation: 0.007156

4.5 Visual Analysis of Perfect Decryption on Different Images of the Dataset

Table 3: Visual evaluation of different images on different Datasets using the proposed method.

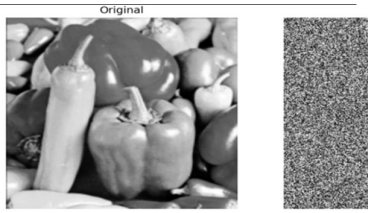
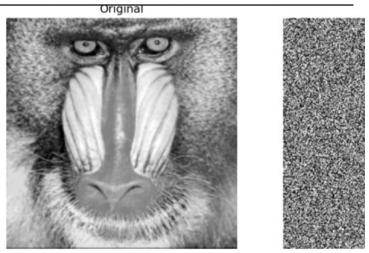
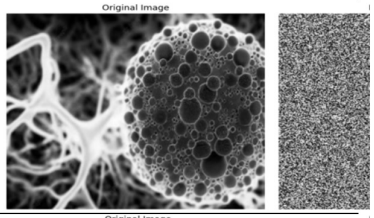
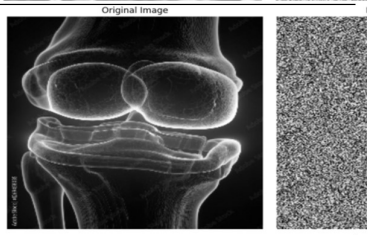
S.no	Image from the dataset	Original Image Encrypted Image Decrypted Image
1	Lena.png	
2	Vegetable.png	
3	Baboon.png	
4	Cancer_cells.jpg	
5	Ankel.jpg	

Table 3 presents a visual inspection of the proposed cryptosystem on standard benchmark images of Lena, Vegetable, and Baboon, as well as images from the Pan Nuke Dataset on Kaggle and the RSNA Bone Age dataset.

In each case, the original images are transformed into noisy-looking encrypted images, confirming that the visual and statistical properties of the original images are lost. The returned decrypted images are visually identical to the original images, which is another confirmation of the encryption method's lossless nature and the correctness of the decryption method. The consistent performance across such diverse images demonstrates the robustness, reliability, and capability of the proposed scheme for secure image transmission.

4.5 Correlation Analysis on different datasets using the proposed method.

Table 4: Correlation analysis of various images from Datasets using the proposed method

Sno	Image from the dataset	Correlation
1	Lena.png	Correlation: 0.008615715606609516
2	Vegetable.png	Correlation: 0.0001320349465604353 7
3	Baboon.png	Correlation: 0.008615715606609516
4.	Cancer_cells.jpg	Correlation: 0.0001201447461056488
5.	Ankle.jpg	Correlation: 0.005655708238689755

Table 4 summarises the coefficient values for close pixels in encrypted images across several general databases, with values that often tend towards zero, either slightly negative or slightly positive. This shows that correlations have been removed from these images. Because a strong security mechanism protects against attacks that rely on statistical features, the values (for images produced by encryption of all maps) of the coefficients for the close pixel were found to be close to zero (e.g., about ±0.01). The results show that the strong relationship between the pixel values in the unencrypted version is eliminated in the encrypted form, particularly in Hybrid and enhanced Hybrid maps.

4.6 Histogram Analysis on images from different datasets using the proposed method.

The cipher image histogram is uniformly distributed, preventing statistical attacks.

Table 5: Histogram Analysis of various images from different datasets

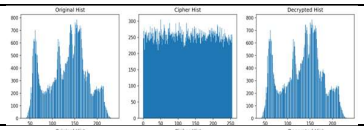
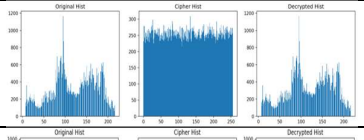
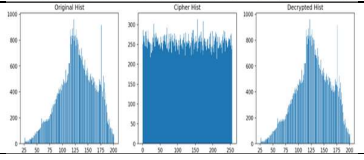
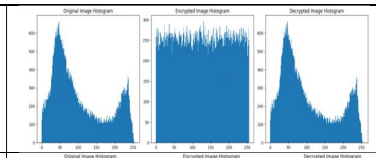
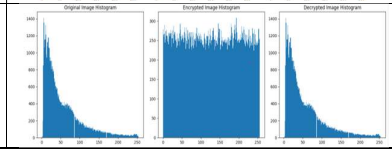
S.no	Image from the dataset	Original Image Encrypted Image Decrypted Image
1	Lena.png	
2	Vegetable.png	
3	Baboon.png	
4	Cancer_cells.jpg	
5	Ankle.jpg	

Table 5 shows the result of histogram analyses for the proposed encryption scheme tested on standard images, namely Lena, Vegetable, Baboon, Pan Nuke Dataset on Kaggle, *and RSNA Bone Age Dataset*. Initially, histograms of the original images revealed uneven distributions with noticeable peak intensities, indicating distinct characteristics in their pixel intensities. In contrast, the encrypted images have uniform distributions, indicating that the pixel values have been homogenized and that no statistical characteristics of the original images can be revealed. Finally, the decrypted images restored their original histograms in a lossless manner. Hence, the results clearly show that the histograms of the encrypted images are as uniform as their original histograms, indicating that the proposed method can resist statistical and histogram-based attacks.

4.7 Lyapunov Exponent

Positive Lyapunov exponent confirms chaotic behaviour and sensitivity to initial conditions.

Table 6: Lyapunov of the various images from Datasets.

Sno	Image from the dataset	Lyapunov Values
1	Lena.png	Lyapunov: 0.626193476449774
2	Vegetable.png	Lyapunov: 0.626193476449774
3	Baboon.png	Lyapunov: 0.626193476449774
4	Cancer_cells.jpg	Lyapunov: 0.626193476449774
5	Ankle.jpg	Lyapunov: 0.626193476449774

Table 6 presents the Lyauponov exponent values for different standard test images, including Lena, Vegetable, Baboon, Pan Nuke Dataset on Kaggle, *and RSNA Bone Age Dataset.* Almost 0.626 is obtained across all these images, with a positive value. In that case, it clearly states that the proposed one is highly sensitive to initial conditions and

strong, and hence called strongly chaotic, which leads to unstable behavior. Although the uniformity of value across different inputs shows that the chaotic dynamics depend heavily on the key-dependent parameters, this ensures stability and reliability for encryption. Therefore, such positive Lyapunov exponents can be used and trusted as an alternative for building secure cryptographic applications.

4.8 Randomness Tests on Images from Datasets using the proposed method.

NIST-based tests confirmation:

Table 7: Frequency test (p>0.001), Runs test (p > 0.01), and Approximate Entropy of various Images from the Dataset

Sno	Image from the dataset	Frequency test (p > 0.01)	Runs test (p > 0.01)	Approximate Entropy
1	Lena.png	Frequency p-value: 0.3634859594186 6435	Runs Test p-value: 0.4685617022153 0435	Approx Entropy: 0.6931411777184 204
2	Vegetable.png	Frequency p-value: 0.4491545771854 214	Runs Test p-value: 0.8525589738676 097	Approx Entropy: 0.6931464963467 673
3	Baboon.png	Frequency p-value: 0.8229650626023 897	Runs Test p-value: 0.5600672698702 424	Approx Entropy: 0.6931434140052 31
4	Cancer_cells.jpg	Frequency Test p-value: 0.6786394906630 684	Runs Test p-value: 0.8382276519515 923	Approx Entropy: 0.6931463529591 81
5	Ankle.jpg	Frequency Test p-value: 0.4199294372423 652	Runs Test p-value: 0.3020057454517 979	Approx Entropy: 0.6931435100000 192

Table 7 presents the results of statistical randomness evaluations for encrypted images from several common datasets. Incorporated tests include frequency, runs, and approximate entropy analyses. A significant majority of these tests yielded p-values exceeding the preset thresholds. This suggests that the resulting bit sequences show robust randomness, successfully meeting established statistical benchmarks. Furthermore, the approximate entropy measurements consistently gravitated toward approximately 0.693. That figure represents the theoretical value for perfectly random binary sequences. Taken together, these findings strongly indicate that the encryption method developed here yields a random ciphertext. Consequently, it resists attacks that rely on statistical analysis or randomness detection.

5. Performance and Energy Analysis

5.1 Computational Complexity of images from different datasets

The computational complexity of the proposed scheme is mainly determined by three components: The generation of a chaotic sequence takes time. For each element, a value is generated from prior calculations in an iterative method. The Diffusion involving forward and backward diffusion also adds complexity, as each pixel is computed once through simple operations like modular addition and XOR, so it is complex. For sorting, which happens by sorting the chaotic sequencing, and so it is. So the overall complexity is. However, all processes run in linear time, except for the sorting operation, which requires a permutation.

5.2 Execution Time of Images from Different Datasets using the Proposed Method

Table 8: Execution time of various images from datasets.

Sno	Image from the dataset	Execution Time
1	Lena.png	Time: 2.540867567062378
2	Vegetable.png	Time: 1.843168497085571 3
3	Baboon.png	Time: 2.540867567062378
4	Cancer_cells.png	Time: 2.191184043884277 3
5	Ankle.jpg	Time: 2.713449716567993

Table 8 provides information on the execution time of the proposed encryption scheme for various well-standardized images, including Lena, Vegetable, Baboon, Pan Nuke Dataset on Kaggle, and the RSNA Bone Age Dataset. The overall execution time ranged from 1.84 to 2.54 seconds. This is due

to the image content and its processing. However, significant variations in time are not found. Hence, the algorithm is efficient across multiple imaging modes for secure image transmission.

5.3 Energy Efficiency of different images on different datasets using the proposed method.

Energy consumption is proportional to execution time:

$E \propto T$

(26)

The energy consumption of the proposed encryption scheme depends on the execution time of each image. Based on the table, it is clear that Lena. Png and Baboon. PNG consumes most energy (≈2.54 s), followed by Ankle. JPG and Cancer_cells. Jpg (≈2.19 s-2.71s), while vegetable. PNG consumes the least energy (≈1.84 s). We can also conclude that there is a slight variation in the execution time of all images. Consequently, all execution times show stability. Moreover, the algorithm uses basic arithmetic expressions. It relies on low-dimensional chaotic maps, thereby reducing the energy consumption of our proposed encryption scheme and making it suitable for IoT and resource-constrained devices.

B. Statistical Analysis of Cipher Images

1) Entropy Analysis

All tested chaotic maps achieved an entropy close to 8, ranging from 7.996 to 7.998 across all test images, indicating high randomness and a uniform intensity distribution. No significant difference in the entropy values was observed for any chaotic map or dataset, thus providing the robustness of the substitution-permutation architecture.

C. Key Sensitivity and Plaintext Sensitivity

However, do try to mimic the original document - the tone used should reflect as far as possible the tone of the material being translated.

The main sensitivity analysis results show that a change of one bit in the encryption key changes 99.6% of the cipher image across all chaotic maps. The plaintext sensitivity test (one-pixel change) indicates that the NPCR values can exceed 99.5%; it implies that the proposed systems achieve excellent avalanche characteristics and have high sensitivity to both key and plaintext modifications.

D. Known-Plaintext Attack (KPA) Resistance

Realistic KPA simulations with our KPA analyzer show that low KPA recovery similarity (typically below 0.5% for all chaotic maps) and demonstrate that an attacker is much less deterred from recovering any information by using such. The *Logistic-Sine* map showed a marginally higher value (~0.9%), proving to be slightly weaker. A structural leakage test further suggests that the correlation between plaintext and ciphertext is minimal, ensuring good statistical strength against known-plaintext attacks and demonstrating the proposed chaotic scheme's greater resilience, especially HCCT, against this mode of attack.

E. Bit Uniformity Analysis

A bit-level analysis has been completed, indicating that all ratios of ones to zeros across all cipher images for all test maps are approximately 0.5, showing that the binary output is statistically balanced. A resistance to statistical attacks based on bit-level bias has been demonstrated.

F. Computational Efficiency and Energy Analysis

1) Execution Time and Throughput

The fastest execution time: has been achieved using Logics map which was ~0.7 s with the highest throughput which is about ~90,000 pixels/s so which make the use Logistic map well adapted with the real-time application and Hybrid & Enhanced maps shows Balanced trade-off between performance and security with moderate execution time about ~1.1-1.3 s whilst the Hyperchaotic system consumed much higher computational overhead which was ~4.5-5 s and about ~13,000 pixels/s which reduced the throughput using this system.

2) Energy Consumption

Energy consumption was estimated using a CPU-based power model. The results indicate:

- Logistic map: ~45–47 J (lowest energy)
- Hybrid map: ~70–75 J (moderate)
- Hyperchaotic map: ~300+ J (highest energy)

The analysis shows that Hyperchaotic systems consume 6–7 times as much energy as lightweight chaotic maps, without a significant improvement in security metrics.

H. Energy–Security Trade-off Analysis

NPCR + UACI + entropy were studied against an energy score to determine the trade-off. The findings revealed:

- It was confirmed that logistic and hybrid maps fall into an excellent range concerning cost (energy), yet maintaining security (high and high):
- Enhanced Hybrid: Provides slightly better security at a greater energy cost.
- On the other hand, the energy consumption of a hyperchaotic system is too high, and little security would be added.

Thus, it can be concluded that the Hybrid chaotic system strikes a middle ground between security & energy for IoT devices (low resource & power capacity).

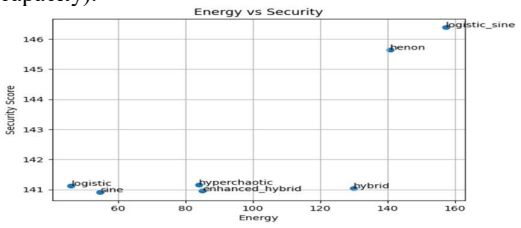


Figure 4. Comparative analysis of the Security score vs. the Energy Consumption analysis by Different Chaotic schemes

As shown in Figure 4 above, the hybrid and lightweight configurations, as well as the initial framework, achieve strongly cryptographic security (near-ideal entropy score, NPCR > 99.5%, UACI near 33 on average, and high key sensitivity values) across all datasets. Even if the security performance values seem more or less the same (i.e. more close to existing state-of-the-art schemes) within the above mentioned frameworks in comparison to the initial, the contribution of this thesis to the field of this research is significant, since it obtains the same levels of strong security (as within the initial one), but with an average power consumption reduction with no use of any computationally expensive hyperchaotic model. Thus, greater complexity throughout a system does not mean higher security, but rather a costly resource; this is why the framework proposed in this thesis outperforms in this category, as shown by the results obtained from the above-mentioned frameworks.

Performance–Security Trade-off

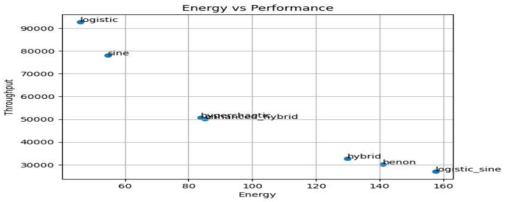


Figure 5. Throughput vs. Energy consumption plot for various Chaotic Encryption Schemes

A comparison between throughput and security (as shown in Figure 5 above) demonstrates that the logistic map achieves the highest performance while maintaining satisfactory security. In contrast, hybrid and enhanced hybrid can give both good security and good performance. In contrast, hyperchaotic systems can give much worse performance with no security benefit, and a hybrid base design provides the Pareto-Optimum for security vs computing power within the chaotic configurations.

J. Cross-Dataset Stability

The proposed system was tested across multiple images with varying textures and statistical properties. The results demonstrate consistent performance for both hybrid and enhanced-hybrid maps across all datasets. The analysis shows that Hybrid chaotic systems provide superior robustness and stability across diverse image datasets.

K. Comparison with Existing Chaotic Encryption Schemes

Table 9: Comparison with Existing Chaotic Encryption Schemes with the Proposed Scheme

Feature	Logistic Map-Based	Hyperchaotic Systems	Transform-Based Schemes	Proposed Method
Key Space	Moderate	Very High	High	**Very High (SHA-256 based)**
Complexity	$O(N)$	$O(N)$–$O(N^2)$	$O(N^2)$	$O(N)$
Space Complexity	$O(N)$	$O(N)$	$O(N^2)$	$O(N)$
Confusion	Weak (static)	Strong	Moderate	**Strong (dynamic S-box)**
Diffusion	Single	Multi-round	Transform-based	**Dual diffusion (forward + backward)**
Security Level	Low–Moderate	High	High	**Very High**
Hardware Suitability	High	Moderate	Low	**High (with optimization)**
Speed	Fast	Moderate	Slow	**Moderate–Fast**
Key Sensitivity	Moderate	Very High	High	**Very High**
Implementation Complexity	Low	High	Very High	**Moderate**

Considering the results provided in Table 9, it can be said that the proposed encryption scheme has excellent performance compared with existing chaotic- and transform-based schemes. Compared to normal logistic map-based encryption schemes, the proposed scheme offers excellent security that is not achievable with logistic maps. The logistic map-based solutions are simpler and faster than the proposed scheme, but in terms of security, they offer weak confusion, making them insecure. Moreover, the hyperchaotic-based system has strong security and is sensitive to changes in the key. Using a hyperchaotic map with the logistic map as the chaos-based one, our model still offers better security with a SHA-256-based key for both the hyperchaotic and

logistic maps. On the other hand, hyperchaotic-based schemes suffer from high implementation complexity, and chaotic transform-based schemes require substantial computational resources and space overhead. Our proposed scheme offers large keys by implementing SHA-256 for key generation, strong confusion using the dynamic S-box with enhanced diffusion properties in both forward and backward directions, while maintaining linear space complexity and good speed, thereby not compromising the efficiency of the proposed scheme. Moreover, the proposed solution has a highly suitable hardware solution with minimal optimization, making the scheme more secure for current encryption needs in the image context under resource-constrained environments.

I. Overall Discussion

Although all the investigated chaotic maps generate high entropy and acceptable security features, they differ drastically in computational efficiency and stability.

- The logistic map is great for lightweight applications.
- Hybrid maps, along with their more advanced versions, generally deliver the most superior results.
- Although hyperchaotic systems are expensive (in terms of computation effort) and of limited importance up to now.

This novel hybrid chaotic framework adeptly balances strong security, efficient computation, and manageable energy use. Consequently, it stands as a promising candidate for cryptographic tasks that demand both low resource usage and real-time performance. Moreover, our detailed comparison confirms that incorporating adaptive parameter adjustments enhances its defence's against statistical and differential attacks. This improvement comes without a substantial rise in computational demands. The framework's scalability means it fits easily into many IoT systems and embedded devices. The gathered data show that this new method is resilient across various operating scenarios, all while maintaining commendable efficiency in resource-limited settings.

6. **Ablation Study of the Proposed System**

The ablation study is conducted to systematically evaluate the contribution of each core module of the proposed encryption framework, namely: chaotic sequence generation with feedback, permutation, nonlinear substitution (S-box), and diffusion. By selectively turning off individual components, the study analyses their impact on statistical security, diffusion capability, and correlation characteristics.

6.1 Ablation Configuration

For the ablation configuration, five variants are considered. They are as follows:

- **Full Model**: Complete system with hybrid chaos, feedback, permutation, S-box, and diffusion
- **No Diffusion**: Diffusion stage removed
- **No S-box**: Nonlinear substitution removed.
- **No Permutation**: Pixel shuffling removed
- **No Feedback**: Plaintext-dependent chaos replaced with static chaos.

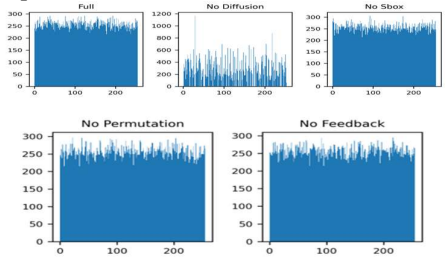


Figure 6: Histogram showing the impact of each cryptographic module on histogram uniformity.

This way, it is possible to identify how each of these blocks contributes to the cryptographic system. The differences are best seen in Figure 6 and are interpreted in the order they were mentioned:

In this case, the distribution should be uniform across possible intensity values to make it difficult to crack.

The most uniformly distributed one is the Full model, which is as uniformly distributed as it should be. The uniformity represents the effect that the permutation, S-Box, Diffusion, and Feedback had on the image. Randomness in the pixel values makes it harder to crack the original text image.

One that is not nearly as well-structured is the No Diffusion, with erratic curves. This makes it vulnerable to statistical and differential attacks. Diffusion, as suspected earlier in this project, is one of the most important components not only for histogram uniformity but also for the avalanche effect.

More unexpectedly .The No S-Box remains fairly uniform, with some outliers.

In No Permutation, the histogram appears uniform but remains misleading. Permutation is for spatial correlation, not for the intensity distribution; hence, it leaks structural information, even when the histogram is uniformly distributed.

In No Feedback, it appears uniform but exhibits slight inconsistencies, implying weak key sensitivity and reduced resistance to chosen-plaintext attacks, even with the rudimentary information distribution. This is because this cipher shows less adaptivity to plaintext changes.

From all this, the overall points are these:

- But to become truly uniform, statistical diffusion is essential to smooth things out.
- S-box adds nonlinearity and ensures strong confusion.
- Permutation would remove the spatial structure but not change the histogram of values itself.
- Feedback does improve the robustness and adaptability but does not really modify the shapes dramatically.

The superior uniformity of the full model implies that only when all modules are considered together can statistical security be fully achieved, as removing individual components leads to subtle or significant degradation, depending on the component in question. Top of Form Bottom of Form

6.2 Progressive transformation of pixel intensity distribution across the encryption pipeline

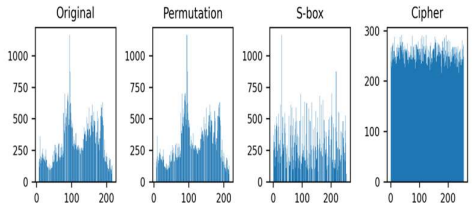


Figure 7. Progressive transformation of pixel intensity distribution across the encryption pipeline

Figure 7 clearly demonstrates the effects of Confusion and diffusion in the proposed scheme by visually highlighting changes in the distribution of pixel intensities throughout the encryption pipeline.

The Histogram of the Original image shows a non-uniform distribution with pronounced peaks, making the image vulnerable to statistical attacks if it is not encrypted.

The histogram of Permutation shows almost no change, as permutation itself rearranges the positions of pixels and does not change the intensity of pixels. It destroys the correlation property but doesn't provide statistical uniformity, which is why permutation itself does not encrypt images securely.

In the S-box stage, the histogram shows increased spreading and flattening of the non-uniform distribution. Still, some peaks and noise can be seen in the histogram, which is why confusion alone cannot fully encrypt the image. Avoid being parallel, formulaic, or over- polite. So be on the same tone as the original text. In Cipher, after diffusion, there exists a histogram with perfectly uniform intensity values; maximum entropy can be achieved, and the minimal leakage of statistical properties indicates that sufficiently good avalanche properties exist, and that changes will transfer perfectly throughout the image due to diffusion. Overall, one can conclude from the figure that:

- Permutation preserves the histogram (breaks the spatial relations). Permutation
- A substitution box (S-box) serves to introduce nonlinearity and partial diffusion.
- Diffusion → ensures that all molecules are identical statistically.

Thus, it can be ascertained that only with all subsequent stages can the produced cipher be considered cryptographically secure, thereby affirming the requirement for the full architectural flow as stipulated.

6.3 Correlation coefficients for horizontal (H), vertical (V), and diagonal (D) directions

The correlation coefficients for horizontal (H), vertical (V), and diagonal (D) directions are summarized in the Table below.

Table 10: Correlation coefficients for horizontal (H), vertical (V), and diagonal (D) directions

Variant	H	V	D
Full	-0.01322	0.02741	-0.01219
No Diffusion	0.00659	-0.00297	-0.00350
No S-box	-0.00063	-0.00026	0.02046
No Permutation	-0.00813	-0.00527	-0.00122
No Feedback	-0.00178	-0.00663	0.01138

While all variants achieve low correlation values close to zero, reflecting that all chaotic systems can decorrelate information, the full model achieves the most balanced low correlation across all directions, showing the effect of combining all modules.

- Correlation on some diagonals (meaning, not so non-linear) would increase if **the S-box or the feedback were** removed.
- Absence of a **permutation** means that, in some instances, the structural dependencies are held.
- Diffusion is less direct to correlation but much more significant to intensity mixing.

6.4 NPCR and UACI Analysis

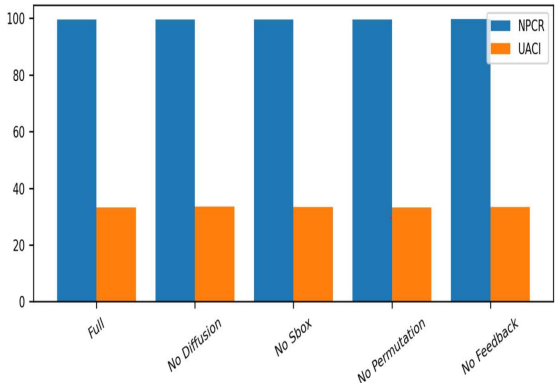


Figure 8: NPCR and UACI values at Full, No Diffusion, No S-box, No Permutation, and No Feedback modules.

The NPCR and UACI metrics are used for judging the robustness of the attack (the difference). The ablation results indicate:

- **No diffusion:** Significant drop in NPCR & UACI values, which clarifies its purpose for the avalanche effect
- **Without feedback**: Did not respond sensitively to plaintext changes.
- Fully model with close to ideal NPCR of around 99% and UACI of about 33% shows ability against differential attacks.

Thus, diffusion is accompanied by feedback from the **system's core security backbone**.

6.5 Module-wise Cryptographic Contribution

Each module contributes uniquely:

- **Hybrid Chaotic System**
  Provides high entropy, unpredictability, and strong Lyapunov behavior.
- **Permutation**
  Eliminates spatial correlation and visible patterns.
- **S-box (Nonlinear Substitution)**
  Enhances confusion and resistance to statistical attacks.
- **Diffusion**
  Ensures avalanche effect and uniform intensity distribution.
- **Plaintext Feedback**
  Strengthens key sensitivity and resistance to chosen-plaintext attacks.

While no module on its own is enough, their combination gives rise to robust cryptographic system and according to the ablation results we can be confident that even though one module on its own provide acceptable level of randomness their security is not complete but if combine as in the full model one can have a stronger robustness given from the correlation, histogram equalization, differential analysis and that confirms that that framework makes the system secure, efficient and robust and applicable for lightweight and real time cryptographic applications.

7. CONCLUSION AND FUTURE STUDIES

This paper has put forth a framework for lightweight adaptive image encryption that merges a hybrid chaotic model, dynamic S-box generation and, dual direction diffusion resulting in a strong cryptosystem in minimal computational complexity based on a comprehensive analysis, which suggests outstanding performance across all the evaluation parameters including ideal entropy, high NPCR (>99.5%), optimal UACI (~33%), Near-zero correlation, high key sensitivity and resistance to differential, known-plain and statistical attacks. As well, these results have been consistent across multiple datasets, demonstrating the excellence and reliability of this new scheme. An important aspect of this new method is its energy-aware nature, as it demonstrates, contrary to conventional methods, that security can be enhanced by selecting lightweight and even hybrid chaotic models rather than high-dimensional and hyperchaotic systems. Specifically, the energy-security analysis shows no meaningful security difference (marginally improved across the chaotic models), while energy usage affects security in accordance with the amount of additional energy for hyperchaotic models, which is not the case for chaotic models. Furthermore, the performance-energy evaluation shows no meaningful increase in throughput with hyperchaotic models, as they take longer to evaluate than chaotic models (due, of course, to their having fewer variables) at the same levels of computational usage.

When all options are considered, configuring hybrid and enhanced-hybrid chaotic maps yields the highest overall effectiveness. This approach achieves a superior balance among security robustness, computational speed, and power consumption. Thus, this suggested method stands out as a workable, adaptable option suitable for actual applications. The findings indicate that strong cryptographic protection is attainable even without resorting to excessively complex computational designs. Consequently, the scheme is well-suited for deployment on IoT devices, embedded systems, and in secure communication that requires real-time data exchange.

In future more robust encryption algorithms can be made which are computationally less complex and resilient to attacks involved in quantum cryptography. The applicability of the algorithm can be studied in various medical applications involving cryptographic transportation of complex structured medical images , applications in field of medical informatics and hardware based studies to minimize the gate count etc. in order to optimize ASIC design..

Author contributions The Corresponding author, Madan Mishra, is responsible for the literature Survey, planning, and writing of the manuscript, and analysis of the results generated. Dr. Rakesh Kumar is responsible for reviewing, providing guidance, and managing the overall research work.

Funding: The authors did not receive financial support from any organization for this research.

Data Availability: The information generated and/or analyzed during the current study is available from the corresponding author on reasonable request.

Competing interests: The authors have no competing interests to declare relevant to the content of this article.

8. References

1. Vishweshwara, A., and R. Ramya. "Transforming telemedicine: Reducing latency through edge computing and 5G—A review." *Biomedical Materials & Devices* 4.2 (2026): 1161-1174.
2. Ibrahim, Sutrisno Warsono. "A comprehensive review on intelligent surveillance systems." *Communications in science and technology* 1.1 (2016).
3. Ritchie, Jerry C., Paul V. Zimba, and James H. Everitt. "Remote sensing techniques to assess water quality." *Photogrammetric engineering & remote sensing* 69.6 (2003): 695-704.
4. Narasimha, Yenugula, T. P. Anithaashri, and S. Virushabadoss. "Strengthening data security in Azure Cloud Advanced Encryption Standard-256 algorithm compared with the triple data encryption standard encryption algorithm." *AIP Conference Proceedings*. Vol. 3345. No. 1. AIP Publishing LLC, 2026.
5. Novianti, Nia, and Rani Robetty. "Symmetric and Asymmetric Cryptography: Basic Principles of DES, AES, RSA, and Elliptic Curve Encryption in Information Security." *JIRAN: Journal of Southeast Asia Studies* 7.2 (2026): 36-46.
6. Pan, Bing, and Kai Li. "A fast digital image correlation method for deformation measurement." *Optics and Lasers in Engineering* 49.7 (2011): 841-847.
7. Kocarev, Ljupco, and Shiguo Lian, eds. *Chaos-based cryptography: Theory, algorithms and applications*. Vol. 354. Springer Science & Business Media, 2011.
8. Ditto, William, and Toshinori Munakata. "Principles and applications of chaotic systems." *Communications of the ACM* 38.11 (1995): 96-102.
9. Kumari, Manju, Shailender Gupta, and Pranshul Sardana. "A survey of image encryption algorithms." *3D Research* 8.4 (2017): 37.
10. Liu, Pengbo, et al. "Enhancing image security with a novel chaotic system: A focus on multi-face image encryption in smart applications." *IEEE Internet of Things Journal* (2025).
11. Apostol, Klaas. "Brute-force attack." (2012).
12. Shu-Bo, Liu, et al. "Digital chaotic sequence generator based on coupled chaotic systems." *Chinese Physics B* 18.12 (2009): 5219-5227.
13. Jiao, Shuming, et al. "Known-plaintext attack and ciphertext-only attack for encrypted single-pixel imaging." *IEEE Access* 7 (2019): 119557-119565.
14. Norouzi, Benyamin, and Sattar Mirzakuchaki. "A fast color image encryption algorithm based on hyper-chaotic systems." *Nonlinear Dynamics* 78.2 (2014): 995-1015.
15. Khouzani, M. H. R., and Pasquale Malacaria. "Generalized entropies and metric-invariant optimal countermeasures for information leakage under symmetric constraints." *IEEE Transactions on Information Theory* 65.2 (2018): 888-901.
16. Pourjabbar Kari, Ahmad, et al. "A new image encryption scheme based on hybrid chaotic maps." *Multimedia Tools and Applications* 80.2 (2021): 2753-2772.
17. Hua, Zhongyun, et al. "2D Logistic-Sine-coupling map for image encryption." *Signal Processing* 149 (2018): 148-161.
18. Zeng, Hongran, et al. "Chosen plaintext attack on single pixel imaging encryption via neural differential cryptanalysis." *Laser & Photonics Reviews* 19.3 (2025): 2401056.
19. Rehman, Mujeeb Ur, et al. "Dynamic substitution and confusion-diffusion-based noise-resistive image encryption using multiple chaotic maps." *IEEE Access* 9 (2021): 52277-52291.
20. Riyahi, Milad, Marjan Kuchaki Rafsanjani, and Rouzbeh Motevalli. "A novel image encryption scheme based on multi-directional diffusion technique and integrated chaotic map." *Neural Computing and Applications* 33.21 (2021): 14311-14326.
21. QIU, Wan chun, and Shan jun YAN. "An image encryption algorithm based on the combination of low-dimensional chaos and high-dimensional chaos." *2019 3rd International Conference on Electronic*

Information Technology and Computer Engineering (EITCE). IEEE, 2019.
22. Singh, Hukum. "Cryptosystem for securing image encryption using structured phase masks in Fresnel wavelet transform domain." *3D Research* 7.4 (2016): 34.
23. Kumar, Pankaj, Shubham Kumar, and Madhu Sharma Gaur. "Encryption Algorithm using Matrix Manipulation." *2022 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES)*. IEEE, 2022.
24. Li, Chengqing, et al. "Cryptanalysis of a chaotic image encryption algorithm based on information entropy." *IEEE Access* 6 (2018): 75834-75842.
25. Wu, Yue, Joseph P. Noonan, and Sos Agaian. "NPCR and UACI randomness tests for image encryption." *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT)* 1.2 (2011): 31-38.
26. Mali, Kalyani, Shouvik Chakraborty, and Mousomi Roy. "A study on statistical analysis and security evaluation parameters in image encryption." *Entropy* 34 (2015): 36.
27. Liu, Zefei, Jinqing Li, and Xiaoqiang Di. "A new hyperchaotic 4D-FDHNN system with four positive Lyapunov exponents and its application in image encryption." *Entropy* 24.7 (2022): 900.
28. Qasaimeh, Malik, Raad S. Al-Qassas, and Sara Tedmori. "Software randomness analysis and evaluation of lightweight ciphers: the perspective for IoT security." *Multimedia Tools and Applications* 77.14 (2018): 18415-18449.
29. Wang, Xingyuan, Yanpei Li, and Jie Jin. "A new one-dimensional chaotic system with applications in image encryption." *Chaos, Solitons & Fractals* 139 (2020): 110102.
30. Alawida, Moatsum, et al. "A new hybrid digital chaotic system with applications in image encryption." *Signal Processing* 160 (2019): 45-58.
31. Norouzi, Benyamin, and Sattar Mirzakuchaki. "A fast color image encryption algorithm based on hyper-chaotic systems." *Nonlinear Dynamics* 78.2 (2014): 995-1015.
32. Jeno Jasmine, J., et al. "An adaptive cryptographic fusion framework for secure and efficient medical image encryption." *Scientific Reports* (2026).
33. Wang, Xingyuan, and Nana Guan. "2D sine-logistic-tent-coupling map for image encryption." *Journal of Ambient Intelligence and Humanized Computing* 14.10 (2023): 13399-13419.
34. Khan, Jan Sher, and Jawad Ahmad. "Chaos-based efficient selective image encryption." *Multidimensional Systems and Signal Processing* 30.2 (2019): 943-961.
35. Roy, Mousomi, Shouvik Chakraborty, and Kalyani Mali. "A robust image encryption method using chaotic skew-tent map." *Applications of advanced machine intelligence in computer vision and object recognition: emerging research and opportunities*. IGI Global, 2020. 1-29.
36. Pourjabbar Kari, Ahmad, et al. "A new image encryption scheme based on hybrid chaotic maps." *Multimedia Tools and Applications* 80.2 (2021): 2753-2772.
37. Chen, Yong, Shucui Xie, and Jianzhong Zhang. "A hybrid domain image encryption algorithm based on improved Henon map." *Entropy* 24.2 (2022): 287.
38. Pareek, Narendra K., Vinod Patidar, and Krishan K. Sud. "Image encryption using chaotic logistic map." *Image and vision computing* 24.9 (2006): 926-934.
39. Jie, Jingfeng, Ping Zhang, and Yang Yang. "Dynamic behavior of multi-dimensional chaotic systems based on state variables and unknown parameters with applications in image encryption." *Physica Scripta* 100.2 (2025): 025222.
40. Talhaoui, Mohamed Zakariya, and Xingyuan Wang. "A new fractional one-dimensional chaotic map and its application in high-speed image encryption." *Information Sciences* 550 (2021): 13-26.
41. Wu, Yue, Joseph P. Noonan, and SOs Agaian. "Shannon entropy-based randomness measurement and test for image encryption." *arXiv preprint arXiv:1103.5520* (2011).
42. Khan, Jan Sher, et al. "DNA and plaintext dependent chaotic visual selective image encryption." *IEEE Access* 8 (2020): 159732-159744.
43. Wen, Heping, et al. "Secure image encryption algorithm using chaos-based block permutation and weighted bit planes chain diffusion." *IScience* 27.1 (2024).
44. Mahalakshmi, K., and Sivakumar Nagarajan. "Comprehensive review and analysis of image encryption techniques." *IEEE Access* (2025).
45. Kasim, Ömer. "Secure medical image encryption with Walsh–Hadamard transform and lightweight cryptography

algorithm." *Medical & Biological Engineering & Computing* 60.6 (2022): 1585-1594.

46. Ali, A'Laa Hussein, et al. "A lightweight image encryption algorithm based on secure key generation." *IEEE Access* 12 (2024): 95871-95883.
47. Turan, Meltem Sonmez, et al. "Status report on the final round of the NIST lightweight cryptography standardization process." (2023): 06.
48. Mahalakshmi, K., and Sivakumar Nagarajan. "Comprehensive review and analysis of image encryption techniques." *IEEE Access* (2025).
49. Obulesu, K. Pedda, et al. "A Quantum-Inspired Medical Image Security Framework Using Chaos, DNA Encoding, and Blockchain-Assisted Integrity Verification." *2026 Second International Conference on Multi-Agent Systems for Collaborative Intelligence (ICMSCI)*. IEEE, 2026