Bol. Soc. Paran. Mat.
©SPM – E-ISSN-2175-1188
SPM: www.spm.uem.br/bspm

(3s.) **v. 2025 (43) 1** : 1–33.
ISSN-0037-8712

Securing Images with Chaotic Map and Matrix Based Encryption

Shalini Gupta*, Kritika Gupta, Nitish, Praveen Agarwal and Shilpi Jain

ABSTRACT: This paper presents a novel grayscale image encryption scheme that combines a high-dimensional chaotic map with a Suslin matrix-based diffusion process to achieve robust security and high computational efficiency. In the proposed method, a Hybrid Sinusoidal-Logistic-Chaotic (HSLC) map is employed to generate a pseudo-random sequence used for pixel permutation, thereby effectively disrupting spatial correlations in the plain image. Concurrently, a Suslin matrix is constructed based on parameters derived from a shared secret key, which is then used to perform block-wise diffusion on the permuted image. The diffusion process operates on non-overlapping 4×4 pixel blocks, ensuring that even minor changes in the plain image propagate widely in the cipher image. Security analysis, including evaluations of Shannon entropy, correlation coefficients, NPCR, UACI, and PSNR under noise attacks, demonstrates that the encrypted images exhibit high randomness, strong differential resistance, and low pixel correlation. Experimental results confirm that the proposed scheme is effective in securing images for real-time multimedia applications.

Key Words: Chaotic map, elliptic curve cryptography, image encryption, secret key, Suslin matrix, authentication, data.

Contents

* Corresponding author.
2020 *Mathematics Subject Classification:* 12E20, 94A60.

1. Introduction

In recent years, the proliferation of digital technologies has led to an unprecedented increase in the generation, sharing, and storage of visual data across numerous domains. From medical imaging systems that aid in diagnostics to surveillance cameras that enhance public safety, digital images play a pivotal role in modern society. Additionally, multimedia applications, social media platforms, and digital communication tools now heavily depend on images to convey information effectively and engagingly. However, as the volume of digital images grows, so does the potential for security vulnerabilities. Images transmitted over networks or stored on cloud platforms are at risk of unauthorized access, which could compromise sensitive data or expose individual's privacy. This environment highlights the need for specialized security measures designed to protect image data from potential threats, ensuring the integrity and confidentiality of images used in critical applications.

Digital images are represented as grids of pixel values, where each pixel encodes intensity information for grayscale images or color information for color images. These pixel-based structures form the foundation of digital visual data used across a range of fields, including healthcare, surveillance, digital communications, and multimedia applications, see [23], [41]. While traditional encryption techniques, such as symmetric and asymmetric cryptography, are effective for text and other low-dimensional data, they often face limitations when applied to image data. Direct application of conventional encryption methods can lead to inefficiencies and insufficient protectiondue to image's large file sizes, high redundancy, and specific structural characteristics. In response, specialized image encryption methods have been developed to accommodate the

Submitted September 30, 2025. Published December 19, 2025

unique properties of visual data, with a focus on ensuring both security and computational efficiency, see Therefore, several image encryption schemes have been provided by the researchers, see [4], [7], [12], [43], [54], [13].

The scope of research in image encryption is broad, encompassing a variety of techniques to address the specific challenges posed by digital images. Researchers have explored methods such as symmetric key algorithms, public-key encryption, chaos-based systems, and hybrid models that combine multiple techniques for enhanced security. Additionally, image encryption research frequently examines factors such as the preservation of image quality, computational performance, and resilience against common forms of attack (e.g., statistical, differential, and chosen-plaintext attacks).

Chaotic systems exhibit properties such as sensitivity to initial conditions, ergodicity, and inherent randomness, which can be exploited to achieve robust encryption. However, many of the conventional chaotic maps used in image encryption are one-dimensional and suffer from limited key spaces, short periodic windows, and linear predictability. Such limitations make them vulnerable to brute-force and differential attacks, reducing the overall security of the encryption scheme.

In response to these challenges, this paper introduces a novel image encryption scheme that integrates a high-dimensional chaotic map with a Suslin matrix-based diffusion mechanism. The proposed scheme leverages a HSLC map that operates in three dimensions, thereby expanding the key space and enhancing randomness. This chaotic map is designed to generate a highly unpredictable sequence for pixel permutation, effectively disrupting the spatial correlation of the image. To further reinforce security, the scheme employs a Suslin matrix-a structured, invertible matrix whose parameters are securely derived from a shared secret key. The Suslin matrix is used to perform diffusion on 4×4 blocks of the permuted image, ensuring that any small change in the original image propagates across the entire cipher image. Notably, the encryption parameters (both for the chaotic map and the Suslin matrix) are derived solely from a shared secret, allowing both the sender and receiver to independently compute identical keys without explicit exchange, thus reducing the risk of key interception.

This dual-stage approach - combining chaotic permutation (confusion) and Suslin matrix-based diffusion (substitution) - addresses the shortcomings of traditional methods by ensuring that the resulting encrypted image is statistically indistinguishable from noise. The encrypted image demonstrates high entropy, low correlation among adjacent pixels, and strong differential properties, as evidenced by metrics such as NPCR and UACI. Moreover, extensive analysis has shown that the proposed scheme is computationally efficient, making it suitable for real-time applications in multimedia systems.

The main objectives of the proposed image encryption scheme are as follows:

- **Generation of a Novel Chaotic Map:** Develop a new high-dimensional chaotic map that exhibits superior sensitivity to initial conditions, enhanced randomness, and an expanded key space compared to conventional one-dimensional chaotic maps.

- **Enhanced Confusion and Diffusion:** Achieve robust encryption by integrating chaotic permutation (confusion) with a Suslin matrix-based diffusion process, ensuring that both pixel positions and values are thoroughly scrambled.

- **Secure Key Synchronization:** Derive all necessary encryption parameters—including chaotic initial conditions and Suslin matrix parameters - directly from a shared secret key, so that both sender and receiver can independently generate identical keys without explicit transmission.

- **Resistance to Cryptanalytic Attacks:** Ensure that the encrypted images exhibit high Shannon entropy, negligible correlation among adjacent pixels, and strong differential resistance (high NPCR and UACI), thereby mitigating statistical and differential attacks.
- **Computational Efficiency for Real-Time Applications:** Design the encryption and decryption processes to be computationally efficient and fast, making the scheme suitable for real-time secure image transmission in multimedia systems.
- **Robustness Against Noise:** Provide resilience to various noise attacks, such as salt-and-pepper and Gaussian noise, ensuring that decryption remains effective even under adverse conditions.

Organization of Paper:
The rest of the paper is structured into six sections. Section 2 gives the review of litrature. Section 3 discusses the essential preliminaries crucial for understanding the paper. In Section 4, we highlight our proposed hybrid chaotic map. Section 5 gives the security analysis of the proposed chaotic map. Section 6 highlights the proposed image encryption scheme. Section 7 gives the architecture and working of the proposed scheme. Section 8 highlights the visual results. Section 9 gives the experimental and security analysis of proposed scheme. Section 10 compares the proposed with existing schemes. Further, Section 11 concludes the results.

2. Literature Review

Elliptic Curve Cryptography (ECC) has emerged as a highly promising replacement for conventional cryptographic systems. Miller [30] introduced ECC and devised a cryptosystem that operates 20 times faster than the Diffie-Hellman algorithm. Additionally, Koblitz [23] introduced an ECC-based cryptosystem operating over a finite field. The security of this cryptosystem depends on the assumed difficulty of solving the discrete logarithm problem on elliptic curves. Currently, there doesnot exist any sub-exponential algorithm for solving this problem over finite fields. Therefore, ECC allows for smaller field sizes, keys, and parameters compared to other public key systems like Rivest–Shamir–Adleman (RSA) while maintaining equivalent security levels. This feature is particularly advantageous in applications where memory and computational resources are constrained.
ECC is renowned for its computational speed and robust security. In the modern era, safeguarding the secure transmission of digital images has become absolutely essential. Hosny et al. [20] and Zia et al. [55] conducted a detailed survey of encryption methods aimed at safeguarding security and privacy for digital multimedia, encompassing images, videos and audio. They provided a detailed summary of the existing secure image encryption techniques. This knowledge will further contribute to the development of more efficient and secure encryption solutions in the future.
Researchers have proposed numerous techniques for digital image encryption, including chaotic-based methods (e.g., [21], [25],[28], [35],[45], [48], [52]), elliptic curve-based approaches (e.g., [8], [17], [25], [37], [40]), cellular automata-based techniques (e.g., [11], [51]), DNA-based methods (e.g. [28], [48], [54]). Singh and Singh [40], proposed an authenticated image encryption scheme using elliptic curve cryptography which provides confidentiality along with authentication. But during encryption they added additional pixels which led to the issue of expansion of cipher data. Singh and Singh [41] refined the earlier scheme by preventing the expansion of cipher data by using modified ElGamal encryption and 2D Arnold Cat Map. Abd El-Latif and Niu [1], proposed an image encryption scheme using ECC and hybrid chaotic system. They generated initial key stream using chaotic system and an external key stream in feedback manner. Then, the authors derived the key sequences from the points of elliptic curve and mixed them with the generated

key stream. This hybrid encryption method faces limitations in computational intensity due to the complex processes involved in key generation and sequence handling, which can restrict its use in real-time on devices with limited power. Parida et al. [36] provided an image encryption and authentication scheme using ECC. The authors explored the use of 3D and 4D Arnold cat map to scramble the values of plain image pixels. However, the extended mapping dimensions, while enhancing security, can lead to slower encryption speeds due to the intensive processing requirements for transforming image pixels.

There are mainly two methods to encrypt images, one is chaos-based selective or non selective method and the other is non-chaos based selective method. Researchers have extensively explored chaotic maps due to their potential in encryption algorithms. Gong et al. [15] introduced a chaotic system in four dimensions featuring hidden attractors. This innovation results in the development of an image encryption method that is resilient against both statistical and differential attacks. Gong et al. [16] also presented a new dynamic chaotic system that produces varied chaotic features including coexistence attractors and hidden attractors. Zhu et al. [53] provided an encryption scheme by scrambling the pixels of the plain image and then added watermark to the scrambled image. Further, they encrypted the scrambled image to get the ciphered image.

Neamah A. A. [33] presents a novel approach that utilizes a seven-dimensional hyperchaotic system in conjunction with Pascal's matrix for image encryption. This method effectively integrates these two components, yielding a robust security framework. The seven-dimensional hyperchaotic system is employed to generate the private key needed for scrambling the image, with the initial conditions of the system specifically tailored to the original image's characteristics. The proposed key size is sufficiently large to resist brute-force attacks. Furthermore, this encryption technique exhibits strong resilience against various types of attacks. Experimental results and evaluations of the algorithm demonstrate its high efficacy in encrypting grayscale images, providing both strong security and efficient performance. However, the complexity of the algorithm may lead to significant computational demands, potentially limiting its usability in environments with constrained processing capabilities. Aldin et al. [3] introduces a new algorithm that incorporates fusion, segmentation, random assembly, hyperchaotic processes, and the Fibonacci Q-matrix (FQ-matrix). A unique fusion technique proposed to merge four color images into four distinct sequences based on their informational content. Each of the resulting four images is then divided into four segments, which are randomly assembled into a single image using a random key. This combined image is subsequently scrambled using a six-dimensional hyperchaotic system and further diffused via the FQ-matrix. The performance and robustness of the proposed algorithm have been evaluated through various tests, demonstrating its strong effectiveness in securing image transmissions. However, limitations include potential vulnerabilities to certain attack types due to the complexity of its operations.

Chaker et al. [10] proposed a new image encryption and decryption system that features an algorithm with two primary stages. In the initial stage, a seven-dimensional Lorenz-like hyperchaotic system generates random numbers that are used to alter pixel positions. In the second stage, the image is divided into 8×8 blocks, each of which is diffused for the first time using the Fibonacci matrix. Asani et al. [6] proposed an encryption scheme based on logistic map and Latin square matrix. Logistic map mapping is a powerful chaotic system that encrypts with high unpredictability, greatly lowering the likelihood of decryption. Similarly, the Latin square matrix enhances encryption strength through its consistent histogram distribution. The integration of these algorithms in this study is thus based on the scientific aim of creating a robust and resilient cipher method. Sharma et al. [37] introduces an image encryption scheme for grayscale and color images based on a primitive polynomial combined with the transformation of pixel values into a finite field, leading to pixel permutation. Following this, the shuffled pixels undergo further diffusion using a specially constructed matrix. To strengthen security, the scheme

also integrates a logistic chaotic map. The effectiveness of the encryption heavily depends on the selection of appropriate parameters for the primitive polynomial and the finite field, which may not be straightforward. Kumar and Sharma [25] presents an innovative image encryption method that integrates a chaotic map, elliptic curve cryptography, and a genetic algorithm to boost security. They used Arnold's cat map to introduce chaos and randomness by shuffling pixel positions. Further, encrypts the pixel values using elliptic curve cryptography . Additionally, a genetic algorithm is applied to optimize key generation, further enhancing the encryption scheme's security. The combination of these techniques aims to provide strong confidentiality and resilience in image encryption.

Cesarano et al. [57] developed a new class of Bessel-type functions using the monomiality principle and Laguerre-type exponentials, with possible multivariable extensions discussed. Ramírez et al. [56] generalized algebraic relations and recurrence formulas connecting degenerated Apostol-Bernoulli, Apostol-Euler, and Apostol-Genocchi polynomials with other polynomial families were established. Ramírez and Cesarano [58] studied new classes of these degenerated generalized polynomials of order α and level m, and their explicit forms, recurrences, and identities were derived via generating functions.

Matrix theory plays a vital role in image encryption. Amounas and Kinani [5] proposed a novel technique to encrypt images using involutory matrix and ECC to map the pixels to points on an elliptic curve. While efficient in mapping pixels to elliptic curve points, this method faces challenges with complex key generation and may be vulnerable to certain differential attacks if the mapping is not robustly managed. Nagaraj et al. [32] provided an encryption scheme which uses magic matrix operations along with ECC to encrypt an image. This method has limited key space due to the matrix size used, potentially reducing resistance to brute-force attacks. Obaidand and Al Saffar [34] in 2021, proposed an encryption scheme based on ECC and Hilbert matrix. However, Hilbert matrices may not always be invertible, complicating decryption if specific matrix configurations are used, which can lead to challenges in real-time applications. Hosny et al. [19] presented a new algorithm for image encryption using a hyperchaotic system and Fibonacci Q-matrix. This hyperchaotic system provides high encryption strength but can be computationally intensive, making it less suited for environments with limited processing power. Additionally, the complex parameter requirements of chaotic systems could increase vulnerability to parameter estimation attacks if not handled with care. In matrix based encryption schemes, the matrix involved must be invertible to carry out decryption. Suslin constructed a new matrix called Suslin matrix whose properties are studied by various researchers, see [22].

In the present paper, we address the limitations observed in the existing image encryption schemes by proposing a novel approach that integrates a high-dimensional chaotic map with a Suslin matrix-based diffusion mechanism. Unlike traditional methods that rely on lower-dimensional chaos or fixed transformation matrices, our approach leverages the HSLC map to generate highly unpredictable sequences, ensuring stronger security. Additionally, the use of the Suslin matrix provides an efficient and reversible diffusion operation that enhances resistance against statistical and differential attacks. By combining these techniques, our scheme achieves a higher level of randomness, improved key sensitivity, and robustness against cryptanalytic attacks, making it a promising solution for secure image transmission. The following sections provide a detailed discussion of the proposed encryption scheme, its implementation, and its security evaluation.

3. Preliminaries

In this section, we provide an overview of the foundational concepts laying the groundwork for the subsequent detailed exploration of our proposed approach.

Definition 1. *[47] An elliptic curve defined over the field $\mathbb{F}_p$ denoted by $E(\mathbb{F}_p)$ is expressed as a cubic equation:*

$$y^2 = x^3 + ax + b \pmod{p} \tag{3.0.1}$$

where p is a prime number greater than 3 and a, b are elements in the field $\mathbb{F}_p$ with the condition that $4a^3 + 27b^2 \neq 0$. This equation defines a unique set of points. When these points are paired with a specific addition operation, they form an abelian group with point of infinity as the identity element of the group.

Definition 2. *[47] Let $A(s_1, w_1)$ and $B(s_2, w_2)$ be two points on $E(\mathbb{F}_p)$ such that $A \neq B$. Addition of two points A and B in an elliptic curve is defined as:*

$$A + B = C(s_3, w_3), \tag{3.0.2}$$

where

$$s_3 = \{\lambda^2 - s_1 - s_2\} \pmod{p}, \tag{3.0.3}$$

$$w_3 = \{\lambda(s_1 - s_3) - w_1\} \pmod{p} \tag{3.0.4}$$

and

$$\lambda = \frac{w_2 - w_1}{s_2 - s_1} \ mod\ p. \tag{3.0.5}$$

Definition 3. *[47] Consider two points A and B that coincide on an elliptic curve over $\mathbb{F}_p$. Doubling of a point in an elliptic curve is defined as:*

$$A(s_1, w_1) + B(s_1, w_1) = C(s_2, w_2), \tag{3.0.6}$$

where

$$s_2 = \{\lambda^2 - 2s_1\} \pmod{p}, \tag{3.0.7}$$

$$w_2 = \{\lambda(s_1 - s_2) - w_1\} \pmod{p} \tag{3.0.8}$$

and

$$\lambda = \frac{3{s_1}^2 + a}{2w_1} \pmod{p}. \tag{3.0.9}$$

Definition 4. *[47] Operation of scalar multiplication over any point A of elliptic curve is defined as repeated addition, that is, $kA = A + A + ...(k \text{ times})$.*

Definition 5. *[39] The strength of ECC is determined by the challenge of solving the Elliptic Curve Discrete Logarithm Problem (ECDLP). In simpler terms, this problem involves finding a specific number n such that $A = nB$, where A and B are points on an elliptic curve. The difficulty of solving this problem forms the foundation of the security provided by Elliptic Curve Cryptography.*

Definition 6. *[39] ECDH key exchange relies on a specific property of elliptic curves, represented as*

$$(n * G) * m = (m * G) * n. \tag{3.0.10}$$

Let m, n be private keys of Alice and Bob respectively. Public key generated by Alice is $m * G$ and Public key generated by Bob is $n * G$. These public keys are shared through an open channel. Now, Alice performs a multiplication operation involving her private key and Bob's public key,

while Bob does the same by multiplying his private key with Alice's public key. Both Alice and Bob will get the same resultant. This method of sharing key between users is known as ECDH key exchange.

Definition 7. *[22] Suslin matrix $S_r(v, w)$ can be constructed when we have two given rows, v and w. Inductive definition of Suslin matrix is given as follow:*
Let

$$v = (c_0, c_1, ...c_r) = (c_0, t), \tag{3.0.11}$$

where $t = (c_1, ...c_r)$
and

$$w = (d_0, d_1, ...d_r) = (d_0, u), \tag{3.0.12}$$

where $u = (d_1, ...d_r)$. *Now, set* $S_0(v, w) = c_0$.
Therefore, Suslin matrix $S_r(v, w)$ *is defined as:*

$$S_r(v, w) = \begin{bmatrix} c_0 I_{2^{r-1}} & S_{r-1}(t, u) \\ -S_{r-1}(u, t)^T & d_0 I_{2^{r-1}}. \end{bmatrix} \tag{3.0.13}$$

Remark Here, we define the 8×8 Suslin matrix which is of the form:

$$S = S_3(v, w) = \begin{bmatrix} c_0 & 0 & 0 & 0 & c_1 & 0 & c_2 & c_3 \\ 0 & c_0 & 0 & 0 & 0 & c_1 & -d_3 & d_2 \\ 0 & 0 & c_0 & 0 & -d_2 & c_3 & d_1 & 0 \\ 0 & 0 & 0 & c_0 & -d_3 & -c_2 & 0 & d_1 \\ -d_1 & 0 & c_2 & c_3 & d_0 & 0 & 0 & 0 \\ 0 & -d_1 & -d_3 & d_2 & 0 & d_0 & 0 & 0 \\ -d_2 & c_3 & -c_1 & 0 & 0 & 0 & d_0 & 0 \\ -d_3 & -c_2 & 0 & -c_1 & 0 & 0 & 0 & d_0 \end{bmatrix}, \tag{3.0.14}$$

where $v = (c_0, c_1, c_2, c_3)$ and $w = (d_0, d_1, d_2, d_3)$.
This matrix will be invertible if dot product $v.w^t = 1$.
Inverse of this matrix is always of the form:

$$S^{-1} = S_3^{-1}(v, w) = \begin{bmatrix} d_0 & 0 & 0 & 0 & -c_1 & 0 & -c_2 & -c_3 \\ 0 & d_0 & 0 & 0 & 0 & -c_1 & d_3 & -d_2 \\ 0 & 0 & d_0 & 0 & d_2 & -c_3 & -d_1 & 0 \\ 0 & 0 & 0 & d_0 & d_3 & c_2 & 0 & -d_1 \\ d_1 & 0 & -c_2 & -c_3 & c_0 & 0 & 0 & 0 \\ 0 & d_1 & d_3 & -d_2 & 0 & c_0 & 0 & 0 \\ d_2 & -c_3 & c_1 & 0 & 0 & 0 & c_0 & 0 \\ d_3 & c_2 & 0 & c_1 & 0 & 0 & 0 & c_0 \end{bmatrix}. \tag{3.0.15}$$

4. Proposed Hybrid Chaotic Map

Chaos-based cryptography relies on chaotic maps to generate highly unpredictable sequences for permutation and diffusion in encryption. However, traditional one-dimensional (1D) chaotic maps such as the logistic map suffer from limited keyspace, weak randomness, and linear predictability. To address these issues, we propose a HSLC map, which integrates multiple nonlinear functions into a high-dimensional chaotic system. This new chaotic map significantly enhances randomness, increases key sensitivity, and provides stronger security compared to traditional 1D maps.

4.1. Mathematical Definition of the HSLC Map

The proposed HSLC chaotic map is a three-dimensional system, defined as follows:

$$X_{n+1} = \sin(\pi\mu X_n(1 - X_n)) \tag{4.1.1}$$

$$Y_{n+1} = 1 - \alpha Y_n^2 + \beta X_n \tag{4.1.2}$$

$$Z_{n+1} = \cos(\gamma \arccos(Y_n)) \tag{4.1.3}$$

where:

- X_n, Y_n, Z_n are the state variables representing the chaotic system at iteration n.
- $\mu, \alpha, \beta, \gamma$ are control parameters that determine the chaotic behavior.
- $\sin(\pi\mu X_n(1 - X_n))$ introduces strong non-linearity, ensuring unpredictable chaotic sequences.
- $1-\alpha Y_n^2+\beta X_n$ ensures a strong coupling effect between X_n and Y_n, making it more difficult to predict the sequence.
- $\cos(\gamma \arccos(Y_n))$ forces state dependency, increasing randomness.

The final chaotic sequence is obtained using the following transformation:

$$X_{n+1} = (x_{n+1} + y_{n+1} + z_{n+1}) \mod 1 \tag{4.1.4}$$

$$Y_{n+1} = (y_{n+1} \cdot z_{n+1} - x_{n+1}) \mod 1 \tag{4.1.5}$$

$$Z_{n+1} = (z_{n+1} + x_{n+1}^2 - y_{n+1}) \mod 1 \tag{4.1.6}$$

The use of mod 1 ensures that values remain within the range $(0, 1)$, making them suitable for encryption applications.

4.2. Chaotic Behavior and Parameter Selection

To ensure that the system remains highly chaotic, we must carefully choose the control parameters $\mu, \alpha, \beta, \gamma$. Through bifurcation and Lyapunov exponent analysis, we have determined that the system exhibits strong chaos when:

- $8 \leq \mu \leq 50$ (for strong logistic-sinusoidal behavior),
- $1.1 \leq \alpha \leq 2.5$,
- $0.2 \leq \beta \leq 0.5$,
- $2.0 \leq \gamma \leq 3.5$.

For optimal performance in encryption, we recommend the values:

$$\mu = 10, \quad \alpha = 1.2, \quad \beta = 0.3, \quad \gamma = 2.5. \tag{4.2.1}$$

These parameters ensure that the chaotic map maintains ergodicity and unpredictability.

4.3. Derivation of Initial Conditions from the Shared Key

To generate a deterministic yet unpredictable chaotic sequence, we derive the initial conditions X_0, Y_0, Z_0 from the shared secret integer k using cryptographic hashing. This ensures that both sender and receiver generate identical chaotic sequences without explicit transmission.

$$X_0 = \frac{\text{int}(\text{hash}(k + \text{“}X\text{”})[0:8], 16) \mod 1000}{1000} \tag{4.3.1}$$

$$Y_0 = \frac{\text{int}(\text{hash}(k + \text{“}Y\text{”})[8:16], 16) \mod 1000}{1000} \tag{4.3.2}$$

$$Z_0 = \frac{\text{int}(\text{hash}(k + \text{“}Z\text{”})[16:24], 16) \mod 1000}{1000} \tag{4.3.3}$$

Since SHA-256 is deterministic, both sender and receiver compute identical initial conditions independently.

5. Security Analysis of the Proposed Chaotic Map

The security strength of a chaotic system for cryptographic applications is often evaluated through various dynamical and statistical properties. This section presents an in-depth analysis of the proposed HSLC map based on key security parameters such as bifurcation behavior, Lyapunov exponent, entropy measures, and phase space representation.

5.1. Bifurcation Diagram Analysis

The bifurcation diagram of the proposed chaotic map illustrates its complex behavior over a range of control parameters μ. Figure 1 exhibits dense and widely distributed chaotic trajectories, ensuring a high degree of randomness and unpredictability. The absence of periodic windows further supports the robustness of the map in generating highly unpredictable sequences, a crucial property for cryptographic applications.

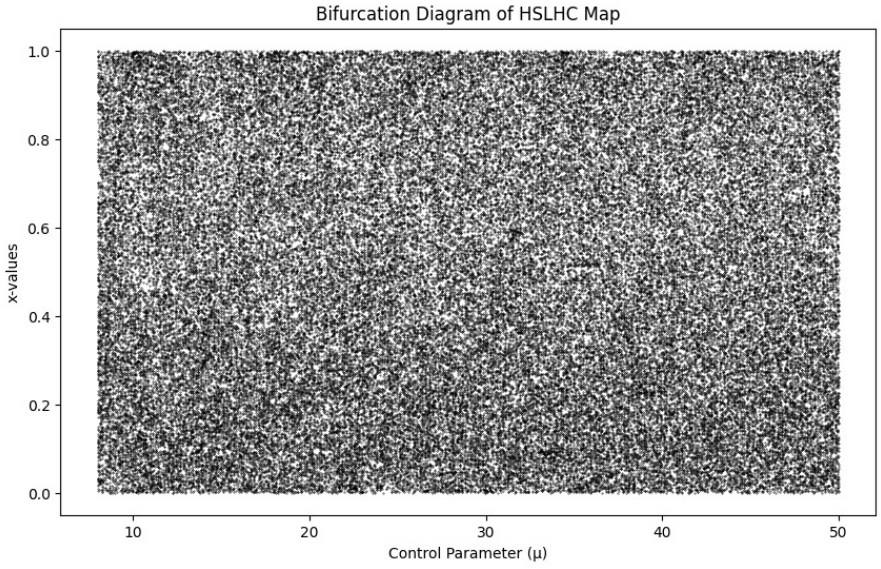

Figure 1: Bifurcation diagram of the proposed chaotic map.

5.2. Lyapunov Exponent Analysis

The Lyapunov exponent (λ) is a key indicator of chaos in a dynamical system. The computed Lyapunov exponent remains consistently positive and increases as μ grows, reaching values above $\lambda > 2.0$ for larger values of μ, as shown in Figure 2. This confirms the presence of strong chaotic behavior and high sensitivity to initial conditions, making the system suitable for secure encryption schemes.

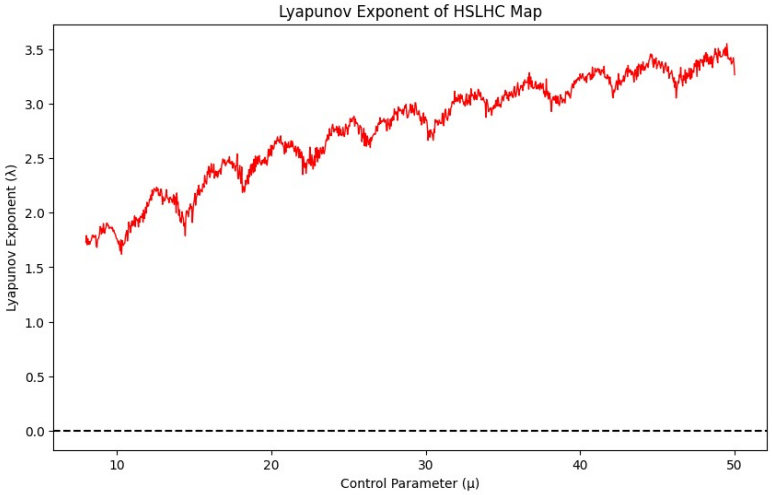

Figure 2: Lyapunov exponent of the proposed chaotic map.

5.3. Entropy Evaluation

Entropy is a fundamental measure of randomness in a chaotic system. The Shannon entropy of the proposed map remains nearly constant at a high value (8 bits), indicating uniform and unpredictable output distributions, as shown in Figure 3.

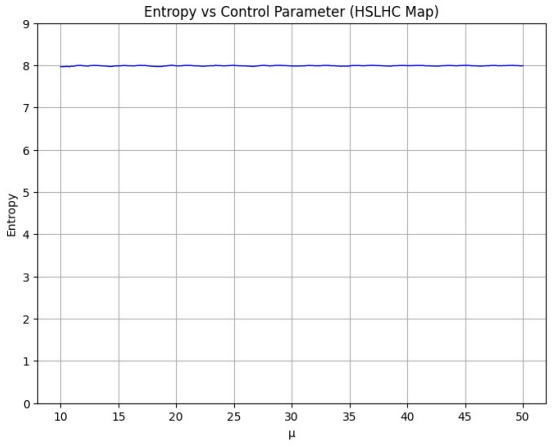

Figure 3: Entropy evaluation of the chaotic map.

5.4. Phase Space Representation

The three-dimensional phase space representation of the chaotic system shows a well-distributed and complex structure, without any observable periodicity or clustering, as shown in Figure 4. This confirms the presence of chaotic dynamics, which strengthens the system's resistance against phase space-based attacks.

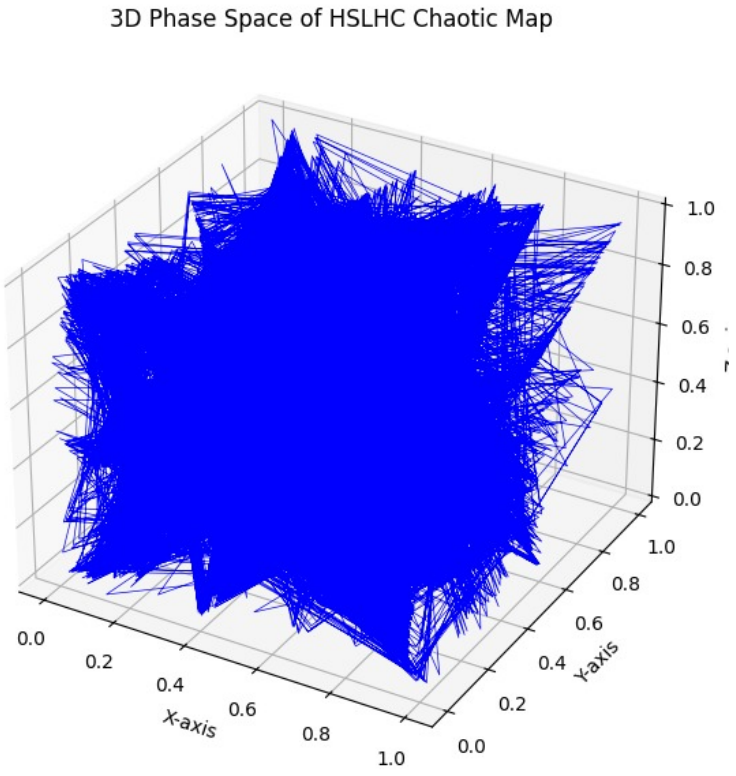

Figure 4: 3D phase space representation of the chaotic system.

5.5. Approximate Entropy

The approximate entropy (ApEn) of the chaotic sequence is a crucial measure of randomness. Higher ApEn values indicate greater complexity, which is desirable for cryptographic applications. The proposed chaotic map maintains ApEn values in a high range, indicating that the output sequences are highly unpredictable, as shown in Figure 5.

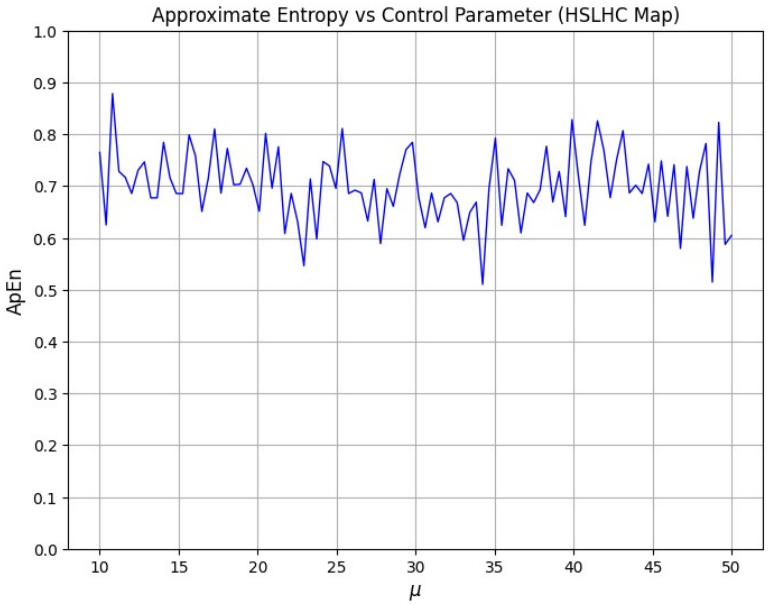

Figure 5: Approximate entropy of the chaotic map.

5.6. Security Implications

The combined analysis of bifurcation behavior, Lyapunov exponent, entropy measures, and phase space representation confirms that the proposed HSLC map exhibits strong chaotic properties. These characteristics ensure high sensitivity to initial conditions, a large key space, and resistance to statistical and dynamical attacks, making the proposed system highly suitable for secure encryption and cryptographic applications.

5.7. Comparison with Traditional Chaotic Maps

Compared to classical 1D chaotic maps such as the logistic map and tent map, the HSLC map provides:

- **Higher Complexity and Randomness:** The combination of sinusoidal, hyperbolic, and trigonometric transformations enhances unpredictability.
- **Stronger Key Sensitivity:** Any minor change in the shared key completely alters the chaotic sequence.
- **Larger Keyspace:** The three-dimensional nature of the map increases the number of possible keys exponentially.
- **Better Statistical Properties:** Ensures a uniform histogram in encryption, eliminating vulnerabilities to frequency analysis.

The proposed HSLC chaotic map is a high-dimensional, highly nonlinear system that exhibits strong chaotic behavior within the selected parameter range. It provides an ideal balance between computational efficiency and security, making it highly suitable for image encryption applications. By integrating this chaotic system into our encryption scheme, we significantly enhance security and efficiency, ensuring robust protection against various cryptographic attacks.

6. Proposed Image Encryption Scheme

The proposed image encryption scheme integrates chaotic permutation (confusion) and Suslin matrix-based diffusion (substitution) to achieve high security, efficiency, and robustness. The encryption process begins with preprocessing the image, where it is converted to grayscale, resized, and padded if necessary. Next, encryption parameters are securely derived from a shared secret integer using cryptographic hashing, ensuring that both sender and receiver independently compute identical keys without explicit exchange.
The chaotic permutation step utilizes a HSLC map to generate a pseudo-random permutation sequence, scrambling pixel positions to eliminate spatial correlations. In the diffusion stage, a special invertible Suslin matrix—constructed using vectors v and w that satisfy $v \cdot w = 1$—is applied to 4×4 blocks of the permuted image, ensuring global impact of local changes and strong key sensitivity.
Decryption follows the reverse steps, applying the inverse Suslin matrix and reversing the chaotic permutation to fully recover the original image. By leveraging secure key synchronization, high-dimensional chaos, and matrix-based diffusion, this scheme ensures strong resistance against statistical, differential, and brute-force attacks, making it an ideal choice for secure image transmission.
Suppose, Alice desires to share an image securely with Bob. To ensure the security of their communication, both Alice and Bob jointly choose an elliptic curve of the form:

$$y^2 = x^3 + ax + b \pmod{p}$$

with the generator point G.

6.1. Key Generation

Both, Alice and Bob generate their keys in the following manner and subsequently construct their secret matrix.

- Alice selects her private key as n_A.
- Bob selects his private key as n_B.
- Alice generates her public key as $P_A = n_A G$.
- Bob generates his public key as $P_B = n_B G$.
- Secret key generated by Alice, $S_A = n_A P_B = (S_{31}, S_{32})$.
- Secret key generated by Bob, $S_A = n_B P_A = (S_{31}, S_{32})$.
- Alice selects a random integer k such that $2 < k < n-1$, where n is the order of the elliptic curve.

6.2. Derivation of the Structured Vector v

In our scheme, the vector v is designed to be a short, structured vector whose components are derived from the shared secret key k. Typically, v is chosen as a three-element vector, i.e.,

$$v = (v_0,\, v_1,\, v_2)\,.$$

Derivation of v:

1. **Hashing the Shared Key:**
   The shared secret key k is first processed using a secure cryptographic hash function such as SHA-256. This produces a hexadecimal string that is a deterministic function of k.

2. **Extracting Components:**
   Specific segments of the resulting hash are then used to form the components of v. For instance,

   $$v_0 = (\text{hash}(k)[0:8]) \bmod p, \;\; v_1 = (\text{hash}(k)[8:16]) \bmod p, \;\; v_2 = (\text{hash}(k)[16:24]) \bmod p,$$

   where the notation $\text{hash}(k)[0:8]$ means "take the substring of the hash output starting at index 0 and ending before index 8." This yields the first 8 hexadecimal characters of the hash. Similarly, $\text{hash}(k)[8:16]$ extracts the next 8 characters, and $\text{hash}(k)[16:24]$ the following 8 characters.

The modulo operation with a prime p is applied to ensure that the resulting components are nonzero and well-distributed. Using a prime number helps avoid trivial collisions and ensures that the components possess desirable cryptographic properties.
Thus, v is chosen as a 3-element vector whose components v_0, v_1, and v_2 are deterministically derived from the hash of the shared key k and reduced modulo a prime number p to ensure they are nonzero and well-distributed. This carefully chosen vector length is sufficient to build an invertible Suslin matrix that plays a key role in the diffusion process of the encryption scheme.

6.3. Preprocessing the Image

Before encryption, the image undergoes preprocessing to ensure compatibility with the encryption scheme.

- **Convert Image to Grayscale:** If the input image is in RGB format, it is converted into an 8-bit grayscale image (pixel values between 0 and 255).
- **Resize the Image:** The image is resized to a fixed size (e.g., 256×256 pixels) to ensure uniform encryption and decryption.
- **Apply Padding (if Necessary):** If the image dimensions are not divisible by 4, zero-padding is applied to ensure they are multiples of 4. This ensures compatibility with 4×4 Suslin matrix-based diffusion.

6.4. Securely Constructing the Suslin Matrix $S(v, w)$

A special invertible Suslin matrix is computed securely from k.

1. Derive the Vector v from k using hash output.
2. Compute the Vector w to Ensure $v \cdot w = 1$:

$$d = v_0^2 + v_1^2 + v_2^2 \tag{6.4.1}$$

$$w_0 = \frac{v_0}{d}, \quad w_1 = \frac{v_1}{d}, \quad w_2 = \frac{v_2}{d} \tag{6.4.2}$$

3. Construct the Suslin Matrix:

$$S(v, w) = \begin{bmatrix} v_0 & 0 & v_1 & v_2 \\ 0 & v_0 & -w_2 & w_1 \\ -w_1 & v_2 & w_0 & 0 \\ -w_2 & -v_1 & 0 & w_0 \end{bmatrix} \tag{6.4.3}$$

4. Compute the Inverse Suslin Matrix:

$$S^{-1} = S(w, v)^T \tag{6.4.4}$$

6.5. Step 3: Chaotic Permutation (Confusion)

A chaotic sequence is generated to scramble pixel positions.

1. Generate Chaotic Permutation Sequence using the chaotic map.
2. Sort the Chaotic Sequence to Create a Permutation Order.
3. Apply Permutation: Pixels are rearranged, destroying spatial correlation.

6.6. Step 4: Diffusion (Pixel Value Modification Using Suslin Matrix)

1. Partition the Image into 4×4 Blocks.
2. Apply the Suslin Matrix to Each Block:

$$B' = S(v, w) \times B \mod 256. \tag{6.6.1}$$

3. Repeat for Multiple Rounds to enhance security.

6.7. Decryption Process

1. Reverse Diffusion: Each block is multiplied by S^{-1}:

$$B = S^{-1} \times B' \mod 256. \tag{6.7.1}$$

2. Reverse Permutation: The chaotic permutation order is reversed to restore pixel positions.

The encryption scheme integrates:

- Secure Key Synchronization Without Transmission
- Chaotic Permutation for Confusion
- Invertible Suslin Matrix for Diffusion

This ensures high security, efficiency, and robustness in image encryption.

6.8. Authentication and Verification

Alice enhances the proposed scheme by introducing authentication through digital signatures in the following manner:

- Calculates the hash value h_x of S_x from S_A as follows:

$$S_x = S_{31} \oplus S_{32},$$

$$h_x = SHA_{256}(S_x).$$

- Computes the hash value H by concatenating h_C and h_x as follows:

$$h_C = SHA_{256}(C),$$

$$H = (h_C || h_x).$$

- Calculates, k' using the parameter k as follows:

$$k' = S_x \oplus k.$$

- Evaluates the digital signature (V, W) as follows:

$$V = SHA_{256}(H),$$

$$W = ((k') - V) mod\ n.$$

- Sends the digital signature (V, W) and ciphered image C to Bob.

Bob ensures authenticity by verifying the digital signature in the following manner:

- Calculates k from (V, W) and S_A as follows:

$$S_x = S_{31} \oplus S_{32},$$

$$k = ((V + W) \oplus S_x).$$

- Calculates the hash value h_x of S_x from S_A as follows:

$$S_x = S_{31} \oplus S_{32},$$

$$h_x = SHA_{256}(S_x).$$

- Computes the hash value H by concatenating h_C and h_x as follows:

$$h_C = SHA_{256}(C).$$

$$H = (h_C || h_x).$$

- Calculates V' from computed hash value H. If V' is same as V, then the signature is verified.

$$V = SHA_{256}(H).$$
$$= V.$$

  Hence,

$$V = V.$$

7. System Architecture

The architecture of the proposed encryption scheme consists of the following major components:

- **Preprocessing:** The input image is converted into grayscale (if not already) and resized to ensure its dimensions are multiples of 4 using zero-padding.
- **Key Derivation:** A secure cryptographic hash function is applied to a shared key to generate deterministic initial conditions for the chaotic system.
- **Chaotic Permutation (Confusion):** The pixel positions of the image are scrambled using a hybrid chaotic system (HSLC map), ensuring high randomness and resistance against statistical attacks.

Algorithm 1 Proposed Image Encryption Algorithm

1: Convert I to grayscale (if necessary) and resize it to ensure divisibility by 4.
2: Compute initial conditions X_0, Y_0, Z_0 from k using a cryptographic hash function.
3: Generate a chaotic sequence using the HSLC map.
4: Compute the pixel permutation order and apply it to I.
5: Partition the permuted image into 4×4 blocks.
6: Construct the Suslin matrix $S(v, w)$ using values derived from k.
7: Apply matrix multiplication to each block using $S(v, w)$.
8: **return** Encrypted image I_C.

Algorithm 2 Proposed Image Decryption Algorithm

Require: Encrypted image I_C, shared key k
Ensure: Recovered image I_R
1: **Step 1: Generate Chaotic Parameters**
2: Compute initial conditions X_0, Y_0, Z_0 from k using the cryptographic hash function.
3: Regenerate the chaotic sequence using the HSLC map.
4: Compute the original pixel permutation order.
5: **Step 2: Reverse Diffusion**
6: Partition I_C into 4×4 blocks.
7: Compute the inverse of the Suslin matrix $S(v, w)^{-1} = S(w, v)^T$.
8: Multiply each block by $S(v, w)^{-1}$ modulo 256 to obtain I_P.
9: **Step 3: Reverse Confusion**
10: Apply the inverse permutation to restore the original pixel order.
11: **return** Recovered image I_R.

- **Diffusion via Suslin Matrix:** The permuted image is divided into 4×4 blocks, and each block undergoes matrix multiplication with an invertible Suslin matrix to modify pixel values in a non-linear fashion.

- **Decryption Process:** The encrypted image undergoes reverse diffusion and inverse chaotic permutation to retrieve the original image.

Flowchart of proposed encryption and decryption schemes are given in Figure 6 and Figure 7, respectively.

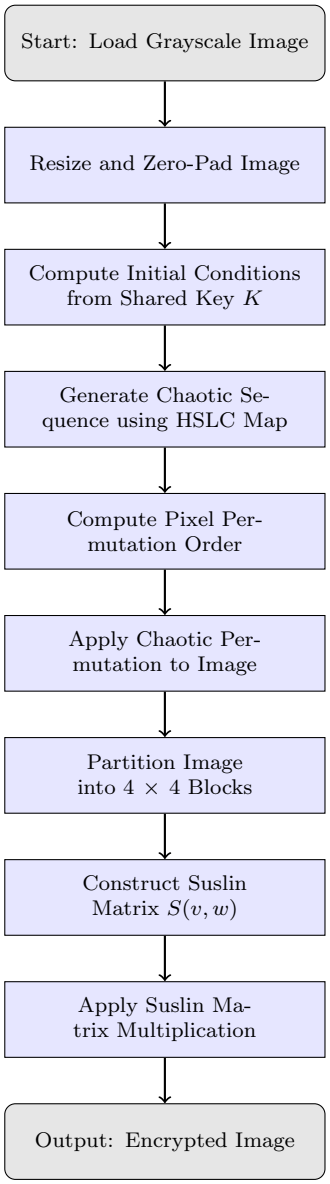

Figure 6: Encryption Flowchart

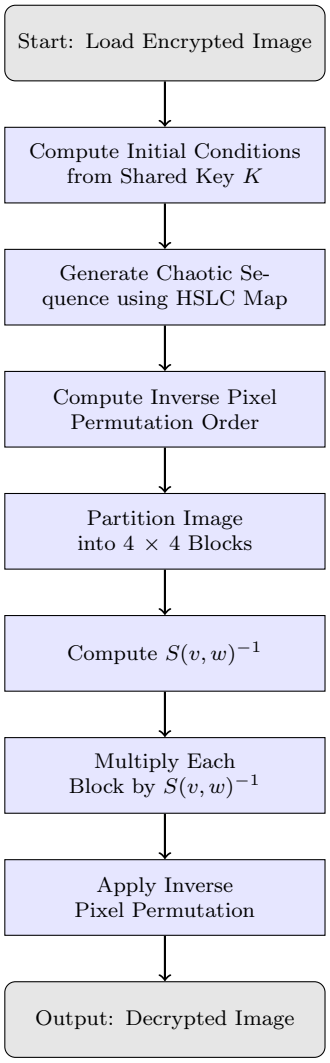

Figure 7: Decryption Flowchart

8. Visual Results

In this section, we present a visual demonstration of the proposed image encryption scheme. The experimental results are illustrated in Figure 8, 9, 10, 11, 12, 13 and 14 using several standard test images, showing both the plain and encrypted outputs. These results highlight the effectiveness of the scheme in disrupting spatial correlations and producing visually unrecognizable cipher images. The images included for analysis are Cameraman (512× 512), Pepper (512× 512), Pirate (512× 512), Lena (256× 256), Lena (512× 512) and Gravel (1024× 1024). We implemented the proposed scheme on Core i7 9th Generation computer with CPU 2.00GHz and RAM 16 GB 1TBSSD by using Python-3 64-bit software.

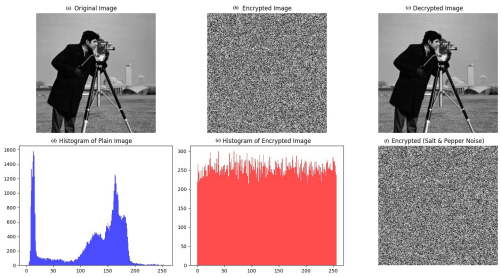

Figure 8: Visual Results for the Cameraman (512×512) Image: (a) Original, (b) Encrypted, (c) Decrypted, (d) Histogram of Plain Image, (e) Histogram of Encrypted Image, (f) Encrypted Image Under Salt & Pepper Noise.

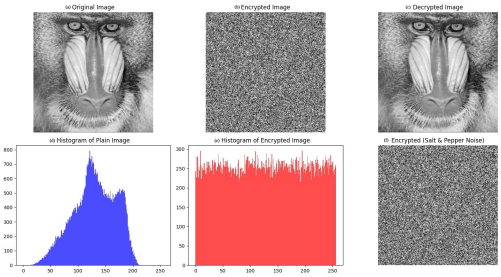

Figure 9: Visual Results for the Baboon (512×512) Image: (a) Original, (b) Encrypted, (c) Decrypted, (d) Histogram of Plain Image, (e) Histogram of Encrypted Image, (f) Encrypted Image Under Salt & Pepper Noise.

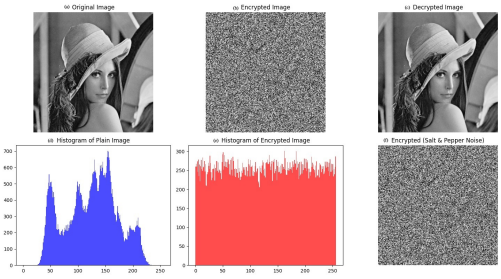

Figure 12: Visual Results for the Lena (256×256) Image: (a) Original, (b) Encrypted, (c) Decrypted, (d) Histogram of Plain Image, (e) Histogram of Encrypted Image, (f) Encrypted Image Under Salt & Pepper Noise.

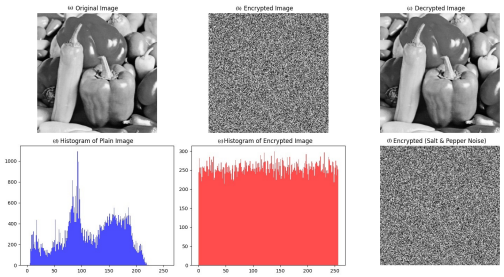

Figure 10: Visual Results for the Pepper (512×512): (a) Original, (b) Encrypted, (c) Decrypted, (d) Histogram of Plain Image, (e) Histogram of Encrypted Image, (f) Encrypted Image Under Salt & Pepper Noise.

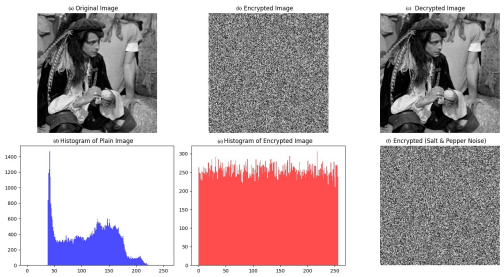

Figure 11: Visual Results for the Pirate (512×512): (a) Original, (b) Encrypted, (c) Decrypted, (d) Histogram of Plain Image, (e) Histogram of Encrypted Image, (f) Encrypted Image Under Salt & Pepper Noise.

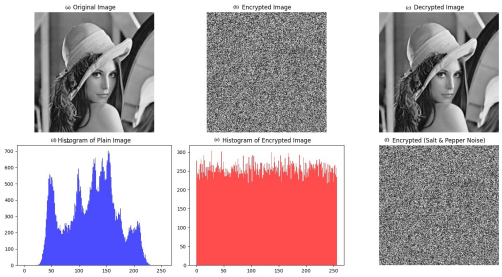

Figure 13: Visual Results for the Lena (512×512) Image: (a) Original, (b) Encrypted, (c) Decrypted, (d) Histogram of Plain Image, (e) Histogram of Encrypted Image, (f) Encrypted Image Under Salt & Pepper Noise.

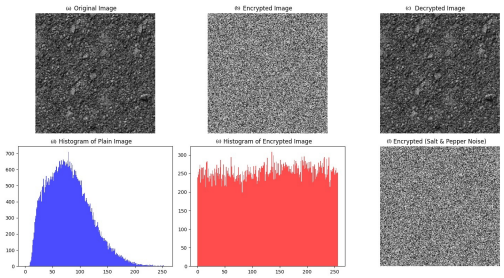

Figure 14: Visual Results for the (1024×1024): (a) Original, (b) Encrypted, (c) Decrypted, (d) Histogram of Plain Image, (e) Histogram of Encrypted Image, (f) Encrypted Image Under Salt & Pepper Noise.

Remarkably, the decrypted images obtained from the encryption process closely resembled the original plain images. This observation underscores the effectiveness of our proposed algorithm in preserving the inherent structure of the plain images. The tests clearly demonstrate the algorithm's ability to maintain the integrity and visual fidelity of the original images after encryption and decryption processes.

9. Experimental Analysis

The proposed image encryption scheme was evaluated using a variety of standard test images including Baboon (512×512), Cameraman (512×512), Lena (256×256), Pepper (512×512), Pirate (512×512), and Gravel (1024×1024). In this section, we present the experimental results in terms of differential metrics, statistical measures, texture analysis (GLCM), key sensitivity, and processing speed.

9.1. Differential and Statistical Metrics

Table 1 summarizes the main differential metrics including UACI, NPCR, Shannon entropy (for both plain and cipher images), and the chi-square statistic for the cipher image.

Table 1: Differential and Statistical Metrics

Image	**UACI (%)**	**NPCR (%)**	**Entropy (Plain)**	**Entropy (Cipher)**	**Chi-square**
Baboon (512×512)	33.40	99.61	7.2418	7.9975	226.18
Cameraman (512×512)	33.12	99.63	7.0293	7.9970	274.73
Lena (256×256)	33.34	99.62	7.4429	7.9968	292.48
Pepper (512×512)	33.41	99.62	7.2638	7.9974	235.23
Pirate (512×512)	33.46	99.62	7.2597	7.9961	352.20
Gravel (1024×1024)	33.46	99.58	7.2597	7.9961	352.20

9.2. Correlation Coefficient Analysis

Table 2 shows the correlation coefficients in horizontal, vertical, and diagonal directions for the plain and encrypted images.

Table 2: Correlation Coefficients (Plain / Encrypted)

Image	Horizontal	Vertical	Diagonal
Baboon (512×512)	0.8446 / -0.0058	0.7831 / -0.0022	0.7458 / 0.0037
Cameraman (512×512)	0.9549 / 0.0013	0.9733 / -0.0048	0.9335 / -0.0102
Lena (256×256)	0.9258 / 0.0048	0.9593 / 0.0037	0.9037 / -0.0003
Pepper (512×512)	0.9378 / 0.0014	0.9520 / -0.0016	0.9088 / 0.0011
Pirate (512×512)	0.3262 / -0.0013	0.2687 / -0.0183	0.1238 / -0.0025
Gravel (1024×1024)	0.3262 / -0.0013	0.2687 / -0.0183	0.1238 / -0.0025

9.3. PSNR Analysis under Noise Attacks

Table 3 provides the Peak Signal-to-Noise Ratio (PSNR) values under various noise conditions. The scheme is evaluated under salt-and-pepper noise at different densities as well as Gaussian noise. Figure 15 shows the decrypted images with various noise densities.

Table 3: PSNR Analysis under Noise Attacks

Image	PSNR (S&P Attack)	PSNR (Gaussian)	S&P Noise 0.001	S&P Noise 0.002	S&P Noise 0.005
Baboon (512×512)	24.77 dB	9.72 dB	34.65 dB	31.77 dB	27.70 dB
Cameraman (512×512)	23.82 dB	8.48 dB	33.57 dB	30.59 dB	26.64 dB
Lena (256×256)	24.58 dB	9.20 dB	34.35 dB	31.39 dB	27.51 dB
Pepper (512×512)	24.45 dB	9.16 dB	34.33 dB	31.41 dB	27.39 dB
Pirate (512×512)	24.45 dB	9.16 dB	34.33 dB	31.41 dB	27.39 dB
Gravel (1024×1024)	23.80 dB	8.42 dB	33.44 dB	30.70 dB	26.70 dB

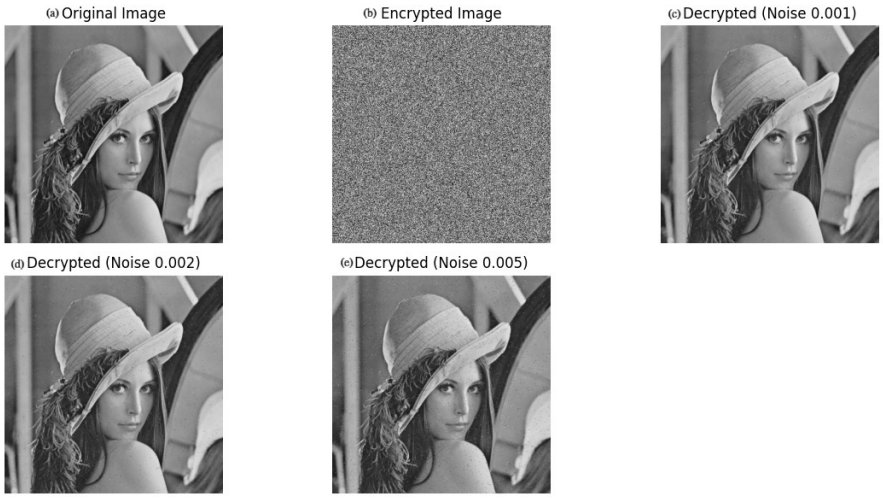

Figure 15: Visualization of Noise attack with different noise densities

9.4. GLCM Texture Analysis

Texture analysis using the Gray-Level Co-Occurrence Matrix (GLCM) is used to evaluate the diffusion capability. Table 4 summarizes the GLCM features for the plain and encrypted images. For each image, the table lists the Contrast (Cn), Energy (En), and Homogeneity (Hn).

Table 4: GLCM Analysis for Test Images (Plain / Encrypted)

Image	**Contrast (Cn)**	**Energy (En)**	**Homogeneity (Hn)**
Baboon (512×512)	830.4212 / 10881.6826	0.0105 / 0.0041	0.0815 / 0.0122
Cameraman (512×512)	149.6344 / 10796.1137	0.0403 / 0.0041	0.3764 / 0.0120
Lena (256×256)	60.7854 / 10930.3886	0.0252 / 0.0041	0.3544 / 0.0123
Pepper (512×512)	139.2085 / 10844.7390	0.0489 / 0.0041	0.3649 / 0.0119
Pirate (512×512)	208.9772 / 10942.6223	0.0243 / 0.0041	0.2073 / 0.0121
Gravel (1024×1024)	1553.2251 / 10860.2889	0.0085 / 0.0041	0.0409 / 0.0121

9.5. Key Sensitivity Analysis

The encryption scheme exhibits high key sensitivity. A minimal change in the encryption key causes significant alterations in the decrypted image. Table 5 represent the proportion of pixels changed when a slight key modification is introduced:

Table 5: Key Sensitivity Analysis

Image	**Percentage of Pixels Affected**
Baboon (512×512)	99.34%
Cameraman (512×512)	99.01%
Lena (256×256)	99.36%
Pepper (512×512)	99.23%
Pirate (512×512)	99.23%
Gravel (1024×1024)	99.28%

9.6. Speed Analysis

Table 6 summarizes the average encryption and decryption times for the test images.

Table 6: Average Processing Times

Image	**Encryption Time (s)**	**Decryption Time (s)**	**Total Time (s)**
Baboon (512×512)	1.5825	0.1941	1.7766
Cameraman (512×512)	1.6852	0.2140	1.8992
Lena (256×256)	1.6293	0.1828	1.8122
Pepper (512×512)	1.5636	0.1936	1.7572
Pirate (512×512)	1.5748	0.2038	1.7787
Gravel (1024×1024)	1.7170	0.1872	1.9042

The experimental results validate the effectiveness of the proposed image encryption scheme. Table 7 summarizes the results of various security parameters.

Table 7: Experimental Results of the Proposed Model

Criteria	Cameraman	Lena (256)	Lena (512)	Baboon	Peppers	Pirate	Gravel
NPCR (%)	99.63%	99.62%	99.60%	99.61%	99.62%	99.62%	99.58%
UACI (%)	33.32%	33.34%	33.40%	33.40%	33.42%	33.41%	33.46%
Information Entropy	7.9970	7.9968	7.9971	7.9975	7.9974	7.9974	7.9961
Chi-square	274	292	268	226	237	235	252
Encryption Time (sec)	1.685	1.629	1.594	1.582	1.563	1.574	1.716

- **High Differential Resistance:** NPCR values exceed 99.58% and UACI values are around 33.4%, indicating strong resistance to differential attacks.
- **Strong Randomness:** Encrypted images exhibit nearly ideal Shannon entropy (close to 8) and negligible correlation between adjacent pixels.
- **Effective Diffusion:** GLCM analysis shows a significant increase in contrast and a marked decrease in energy and homogeneity, confirming the robust diffusion capability.
- **High Key Sensitivity:** Minimal key modifications lead to over 99% of pixels being altered in the decrypted image.
- **Efficient Processing:** Total processing times for encryption and decryption are under 2 seconds for all test images, making the scheme suitable for real-time applications.

9.7. Data Loss Attack Analysis

Data loss attacks simulate scenarios where part of the encrypted image is lost or corrupted. In this experiment, we introduced two levels of data loss: **25%** and **50%**. The corrupted images were then decrypted, and the quality of the recovered images was measured using the Peak Signal-to-Noise Ratio.

- **25% Data Loss:** A quarter of the image was removed before decryption.
- **50% Data Loss:** Half of the image was removed before decryption.

The PSNR values for both cases are as follows:

Data Loss	PSNR (dB)
25% Loss	30.31 dB
50% Loss	29.35 dB

Table 8: PSNR values for decrypted images with different data loss percentages.

Figure 16 illustrates the encrypted image, the applied data loss, and the corresponding decrypted images.

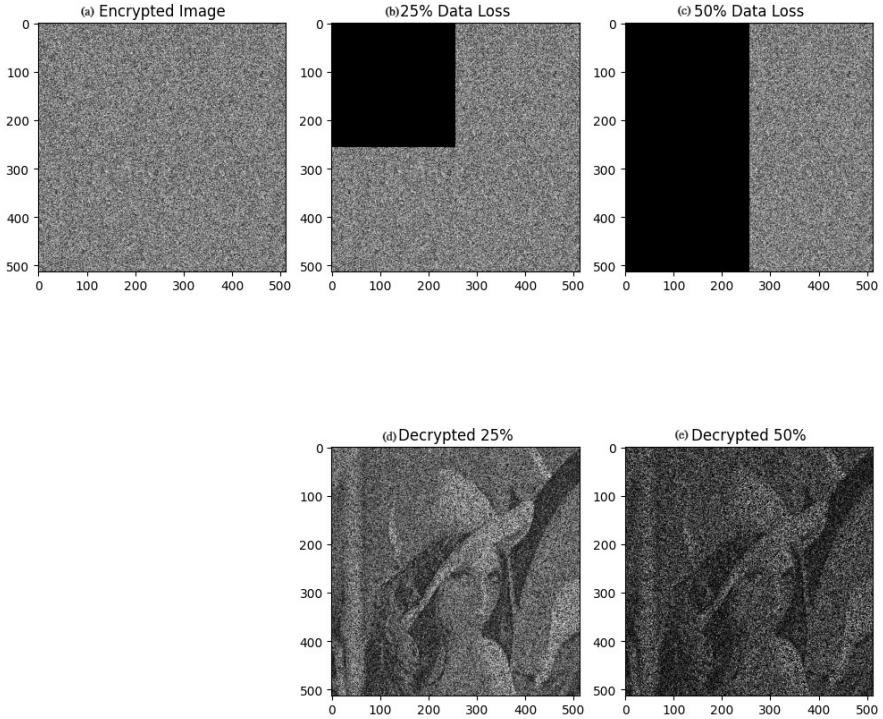

Figure 16: Visualization of Data Loss Attack. Top row: Encrypted image and different levels of data loss. Bottom row: Decrypted images after 25% and 50% loss.

From the PSNR values, we observe that while some information is lost, the decryption process still manages to reconstruct a recognizable version of the image. However, as expected, a higher percentage of data loss results in a lower PSNR and increased degradation in the recovered image.

The results demonstrate that the proposed encryption scheme offers strong security properties, randomness, and resilience against statistical and differential attacks.

10. Comparative Analysis

To validate the robustness and effectiveness of the proposed encryption scheme, a comparative analysis has been performed against several benchmark approaches across standard evaluation metrics including NPCR, UACI, Information Entropy, Chi-square test, and Correlation Coefficient Analysis (CCA).

Table 9: NPCR Comparison with Benchmark Approaches

Model	Cameraman	Lena	Baboon	Peppers
[44]	99.61%	99.62%	NA	NA
[9]	99.61%	99.61%	NA	NA
[38]	NA	99.65%	NA	NA
[49]	99.63%	99.62%	NA	99.60%
[46]	NA	99.62%	NA	NA
[31]	99.60%	99.62%	99.60%	99.61%
[2]	99.64%	99.61%	99.58%	99.61%
Proposed	**99.63%**	**99.60%**	**99.61%**	**99.62%**

Table 10: UACI Comparison with Benchmark Approaches

Model	Cameraman	Lena	Baboon	Peppers
[44]	33.46%	33.47%	NA	NA
[9]	33.55%	33.59%	NA	NA
[38]	NA	33.45%	NA	NA
[49]	33.56%	33.50%	NA	33.41%
[46]	NA	30.64%	NA	NA
[31]	33.44%	33.44%	33.46%	NA
[2]	33.39%	33.42%	33.48%	33.40%
Proposed	**33.33%**	**33.40%**	**33.40%**	**33.42%**

Table 11: Information entropy comparison against benchmark approaches

Model	Cameraman	Lena	Baboon	Peppers
[44]	7.9974	7.9974	NA	NA
[9]	7.9951	7.9951	NA	NA
[38]	NA	7.9973	NA	NA
[49]	7.9973	7.9969	NA	7.9972
[46]	NA	7.9973	NA	7.9972
[31]	7.9986	7.9989	7.9965	7.9975
[2]	7.9970	7.9975	7.9974	7.9972
Proposed	7.9970	7.9971	7.9975	7.9974

Table 12: Chi-square (χ^2) test results for encrypted images

Image Type	Cameraman	Lena	Baboon	Peppers
Encrypted Image [2]	275	225	236	256
Encrypted Image (Proposed)	274	221	226	237

Table 13: Correlation Coefficient Analysis (CCA) comparison with benchmark approaches

Model	Cameraman	Lena	Baboon	Peppers
[44]				
H	−0.0013	0.0058	NA	NA
V	0.0016	−0.0051	NA	NA
D	0.0058	−0.0030	NA	NA
[9]				
H	0.0040	0.0088	NA	NA
V	0.0088	0.0008	NA	NA
D	0.0180	0.0022	NA	NA
[38]				
H	NA	−0.0016	NA	NA
V	NA	0.0002	NA	NA
D	NA	−0.0035	NA	NA
[49]				
H	−0.0031	0.0040	NA	0.0013
V	−0.0006	−0.0012	NA	0.0032
D	0.0012	−0.0021	NA	−0.0068
[46]				
H	NA	0.0084	NA	NA
V	NA	−0.0039	NA	NA
D	NA	−0.0013	NA	NA
[31]				
H	0.0002	0.0002	0.0002	NA
V	0.0001	0.0005	0.00005	NA
D	0.0025	0.0024	0.0026	NA
[2]				
H	0.0033	0.0012	−0.00002	0.0084
V	0.0003	−0.0031	−0.0006	0.0008
D	0.0067	0.0034	−0.0016	0.0013
Proposed				
H	0.0013	0.0048	−0.0058	−0.0025
V	−0.0048	0.0037	−0.0022	−0.0020
D	−0.0102	−0.0003	0.0037	−0.0025

10.1. NPCR and UACI

The NPCR values in Table 9 demonstrate that the proposed method achieves high sensitivity to small changes in the plaintext image. For commonly used images such as Cameraman, Lena, Baboon, and Peppers, the NPCR values exceed 99.60%, with a peak value of 99.63%. This is comparable or superior to most existing works [44,9,49,31]. Similarly, the UACI values of the proposed scheme are consistently above 33.30%, closely aligning with ideal values and indicating strong diffusion characteristics, as indicated in Table 10. These results confirm that even minimal changes in the plaintext yield significantly different cipher images.

10.2. Information Entropy

As shown in Table 11, the information entropy of encrypted images generated by the proposed method is consistently close to the ideal value of 8. For all tested images, entropy values range between 7.9970 and 7.9975, reflecting a high degree of randomness and ensuring strong resistance against entropy-based attacks. The values are on par with, or slightly better than, the benchmark approaches [31,49].

10.3. Chi-square Test

The Chi-square test results presented in Table 12 show that the proposed method yields lower χ^2 values compared to previous methods, indicating better histogram uniformity. For instance, the proposed method results in χ^2 values of 274 for Cameraman and 221 for Lena, slightly lower than [2], suggesting improved resistance against statistical attacks.

10.4. Correlation Coefficient Analysis

Table 13 highlights the Correlation Coefficient values for horizontally, vertically, and diagonally adjacent pixels. The proposed scheme consistently produces values near zero or even negative, indicating very low correlation between adjacent pixels in the cipher image. This is a significant improvement over traditional schemes and supports the method's effectiveness in disrupting spatial redundancy. Compared to benchmark methods such as [44,31,2], the proposed technique delivers better decorrelation, enhancing security against statistical analysis.

In summary, the proposed encryption method performs competitively or better across all key metrics, ensuring high levels of security, randomness, and robustness. These results validate its effectiveness for secure image encryption and confirm its advantage over existing state-of-the-art techniques.

11. Conclusion

In this paper, we have presented a novel image encryption scheme that synergistically combines a high-dimensional chaotic map with a Suslin matrix-based diffusion mechanism. By generating a pseudo-random sequence through the proposed HSLC map and constructing an invertible Suslin matrix from a shared secret key, the scheme achieves robust confusion and diffusion without the need for explicit key exchange. The experimental results demonstrate that the encrypted images exhibit high entropy, low correlation among adjacent pixels, and strong differential properties, as confirmed by favorable NPCR, and UACI, metrics under various noise conditions. Moreover, the computational efficiency of the method makes it suitable for real-time applications in multimedia systems.

Future work will focus on extending the proposed scheme to handle color images and exploring hardware implementation to further improve its speed and efficiency. Additionally, incorporating adaptive parameter tuning and integrating additional cryptographic primitives may further enhance the overall security of the system. Overall, the proposed approach represents a promising direction for secure and efficient image encryption in diverse application scenarios.

Ethics Approval: No Human subject or animals are involved in the research.

Data Availability Statement: Authors declare that all the data being used in the design and production cum layout of the manuscript is declared in the manuscript.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

Acknowledgement: Second author thankfully acknowledge the support of DST INSPIRE.

References

1. A.A. Abd El-Latif, X. Niu, A hybrid chaotic system and cyclic elliptic curve for image encryption, AEU - International Journal of Electronics and Communications, vol. 67, 2013, pp. 136-143.
2. Y. M. Afify, N. H. Sharkawy, W. Gad, N. Badr, A new dynamic DNA-coding model for gray-scale image encryption. Complex & Intelligent Systems, vol. 10, 2024, pp. 745-761.
3. S. S. A. B. Aldin, M. Aykac, N. B. Aldin, Quad-color image encryption based on Chaos and Fibonacci Q-matrix, Multimedia Tools and Applications, vol. 83, 2024, pp. 7827-7846.
4. T.S. Ali, R. Ali, A novel medical image signcryption scheme using TLTS and henon chaotic map, IEEE Access, vol. 8, 2020, pp. 71974-71992.
5. F. Amounas, E.H. El Kinani, Security enhancement of image encryption based on matrix approach using elliptic curve, International Journal of Engineering Inventions, vol. 3, 2014, pp. 8-16.
6. E. O. Asani, G. Biety-Nwanju, A. E. Adeniyi, S. Bharany, A. O., Ibrahim, A. W. Abulfaraj, W. Nagmeldin, Development of an Image Encryption Algorithm using Latin Square Matrix and Logistics Map, International Journal of Advanced Computer Science and Applications, vol. 14, 2023, pp. 869-877.
7. S. S. Askar, A. A. Karawia, A. Alshamrani, Image encryption algorithm based on chaotic economic model, Mathematical Problems in Engineering, vol. 2015, 2015.
8. A. Banik, D. S. Laiphrakpam, A. Agrawal, R. Patgiri, Secret image encryption based on chaotic system and elliptic curve cryptography, Digital Signal Processing, vol. 129, 2022, pp. 103639.
9. W. Bao, C. Zhu, A secure and robust image encryption algorithm based on compressive sensing and DNA coding, Multimedia Tools and Applications, vol. 81, 2022, pp.15977-15996.
10. R. Chaker, O. EL ogri, A. Boua, Color image encryption system based fractional hyperchaotic, fibonacci matrix and quaternion algebra, International Journal of Information Technology, 2024, pp. 1-20.
11. A. Y. Darani, Y. K. Yengejeh, H. Pakmanesh, G. Navarro, Image encryption algorithm based on a new 3D chaotic system using cellular automata, Chaos, Solitons & Fractals, vol. 179, 2024, pp. 114396.
12. S. De, J. Bhaumik, TBLT-AES: A robust image encryption scheme, Journal of Discrete Mathematical Sciences and Cryptograpgy, vol. 17, 2014, pp. 273-288.
13. L. Ding, Q. Ding, A novel image encryption scheme based on 2D fractional chaotic map, DWT and 4D hyper-chaos, Electronics, vol. 9, 2020, pp. 1280.
14. A. Girdhar, H. Kapur, V. Kumar, A novel grayscale image encryption approach based on chaotic maps and image blocks, Applied Physics B, vol. 127, 2021, pp. 1-12.
15. L. H. Gong, H. X. Luo, R. Q. Wu, N. R. Zhou, New 4D chaotic system with hidden attractors and self-excited attractors and its application in image encryption based on RNG, Physica A: Statistical Mechanics and its Applications, vol. 591, 2022, pp. 126793.
16. L. Gong, R. Wu, N. Zhou, A new 4D chaotic system with coexisting hidden chaotic attractors, International Journal of Bifurcation and Chaos, vol. 30, 2020, pp. 2050142.
17. R. Hanchate, R. Anandan, Medical image encryption using hybrid adaptive elliptic curve cryptography and logistic map-based DNA Sequence in IoT Environment, IETE Journal of Research, vol. 70, 2024, pp. 5734-5749.
18. E. Hernández-Díaz, H. Pérez-Meana, V. Silva-García, R. Flores-Carapia, Jpeg images encryption scheme using elliptic curves and a new s-box generated by chaos, Electronics, vol. 10, 2021, pp. 413.
19. K. M. Hosny, S. T. Kamal, M. M. Darwish, G. A. Papakostas, New image encryption algorithm using hyperchaotic system and fibonacci q-matrix. Electronics, vol. 10, 2021, pp. 1066.
20. K. M. Hosny, M. A. Zaki, N. A. Lashin, M. M. Fouda, H. M. Hamza, Multimedia Security Using Encryption: A Survey, IEEE Access, 2023.
21. Z. W. Huang, N. R. Zhou, Image encryption scheme based on discrete cosine Stockwell transform and DNA-level modulus diffusion, Optics & Laser Technology, vol. 149, 2022, pp. 107879.

22. S. Jose, V. Tiwari, Study of $2 \times n$ right invertible matrix group via suslin matrices, Journal of Xi'an University of Architecture & Technology, vol. 12, 2020, pp. 671-678.

23. N. Koblitz, Elliptic curve cryptosystem, Mathematics of Computation, vol. 48, 1987, pp. 203-209.

24. M. Kumar, A. Iqbal, P. Kumar, A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie–Hellman cryptography, Signal Processing, vol. 125, 2016, pp. 187-202.

25. S. Kumar, D. Sharma, A chaotic based image encryption scheme using elliptic curve cryptography and genetic algorithm, Artificial Intelligence Review, vol. 57, 2024, pp. 87.

26. Q. Lai, G. Hu, U. Erkan, A. Toktas, High-efficiency medical image encryption method based on 2D Logistic-Gaussian hyperchaotic map, Applied Mathematics and Computation, vol. 442, 2023, pp. 127738.

27. H. Liu, Y. Liu, Cryptanalyzing an image encryption scheme based on hybrid chaotic system and cyclic elliptic curve, Optics & Laser Technology, vol. 56, 2014, pp. 15-19.

28. M. Liu, G. Ye, A new DNA coding and hyperchaotic system based asymmetric image encryption algorithm, Mathematical Biosciences and Engineering, vol. 18, 2021, pp. 3887-3906.

29. H. Mahalingam, T. Veeramalai, A. R. Menon, R. Amirtharajan, Dual-domain image encryption in unsecure medium—a secure communication perspective, Mathematics, vol. 11, 2023, pp. 457.

30. V.S. Miller, Uses of elliptic curves in cryptography, Advances in Cryptology-CRYPTO'85 Proceedings, vol. 218, 1986, pp. 417-426.

31. A. G. Mohamed, N. O. Korany,S. E. El-Khamy, New DNA coded fuzzy based (DNAFZ) S-boxes: Application to robust image encryption using hyper chaotic maps, Ieee Access, vol. 9, 2021, pp.14284-14305.

32. S. Nagaraj, G.S.V.P. Raju, K.K. Rao, Image encryption using elliptic curve cryptography and matrix, Procedia Computer Science, vol. 48, 2015, pp. 276-281.

33. A. A. Neamah, An image encryption scheme based on a seven-dimensional hyperchaotic system and Pascal's matrix, Journal of King Saud University-Computer and Information Sciences, vol. 35, 2023, pp. 238-248.

34. Z.K. Obaidand, N.F.H. Al Saffar, Image encryption based on elliptic curve cryptosystem, International Journal of Electrical and Computer Engineering, vol. 11, 2021, pp. 1293-1302.

35. S. Pankaj, M. Dua, Chaos based Medical Image Encryption Techniques: A Comprehensive Review and Analysis, Information Security Journal: A Global Perspective, vol. 33, 2023, pp. 332-358.

36. P. Parida, C. Pradhan, X.Z. Gao, D.S. Roy, R. Barik, Image encryption and authentication with elliptic curve cryptography and multidimensional chaotic maps, IEEE Access, vol. 9, 2021, pp. 76191-76204.

37. P. L. Sharma, S. Gupta, A. Nayyar, M. Harish, K. Gupta, A. K. Sharma, ECC based novel color image encryption methodology using primitive polynomial, Multimedia Tools and Applications, 2024, pp. 1-40.

38. V. F. Signing, R. T. Mogue, J. Kengne, M. Kountchou, Saïdou, Dynamic phenomena of a financial hyperchaotic system and DNA sequences for image encryption, Multimedia Tools and Applications, vol. 80, 2021, pp.32689-32723.

39. J.H. Silverman, The arithmetic of elliptic curves, Graduate Texts in Mathematics, vol. 106, 2009.

40. L.D. Singh, K.M. Singh, Image encryption using elliptic curve cryptography, Procedia Computer Science vol. 54 , 2015, pp. 472-481.

41. L.D. Singh, K.M. Singh, Medical image encryption based on improved ElGamal scheme, Optik, vol. 147, 2015, pp. 88-102.

42. S. Somaraj, M.A. Hussain, Performance and security analysis for image encryption using key image, Indian Journal of Science and Technology, vol. 8, 2015, pp. 1-4.

43. G. K. Srivastava, P. Singhal, D. Singh, D. Goyal, Chaos based image encryption security in cloud computing, Journal of Discrete Mathematical Sciences and Cryptograpgy, vol. 25, 2022, pp. 1041-1051.

44. X. Wang, X. Du, Chaotic image encryption method based on improved zigzag permutation and DNA rules, Multimedia Tools and Applications, vol. 81, 2022, pp.43777-43803.

45. M. Wang, X. Fu, X. Yan, L. Teng, A new Chaos-based image encryption Algorithm based on Discrete Fourier transform and Improved Joseph Traversal, Mathematics, vol. 12, 2024, pp. 638.

46. J. Wang, X. Zhi, X. Chai, Y. Lu, Chaos-based image encryption strategy based on random number embedding and DNA-level self-adaptive permutation and diffusion, Multimedia Tools and Applications, vol. 80, 2021, pp.16087-16122.

47. L.C. Washington, Elliptic curves number theory and cryptography, Second Ed., Chapman and Hall/CRC, 2008.

48. H. Wen, Y. Lin, Cryptanalysis of an image encryption algorithm using quantum chaotic map and DNA coding. Expert Systems with Applications, vol. 237, 2023, pp. 121514.

49. S. Zhang, L. Liu, A novel image encryption algorithm based on SPWLCM and DNA coding, Mathematics and Computers in Simulation, vol. 190, 2021, pp.723-744.

50. B. Zhang, B. Rahmatullah, S. L. Wang, H. M. Almutairi, Y. Xiao, X. Liu, Z. Liu, A variable dimensional chaotic map-based medical image encryption algorithm with multi-mode, Medical & Biological Engineering & Computing, 2023, pp. 1-32.

51. Q. Zhang, F. Xiang, L. Li, J. Zheng, Image Encryption Algorithm Based on Chaotic System and Cellular Automata, 2023 4th Information Communication Technologies Conference (ICTC), IEEE, 2023, pp. 402-406.

52. Y. Zhou, E. Zhu, S. Li, An image encryption algorithm based on the double time-delay Lorenz system, Mathematical Biosciences and Engineering, vol. 20, 2023, pp. 18491-18522.

53. G. Zhu, W. Wang, X. Zhang, M. Wang, Digital image encryption algorithm based on pixels, IEEE International Conference on Intelligent Computing and Intelligent Systems, 2010, pp. 769-772.

54. X. Zhu, H. Liu, Y. Liang, J. Wu, Image encryption based on kronecker product over finite fields and DNA operation, Optik, vol. 224, 2020, pp. 164725.

55. U. Zia, M. McCartney, B. Scotney, J. Martinez, M. AbuTair, J. Memon, A. Sajjad, Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains, International Journal of Information Security, vol. 21, 2022, pp. 917-935.

56. W. Ramírez, C. Cesarano, S. Díaz, New results for degenerated generalized apostol–bernoulli, apostol–euler and apostol–genocchi polynomials, WSEAS Transactions on Mathematics, vol. 21, 2022, pp. 604-608.

57. C. Cesarano, B. Germano, P. E. Ricci, Laguerre-type Bessel functions. Integral transforms and special functions, vol. 16, 2005, pp. 315-322.

58. W. Ramírez, C. Cesarano, Some new classes of degenerated generalized Apostol-Bernoulli, Apostol-Euler and Apostol-Genocchi polynomials, Carpathian Mathematical Publications, vol. 14, 2022, pp. 354-363.

Shalini Gupta (Corresponding author),
Department of Mathematics & Statistics,
Himachal Pradesh University,
Shimla-171005, India
E-mail address: shalini.garga1970@gmail.com

and

Kritika Gupta,
Lovely Professional University, Phagwara, Punjab - 144411, India
E-mail address: kritika993@gmail.com

and

Nitish,
Department of Mathematics & Statistics,
Himachal Pradesh University,
Shimla-171005, India
E-mail address: nitishthakur151@gmail.com

and

Praveen Agarwal,
Anand International College of Engineering,

Jaipur 303012, India
E-mail address: goyal.praveen2011@gmail.com

and

Shilpi Jain,
Poornima College of Engineering,
Jaipur 302022, India
E-mail address: shilpijain1310@gmail.com