A Robust Scheme for Encrypting Images Using Lorenz chaotic Scheme and Sine Map with gene Coding

Umer Farooq[1], Yawar Azad[2]
[1]Mtech Student, Government College of Engineering and Technology, Chack Bhalwal, Jammu, India
[2]Assistant Professor, Government College of Engineering and Technology, Chack Bhalwal, Jammu, India

Abstract—**For increased security, this research proposes a revolutionary picture encryption system that combines DNA coding with chaotic scrambling. The Lorenz chaotic system's chaotic sequences enable inter-block scrambling, which successfully rearranges picture blocks to produce strong confusion. The sine map then produces pixel value diffusion sequences, in which dynamically chosen rules motivated by chaotic values encode each pixel into a DNA sequence. The final encryption picture is created by decoding after a DNA XOR operation further diffuses the pixel data. To ensure key sensitivity and resistance to plaintext-related attacks, the SHA-512 hash of the plaintext image is used to construct the initial conditions and parameters (y1, y2, y3, y4, y5, y6, σ, ρ, a, m, n). Strong encryption performance is indicated by the experimental findings, which show a uniform histogram distribution, low correlation coefficients, high NPCR and UACI, and almost perfect entropy. The technique is appropriate for secure picture transmission as security evaluations validate its resistance to typical attacks, such as differential, statistical, and chosen plaintext attacks.**

Index Terms—**Image Encryption, Lorenz Hyperchaotic System, Sine Map, DNA Coding, SHA-512, Chaotic Scrambling**

I. INTRODUCTION

Over the past ten years, the quick development of data communication and information processing has drastically changed industries including commerce, healthcare, education, and military. To safeguard sensitive data, these domains depend more and more on safe and effective data transfer. However, protecting data integrity, confidentiality, and authenticity from possible attackers is just one of the many difficulties in guaranteeing data security during transmission over public networks. Data encryption at the source is a more practical and economical way to take advantage of already-existing public network infrastructures, even if encrypting communication channels through private networks is a feasible alternative but comes with significant expenses.

Secure data communication is based on cryptology, which includes cryptography and cryptanalysis. While cryptanalysis assesses how resilient these cryptographic systems are to possible assaults, cryptography entails converting plaintext into ciphertext, making it unreadable to unauthorized parties. The suggested study introduces a unique symmetric cryptographic technique that uses DNA encoding and chaotic systems to provide strong data security. To ensure key sensitivity and unpredictability, the encryption procedure starts with the creation of starting values and system settings based on the input image's SHA-512 hash. Next comes inter-block scrambling, which rearranges picture blocks using chaotic sequences produced by the Lorenz hyperchaotic system, causing a great deal of uncertainty. Then, using dynamically chosen criteria, DNA encoding converts pixel values into DNA sequences, adding even more intricacy. In order to disperse plaintext information across the ciphertext and guarantee great statistical randomness and resistance to differential assaults, the diffusion phase combines chaotic sequences from the sine map with DNA operations. These procedures are reversed in the decryption process, which uses the same chaotic parameters and DNA principles to precisely restore the original data.

As described in his groundbreaking work on the communication theory of secrecy systems, Shannon's concepts of confusion and diffusion are upheld by this cryptographic framework. The originator of information theory, Claude E. Shannon, stated this in his 1949 work "Communication theory of secrecy systems" [1]. Confusion complicates the relationship between the key and the ciphertext [2]. It is difficult to

ascertain the relationship between the input and output when diffusion is present since it completely hides the connection between the plain and encrypted text. The link between the plaintext, ciphertext, and secret key is obscured by the intricate interaction of chaotic sequences and DNA encoding. By using DNA-based and scrambling techniques to distribute pixel values throughout the image, diffusion makes it computationally impossible to undo the change without the right key. Metrics like the Number of Pixels Change Rate (NPCR), Unified Average Changing Intensity (UACI), correlation coefficients, and information entropy are used to validate the security of the suggested system, which is made to withstand cryptanalytic attacks. This ensures that the ciphertext is highly random and independent of the plaintext and key.

This study tackles the increasing need for effective, reliable, and secure cryptographic algorithms that can safeguard sensitive data while it is being sent over public networks by combining chaotic systems with DNA encoding. By providing a complex yet computationally viable method of meeting Shannon's criteria for secure communication, the suggested strategy advances the development of cryptosystems.

II. Chaos in cryptography

According to Edward Lorenz, chaos is a situation in which "The future is determined by the present, but the future is not determined by the approximate present" [1]. Chaos, which comes from the Greek word "Xaos," is a lack of order and predictability that shows itself as complicated, erratic events in both natural and artificial systems, including traffic, weather, and nonlinear dynamics [In paper Strogatz commentary]. Lorenz laid the groundwork for chaos theory in 1963 by identifying the non-periodic and unpredictable character of weather and modeling it using the 3D Lorenz chaotic system [1]. Deterministic systems with sensitive starting condition dependency and aperiodic, long-term behavior are described by chaos theory [2] Chaotic systems are perfect for cryptography because of their aperiodicity, determinism, and sensitivity to beginning circumstances. This allows for the creation of unexpected encryption sequences, which are used in the suggested method using the Lorenz hyperchaotic system and sine map.

Aperiodic long-term behavior, where chaotic trajectories avoid convergence to fixed or periodic orbits, ensuring unpredictability; deterministic nature, which separates chaos from randomness by permitting reproducible trajectories given precise initial conditions; and sensitivity to initial conditions, where slight variations in starting states result in exponentially diverging trajectories, making prediction impossible, are the three main features of chaos that meet cryptographic requirements. Shannon's theories of confusion and diffusion are reflected in these characteristics. While aperiodicity guarantees confusion by hiding the connections between plaintext, ciphertext, and keys, the sensitivity and ergodicity of chaotic systems offer diffusion by spreading initial circumstances throughout chaotic circles. Chaotic systems are perfect for cryptography because of these features, especially when it comes to picture encryption. Chaos-based cryptography increases attack resistance by using nonlinear dynamical systems, including the sine map and Lorenz system, to create pseudo-random sequences for rearranging keys and pixels. This method has shown adaptability in secure communication by being used in a variety of cryptographic structures, such as block and stream ciphers, and data formats, such as text, pictures, and video.

II. Representation in Chaos Theory

Differential equations, like the Lorenz system, and discrete equations are the two main methods used by chaos theory to explain system dynamics.

A. Explicit Equations

Discrete equations use recurrence relations to model the behavior of systems at certain time periods. The status of the system changes as:

$$x_{n+1} = f(x_n)$$

where x_n is the state at the $n - th$ time step, and $f(x_n)$ uses the prior state to define the state transition.

B. Lorenz System Differential Equations

Differential equations use rates of change to explain the development of continuous systems. Continuous changes in system variables over time are modelled by the Lorenz system, a collection of differential equations that may be written as follows:

$$\frac{dy}{dx} = g(x, t)$$

Where $g(x, t)$ controls the ongoing change in the state of the system.

III. Bifurcation diagram

In chaos theory, a bifurcation diagram is a graphical depiction that shows how a system's behavior varies when a control parameter is changed. It displays transitions between several dynamical regimes, including fixed points, periodic cycles, or chaos, by charting the system's stable states, periodic orbits, or chaotic attractors against the parameter.

As the parameter a changes, the sine map, which is defined as $x_{n+1} = a\sin(\pi x_n)$ shows bifurcations. The scheme joins to a stable point for tiny a. The suggested encryption system uses a $a = 0.9$ and higher, where periodic orbits and finally chaotic behavior result from period doubling bifurcations as a grows. A series of period-doubling pathways leading to chaos are depicted in the bifurcation diagram. The Figure 1) shows the bifurcation diagram of sine map.

The Lorenz system exhibits bifurcations mainly with regard to the parameter ρ. It is governed by differential equations $\dot{x} = \sigma\,(y - x)$, $\dot{y} = x\,(\rho - z) - y$, and $\dot{z} = xy - \beta z$. The system stabilizes at fixed places for low ρ. It moves from Hopf bifurcations to periodic orbits and finally to chaotic attractors, as used in the suggested hyperchaotic scrambling, when ρ rises (e.g., $\rho = 28$). The bifurcation diagram shows intricate shifts from order to disorder. The Figure 2) shows the bifurcation diagram of Lorenz system.

IV. Lyapunov Exponent

The Lyapunov exponent, a key indicator of chaotic behavior, quantifies how quickly neighbouring pathways of a dynamical system diverge or converge. Chaos is indicated by a positive Lyapunov exponent, which highlights the system's sensitivity to beginning circumstances by representing the exponential divergence of originally near paths. Periodic behavior is indicated by a zero exponent, but convergence to a stable state is suggested by a negative exponent. The degree of unpredictability in chaotic systems is determined by the dominance of the greatest Lyapunov exponent. Lyapunov exponents are useful for explaining how systems behave over time, particularly in domains like predictability, stability, and chaos. Lyapunov exponents may be used to understand both chaotic systems (with nonzero exponents) and exceptional structures (with zero exponents) [3].

The parameter a determines the Lyapunov exponent for the sine map, which is specified as as $x_{n+1} = a\sin(\pi x_n)$. The suggested encryption scheme's Lyapunov exponent, which is usually between 0.5 and 1, is positive for a = 0.9, demonstrating chaotic behavior brought on by fast trajectory divergence. With parameters of σ = 10, ρ = 28, and β = 8/3, the largest Lyapunov exponent for the 3D Lorenz system, which is governed by $\dot{x} = \sigma\,(y - x)$, $\dot{y} = x\,(\rho - z) - y$, and $\dot{z} = xy - \beta z$, is roughly 0.9, indicating strong chaotic dynamics due to exponential trajectory separation. This increases the security of the proposed chaotic scrambling.

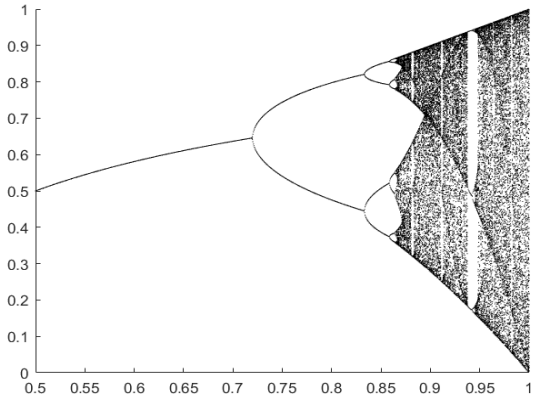


Figure 1: Bifurcation diagram of sine map.

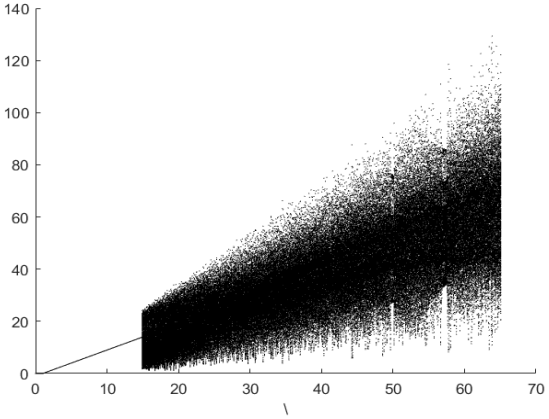
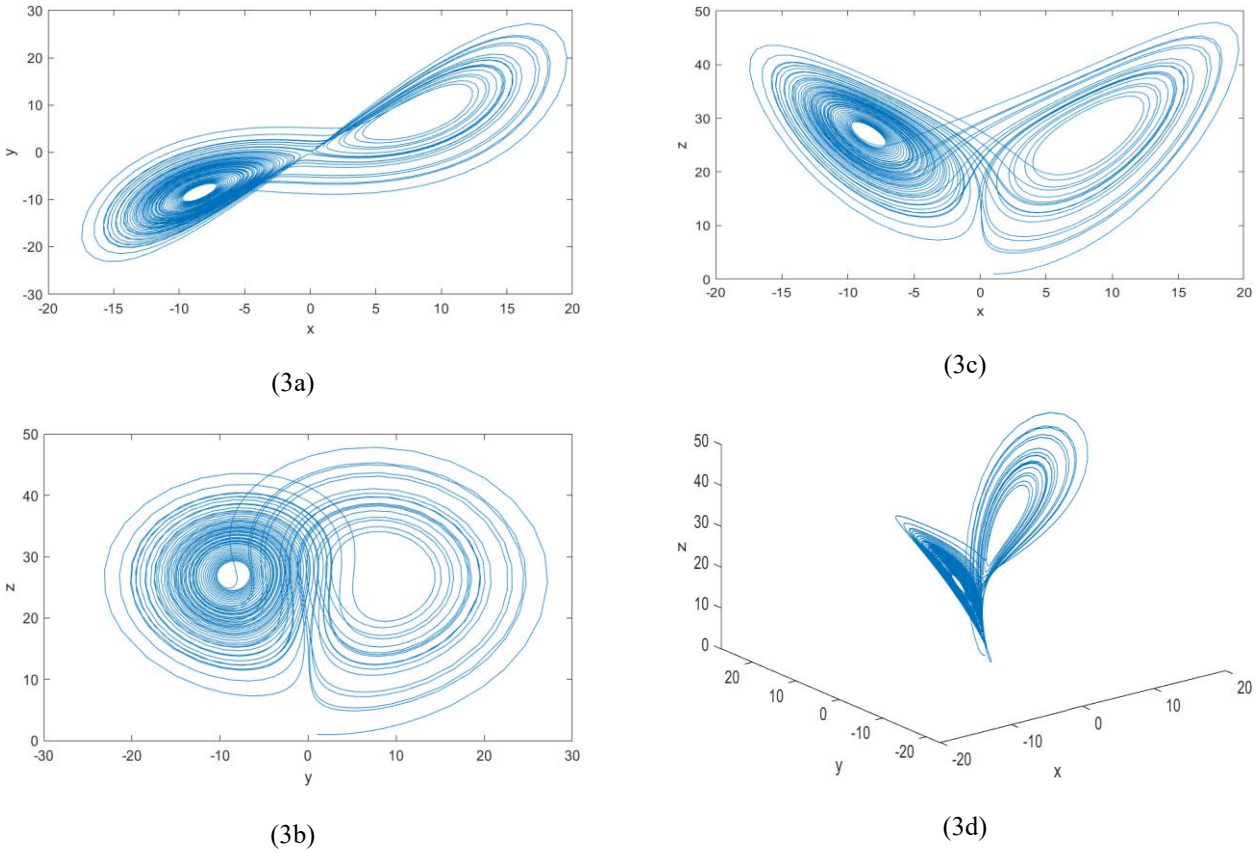


Figure 2: Bifurcation diagram of Lorenz system

Table 1

Length of the key

Algo	Key Space
Suggested	2^{512}
[4]	2^{232}
[5]	2^{299}
[6]	10^{161}



(3a) (3c)

(3b) (3d)

Figure 3: (3a) X-Y segment planetary, (3b) Y-Z segment planetary, (3c) X-Z segment planetary, and (3d) X-Y-Z phase planetary are the attractors of the Lorenz system.

Table 2
Addition operation.

+	T	A	C	G
T	T	A	C	G
A	A	T	G	C
C	C	G	T	A
G	G	C	A	T

Table 3
Subtraction operation

+	T	A	C	G
T	T	A	C	G
A	A	T	G	C
C	C	G	T	A
G	G	C	A	T

Table 4
XOR Operation

⊕	T	A	C	G
T	T	G	A	C
A	G	A	T	C
C	A	T	C	G
G	C	C	G	T

Table 5
XNOR operation

⊙	T	A	C	G
T	A	C	G	T
A	C	A	T	G
C	G	T	A	C
G	T	G	C	A

V. Literature Survey

Hyperchaotic systems are analyzed by Qi et al. [7], who highlight their benefits over regular chaos, including more disorder, wider frequency bandwidths, and multiple positive Lyapunov exponents (LEs). They suggest a novel hyperchaotic system with intricate dynamics, which is confirmed by spectral investigations, Poincaré maps, and bifurcation analysis.

Using logistic maps and dynamic key updates, Ismail et al [8]. provide a chaos-based picture encryption technique that improves security by pixel-wise key change and feedback mechanisms. Results from experiments show that it is resilient to assaults and provides effective real-time encryption for digital photos.

A hyper-chaotic picture encryption system that combines one-round diffusion and pseudo-random key generation is proposed by Norouzi and Mirzakuchaki [9]. By using plaintext-dependent key streams, the technique improves security while guaranteeing robustness and efficiency with high NPCR (>99.80%) and UACI (>33.56%) values.

Yu et al. [10] provide a double-image encryption method that makes use of spatiotemporal chaos (NCML) and DNA insertion/deletion operations. By using mutual encryption and plaintext-dependent key streams, the technique improves security while attaining high sensitivity, resilience to assaults, and increased encryption efficiency.

Zhou and Wang [11] provide a closed-loop block diffusing picture encryption approach created on a conventional hyper-chaotic scheme. With its anti-reconstruction features and plaintext-ciphertext-dependent secret streams, the technique improves security while exhibiting high sensitivity and resilience to assaults.

For picture encryption and pseudo-random bit creation, Volos et al. [12] suggest a unique 1D chaotic map with layered sinusoidal terms and hyperbolic tangent. By using pixel shuffling and XOR operations, the system performs safe encryption, passes NIST testing, and exhibits strong chaotic features.

For safe picture encryption, Gao [13] suggests a 2D hyperchaotic map built from 1D chaotic maps. By using row/column scrambling and bidirectional diffusion to provide strong encryption performance, the method exhibits complicated dynamics using 0-1 testing and Lyapunov exponents.

2. An overview of related techniques

2.1 Sine Map in Chaotic Cryptography

One-dimensional sine maps are frequently used in secure communication systems because they are straightforward yet effective chaotic maps with intricate dynamic behavior. The following is its mathematical formulation as it appears in the suggested encryption scheme:

$$x_{n+1} = a \sin(\pi x_n) \tag{1}$$

where a is the control constraint and $xn \in [0, 1]$ is the state at the n-th iteration. The sine map produces aperiodic, nonconvergent, and extremely sensitive to beginning circumstances chaotic sequences when $a \in [0.87, 1]$ [14]. The suggested system uses $a \in [0.9, 1]$, which is in line with the chaotic regime utilized for diffusion in the encryption process, to guarantee robust chaotic behavior and prevent periodic windows.

2.2 Lorenz chaotic System

A well-known rchaotic system, the Lorenz system, has complicated orbital expansion and folding features that result in complex dynamic behavior. This complexity improves flexibility and security in cryptographic applications by allowing the simultaneous production of numerous pseudo-random sequences. The Lorenz system is perfect for strong encryption algorithms because it provides a wider key space and more resilience to assaults than low-dimensional chaotic systems. The following is its mathematical formulation as it appears in the suggested encryption scheme:

$$\begin{cases} \dot{x} = \sigma (y - x) \\ \dot{y} = x(\rho - z) - y \\ \dot{z} = xy - \beta z \end{cases} \tag{2}$$

where the control parameters are σ, ρ, and β. Aperiodic, unexpected sequences are produced by the system's hyperchaotic behavior when $\sigma = 10$, $\beta = 8/3$, and $\rho \in [24.74, 28.4]$. The suggested approach ensures excellent randomness and security with effective computing efficiency by using $\rho = 28$ to create chaotic attractors for inter-block scrambling. In Figure (3d), the chaotic attractor is displayed.

2.3 The Process and Function of DNA Coding

The tetrad bases that variety up deoxyribonucleic acid (DNA) are adenine (A), thymine (T), cytosine (C), and guanine (G). These nucleotides couple with one another to create complementary pairings, with A pairing with T and C with G. Conferring to Table 6 of the suggested algorithm's DNA coding scheme, each pair of bits in binary representation corresponds to a nucleotide base, producing eight viable encoding rules.

One of the eight encoding rules is used throughout the encryption process to convert the gray value of each 8-bit pixel into a string of four DNA bases. For example, depending on the dynamically chosen rule formed from chaotic sequences created by the sine map, a pixel with a grey value of 69, represented in binary as 01000101, can be encoded as GACT, CAGT, GTCA, CTAG, AGTC, TCAG, ACGT, or TGCA. By utilizing the four DNA operations—addition (+), subtraction (-), XOR, and XNOR—described in Table 2 Table 3, Table 4, Table 5), correspondingly, the suggested method improves security. In order to achieve resilient diffusion, these processes modify DNA sequences. The suggested strategy mainly uses the XOR operation to change pixel data, guaranteeing strong unpredictability and defence against cryptanalytic assaults.

Table 6

Eight predetermined encoding rules are used to map binary pairs to DNA bases.

Rule No.	00	01	10	11
1	A	G	C	T
2	A	C	G	T
3	C	A	T	G
4	C	T	A	G
5	G	A	T	C
6	G	T	A	C
7	T	C	G	A
8	T	G	C	A

3 Encryption and Decryption

The suggested encryption technique secures a grayscale picture of size $M \times N$ by utilizing the confused features of the Lorenz chaotic scheme and the sine map, where N represents the amount of columns and M the amount of rows. Scrambling and diffusion are the two main phases of the procedure, and both make use of unpredictable sequences to improve security.

During the scrambling step, inter-block scrambling is accomplished using disordered orders produced by the Lorenz confused scheme. To achieve considerable confusion, the image is partitioned into blocks of size $m \times n$, which are then reconfigured according to the chaotic sequence to disturb pixel locations. Pixel values are changed during the diffusion stage using chaotic sequences from the sine map. The chaotic sequence determines which of eight dynamically chosen DNA encoding rules is used to initially encode each pixel into a DNA sequence. The encoded sequences are then subjected to a DNA XOR process, which further modifies pixel values to guarantee diffusion. Ultimately, the DNA sequences are decoded back to pixel values, creating a very unpredictable and impenetrable cipher picture.

3.1 Generation of Key and System Initial Value

The suggested approach uses the extremely sensitive SHA-512 hash function to provide strong protection against identified plain-text and selected plaintext outbreaks. The SHA-512 procedure uses the raw picture as input, producing a 128-bit hex string that is then transformed into a 512-bit binary sequence. 16 groups of 32 bits each make up this sequence, which are represented as follows:

$$SK = SK_1 SK_2 \ldots SK_{16} \tag{3}$$

From this key, the following equations are used to determine the block sizes m and n, as well as the beginning conditions and parameters for the Lorenz chaotic system and sine map:

$$\begin{aligned} y_1 &= \frac{\text{bi2de}(SK_1 \oplus SK_2)}{2^{32}} \\ y_2 &= \frac{\text{bi2de}(SK_2 \oplus SK_3)}{2^{32}} \\ y_3 &= \frac{\text{bi2de}(SK_3 \oplus SK_4)}{2^{32}} \\ y_4 &= \frac{\text{bi2de}(SK_4 \oplus SK_{11})}{2^{32}} \\ y_5 &= \frac{\text{bi2de}(SK_5 \oplus SK_{12})}{2^{32}} \\ y_6 &= \frac{\text{bi2de}(SK_6 \oplus SK_{13})}{2^{32}} \end{aligned} \tag{4}$$

$$\sigma = 10 + 5 \times \frac{\text{bi2de}(SK_{14} \oplus SK_{15})}{2^{32}} \tag{5}$$

$$\rho = 28 + 10 \times \frac{\text{bi2de}(SK_{16} \oplus SK_1)}{2^{32}} \quad (6)$$

$$\beta = \frac{8}{3} + 2 \times \frac{\text{bi2de}(SK_2 \oplus SK_3)}{2^{32}} \quad (7)$$

$$a = 0.9 + 0.1 \times \frac{\text{bi2de}(SK_4 \oplus SK_5)}{2^{32}} \quad (8)$$

$$m = \text{mod}(\text{bi2de}(SK_1 \oplus SK_2 \oplus SK_3), 5) + 2 \quad (9)$$

$$n = \text{mod}(\text{bi2de}(SK_2 \oplus SK_5 \oplus SK_7), 5) + 2 \quad (10)$$

If a binary integer is converted to its decimal counterpart by bi2de(x), the XOR operation is shown by $\oplus$, and the modulo action is represented by mod (i, j). In order to provide a safe and dynamic encryption procedure, these parameters (y1, y2, y3, y4, y5, y6, σ, ρ, β, a, m, n) start the chaotic systems and specify the block sizes for scrambling.

3.2 The algorithm that scrambles

The suggested scrambling technique uses confused orders produced by the Lorenz confused scheme to encode a grayscale plain picture P of dimensions $M \times N$. The following are the specific steps:

Step 1: To ensure compatibility with block-based scrambling, the simple picture P of dimensions $M \times N$ is padded to create an image Pb of dimensions $Mb \times Nb$, where M_b and N_b are the closest multiples of block sizes m and n, respectively.

Step 2: The Lorenz chaotic system is iterated $M_b \times N_b$ times to yield three disordered arrangements $X1$, $Y1$, and $Z1$, using starting values y1, y2, and y3 and parameters σ, ρ, and β that are obtained from the SHA512 hash.

Step 3: A scrambling sequence $A1$ is created by processing the chaotic sequence $X1$:

$$A_1 = mod\left(\left\lfloor \frac{|X_1(\text{end}-BLK+1:\text{end})|}{\max(|X_1|)+10^{-10}} \times \text{BLK} \right\rfloor, \text{BLK}\right) \quad (11)$$

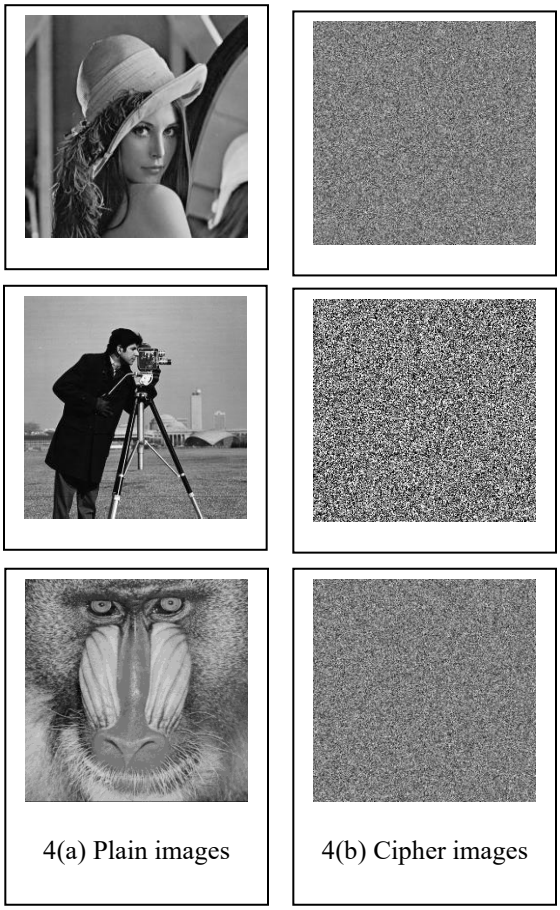
where |X1| indicates the absolute value, floor(x) rounds down x, and X1 ($end - k + 1$: end) chooses the final k components of X and $BLK = \frac{M_b \times N_b}{m \times n}$.

Step 4: The blocks of Pb are rearranged using the permutation indices that are obtained from sorting the sequence $A1$. Furthermore, a seed value is calculated as follows:

$$\text{seed} = mod\left(\sum \left| X_1\left(\text{end} - \frac{M_b \times N_b}{m \times n} + 1 : \text{end}\right)\right|, 2^{32} - 1\right) \quad (12)$$

is used to increase the scrambling effect by performing a pseudo-random shuffle of block indices.

Step 5: To create the scrambled picture Ps of size $M \times N$, the blocks of Pb are reassembled in accordance with the shuffled indices, and the padded pixels are eliminated, thereby confusing the pixel placements.



4(a) Plain images 4(b) Cipher images

Figure 4: Result of Encryption and decryption simulation: 4(a) pictures plain; 4(b) encrypted;

3.3 Generation Diffusion Algorithm

The suggested diffusion technique uses chaotic sequences from the sine map and DNA operations to alter the pixel values of a scrambled picture Ps of dimensions $M \times N$ in order to additional obfuscate the plaintext

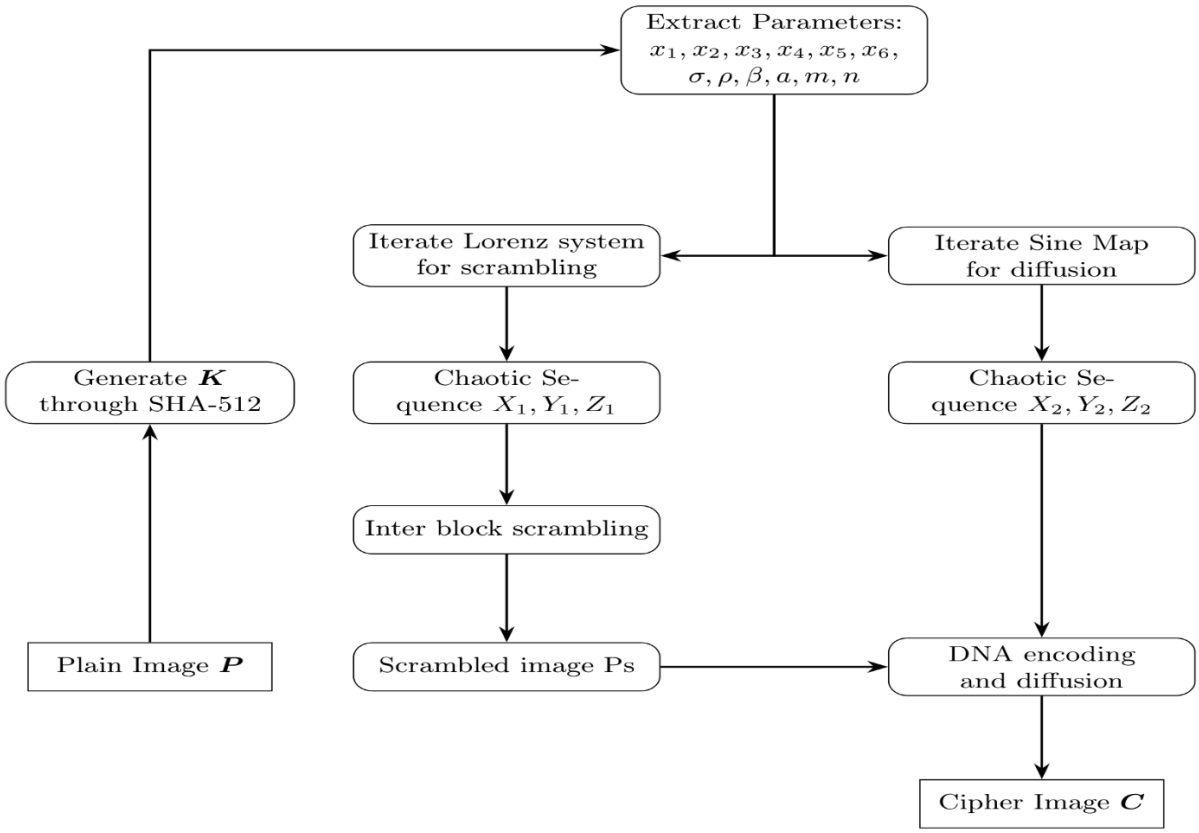


Figure 5: Over all encryption process

information and improve resistance to cryptanalytic assaults. The following are the specific steps:

Step 1: The sine map is iterated $2 \times M \times N$ periods to yield three confused orders $X2$, $Y2$, and $Z2$, using starting values y4, y5, y6, and parameter a.

Step 2: A diffusion sequence F is created by processing the sequence $Z2$:

$$(F = \mathrm{mod}(\lfloor Z_2[MN+1{:}2MN] \times 2^{14} \rfloor, 256)) \quad (13)$$

where floor(x) rounds down once F is transformed into a $M \times N$ matrix.

Step 3: To create an intermediate image $P2$, the picture element of the chaotic image Ps are changed.

$$(P_2(i,j) = \mathrm{mod}(P_s(i,j) + F(i,j), 256)) \quad (14)$$

where the pixel values stay inside the range [0,255] with $i = 1$ to M, $j = 1$ to N.

Step 4: From $X2$, a DNA encoding rule sequence R is produced, chosen from eight DNA encoding rules and reformed into a $M \times N$ matrix (Table 1).

$$R = \mathrm{mod}(\lfloor X_2[MN+1{:}2MN] \times 2^{14} \rfloor, 8) + 1) \quad (15)$$

Step 5: Using the matching rule from R, each picture element of $P2$ is transformed into a DNA arrangement, creating the DNA-encoded picture PD. Likewise, the DNA sequence D is encoded from the sequence F.

Step 6: PD and D are combined using a DNA XOR technique Table 4:

$$C_1(i,j) = PD(i,j) \oplus D(i,j)) \quad (16)$$

where the DNA-diffused sequence $C1$ is found via the DNA $\oplus$.

Step 7: The final cipher picture C of size $M \times N$ is created by decoding the sequence $C1$ back to pixel values using the rule sequence R.

The decryption process reverses these steps using the same chaotic parameters and DNA rules to recuperate the original picture. The encryption flowchart is depicted in Figure 5.

3.4 Decryption Process

Using the identical beginning circumstances and parameters (y1, y2, y3, y4, y5, y6, σ, ρ, β, a, m, n) produced from the SHA-512 hash of the plain-text picture, the proposed technique reverses the encryption stages in the decryption process. Initially, the same dynamically chosen rules from the sine map sequence are used to encode the cipher picture into DNA sequences. To reverse the diffusion, the appropriate sine map chaotic order is used to do the DNA XOR process in reverse. The inverse inter-block scrambling is then carried out by the Lorenz hyperchaotic system, which creates sequences to return the blocks to their initial locations. Ultimately, the simple image is recreated by decoding the DNA sequences back to pixel values. This symmetric technique takes use of the chaotic systems' deterministic character to guarantee precise recovery.

3.5 Pseudocode for Encryption Algorithm

BEGIN ENCRYPTION ALGORITHM
INPUT: Basic picture P of dimensions M × N
1: Generate initial values (y1, y2, y3, y4, y5, y6, sigma, rho, beta, a, m, n) using SHA-512 hash of P
2: Pad P to size Mb × Nb (multiples of m × n) to create padded image Pb
3: Iterate Lorenz system with (y1, y2, y3, sigma, rho, beta) to generate chaotic sequence X1
4: Transform X1 to sequence A1 and sort to get permutation indices for inter-block scrambling
5: Shuffle block indices using A1 and rearrange Pb blocks to create scrambled image Ps
6: Iterate sine map with (y4, y5, y6, a) to generate chaotic sequence Z2
7: Compute diffusion sequence F from Z2 and modify Ps to get P2 using F
8: Encode P2 into DNA sequences using sine map-derived rules
9: Apply DNA XOR operation with F-encoded DNA to diffuse, producing DNA sequence C1
10: Decode C1 to obtain final encrypted image C
OUTPUT: Jumbled image C
END ENCRYPTION ALGORITHM

3.6 Pseudocode for Decryption Procedure

START DECRYPTION ALGORITHM
INPUT: Jumbled picture C of dimensions M × N, same initial values (y1, y2, y3, y4, y5, y6, sigma, rho, beta, a, m, n)
1: Generate initial values (y1, y2, y3, y4, y5, y6, sigma, rho, beta, a, m, n) using SHA-512 hash of original P
2: Pad C to size Mb × Nb (multiples of m × n) to create padded image C_b
3: Iterate sine map with (y4, y5, y6, a) to generate chaotic sequence Z2
4: Encode C into DNA sequences using sine map-derived rules
5: Apply reverse DNA XOR operation with Z2-derived sequence to undo diffusion, getting D1
6: Decode D1 to obtain diffused image P2
7: Iterate Lorenz system with (y1, y2, y3, sigma, rho, beta) to generate chaotic sequence X1
8: Transform X1 to sequence A1 and use inverse permutation indices to unscramble blocks
9: Remove padding from unscramble image to recover plain image P
OUTPUT: Decrypted image P
END DECRYPTION ALGORITHM

4. Safety examination and simulation findings

This segment tests the suggested encryption technique on grayscale photos to assess its security and performance. Visual results and quantitative security measures are used to evaluate the algorithm's efficacy, guaranteeing strong defence against a range of threats.

4.1 Simulation Outcomes

Standard grayscale photographs having a resolution of 256 × 256, such as Lena, Cameraman, Boat, and Baboon, were chosen as examination pictures for assessment. With settings taken from SHA-512, the encryption procedure uses the Lorenz hyperchaotic system for scrambling and the sine map for diffusion. In order to demonstrate successful encryption and precise decoding, Figure 4(a) *Plain images* shows the plain photos, their matching encrypted images, and the decoded picture. The decoded photos are visually similar to the originals, demonstrating the algorithm's reversibility, but the encrypted images show no recognizable patterns, suggesting successful confusion and diffusion.

4.2 Analysis of Key Spaces

An encryption technique is more secure when its key space is wider because it can withstand brute-force attacks better. The suggested approach generates beginning conditions (y1, y2, y3, y4, y5, y6),

parameters for the Lorenz hyperchaotic system (σ, ρ, β), the sine map parameter (a), and block sizes (m, n) built on the SHA-512 hash of the input picture. A 512-bit binary sequence is produced by the SHA-512 hash, giving rise to a key space of 2^{512}. This is far higher than the 2^{100} threshold, which is generally thought to be enough for fending against exhaustive attacks. Table 1 illustrates the suggested algorithm's higher resilience to brute-force assaults by contrasting its key space with those of other encryption algorithms.

4.3 Analysis of key sensitivities

To prevent unwanted access, a strong picture encryption method must be very delicate to its key, meaning that even a little change in the key produces a significantly different decoded image. The key for the suggested approach consists of 12 parameters that are taken from the SHA-512 hash: block sizes (m, n), Lorenz system parameters (σ, ρ, β), initial conditions (y1, y2, y3, y4, y5, y6), and the sine map parameter (a). A grayscale picture is encrypted using the original key set, represented by $\mu 0$, in order to assess key sensitivity. The algorithm's high sensitivity to key changes is then demonstrated by the completely unintelligible picture that results from decrypting the image with a changed key that differs by only one bit. This phenomenon results from the chaotic nature of the sine map and Lorenz system, where even little changes to the parameters or beginning circumstances cause trajectories to diverge rapidly. As a result, decryption yields a random, incomprehensible result in the absence of the precise key, demonstrating the algorithm's strong key sensitivity and resilience to assaults.

4.4 Analysis of Histograms

The histogram of a picture graphically displays the distribution of its pixel values. Uneven grayscale distributions are common in plain photographs, exposing patterns that an attacker might take advantage of. To improve resistance to statistical assaults, an efficient encryption method should provide a cipher picture with a uniform histogram that masks these patterns. The encrypted pictures show a relatively uniform pixel value distribution in the suggested approach, which makes use of the sine map for dissemination and the Lorenz confused scheme for scrambling. The algorithm's resilience against statistical assaults is confirmed by its uniformity, which is made possible by the chaotic sequences and DNA operations. It guarantees that an attacker cannot extract any significant statistical information. Figure 6(a) through 6(h) shows the histogram investigation of red, green and blue (RGB) channel of image 5.1.11.

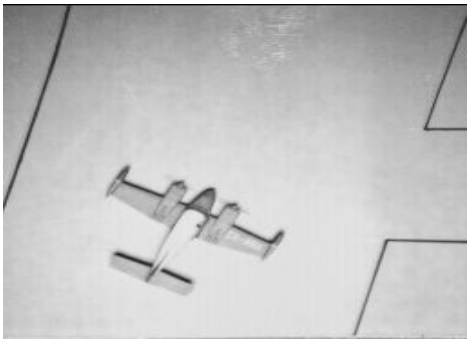


Figure 6 (a): Plain Image 5.1.11.tiff

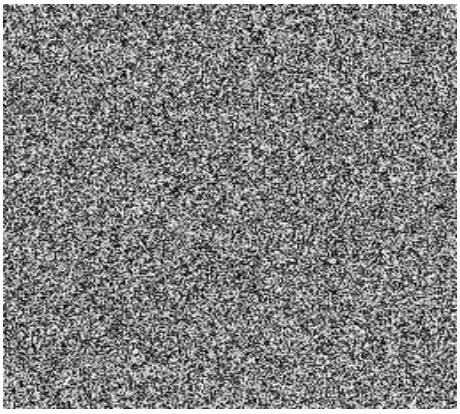


Figure 6 (b): Cipher Image 5.1.11.tiff

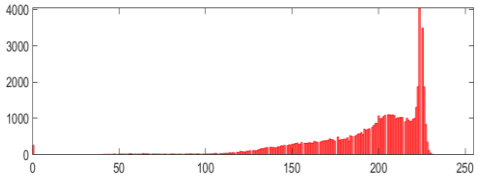


Figure 6 (c): Plain Image - Red Channel

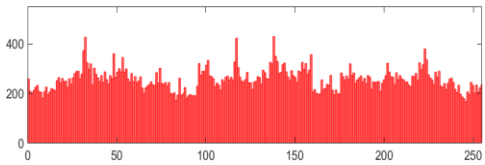


Figure 6 (d): Cipher Image - Red Channel

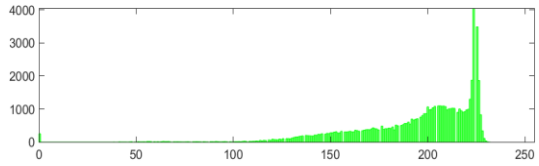


Figure 6 (e): Plain – G- Frequency

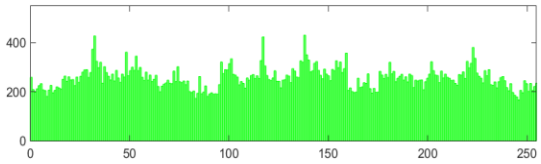


Figure 6 (f): Cipher – G- Frequency

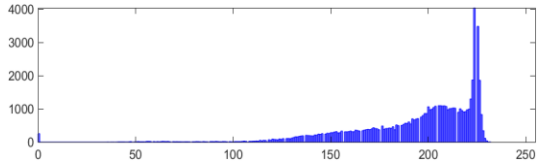


Figure 6 (g): Plain – B-Frequency

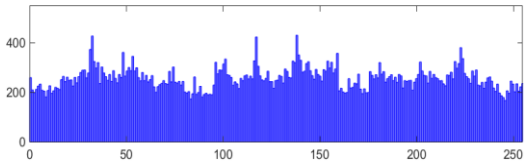


Figure 6 (h): Cipher – B-Frequency

4.5 Analysis of Correlation

Because of their comparable gray values, neighboring pixels in digital photographs frequently show high correlations, which might jeopardize the security of encryption. To withstand statistical assaults, a strong encryption method has to reduce these correlations. The proposed method evaluates the connection between next to pixels in diagonal, vertical, and horizontal dimensions using the Pearson correlation coefficient. It does this by using the Lorenz hyperchaotic system for scrambling and the sine map for diffusion. This is how the correlation coefficient r_{xy} is computed:

$$r_{ab} = \frac{C(a,b)}{\sqrt{D(a)} \cdot \sqrt{D(b)}}) \quad (17)$$

$$C(a,b) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(a))(b_i - E(b)) \quad (18)$$

$$E(a) = \frac{1}{N}\sum_{i=1}^{N}(a_i) \quad (19)$$

$$D(a) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(a))^2 \quad (20)$$

where E(a) and D(a) specify the expectation and variance of a, respectively, $C(a, b)$ is the covariance, N = 8000 is the number of randomly chosen pixel pairs, and a and b are the gray values of two neighbouring picture element. The definitions of the sequences are: Vertically, a = P (a, b), y = P (a, b+1) or P (a, b−1), The vertical formula is a = P (a, b), b = P (a + 1, b), or P (a − 1, b). A diagonal equation is a = P (a, b), b = P (a + 1, a + 1) or P (a − 1, b − 1), where P is the plain or encrypted picture matrix. Strong correlations are shown in all directions for the plain picture (like Lena), but the encrypted image exhibits far lower correlations—nearly zero—because of the chaotic scrambling and DNA-based diffusion. This significant decrease in correlation demonstrates how well the algorithm breaks pixel associations, strengthening defences against statistical assaults. Table 7 lists the correlation test results.

4.6 Differential Outbreak Examination

To prevent differential attacks, a strong picture encryption technique must guarantee that there are noticeable variations between the encrypted and plain images even if just one pixel is changed. A differential attack involves changing certain pixel values in the original picture, converting the different image as well, and then comparing the two to infer details about the encryption process. The suggested. Two important metrics—the (NPCR) and the (UACI)—are used to assess the procedure's flexibility against differential assaults using the Lorenz hyperchaotic system and sine map. These measurements measure the one-pixel difference between two encrypted pictures, $C1$ and $C2$, which are obtained from basic images. The NPCR calculates the proportion of pixels that vary between the two pictures and appears like this:

$$\text{NPCR} = \frac{\sum_{p=1}^{W}\sum_{q=1}^{H}\delta(p,q)}{W \times H} \times 100\% \quad (21)$$

where the picture dimensions is represented by W × H, and δ (p, q) = 1 if S1 (p, q) ≠ S2 (p, q), and δ (p, q) = 0. The UACI, which is defined as follows, measures the regular strength of the variations among the dual images:

$$\text{UACI} = \frac{\sum_{p=1}^{W}\sum_{q=1}^{H}|S_1(p,q) - S_2(p,q)|}{255 \times W \times H} 100\% (22)$$

where the absolute difference in pixel values at location (p, q) is represented by |S1 (p, q) − S2 $(p, q$ |. Strong resistance to differential assaults is indicated by high NPCR and UACI values, which the suggested algorithm accomplishes thanks to its chaotic scrambling and DNA-based diffusion processes. Table 8 and Table 9 shows the NPCR and UACI evaluation with comparison other systems.

Table 7

Original and Cipher Image Correlation Statistics

Image	Plain			Cipher		
	Diagonal	Vertical	Horizontal	Diagonal	Vertical	Horizontal
Lenna	0.9572	0.9848	0.9717	0.0066	-0.0009	-0.0103
cameraman	0.9080	0.9618	0.9264	-0.0121	-0.0026	-0.0001
5.1.09	0.9068	0.9343	0.9029	-0.0312	0.0060	0.0116
5.2.08	0.8608	0.8971	0.9369	-0.0091	-0.0092	-0.0192
5.3.01	0.9674	0.9776	0.9762	-0.0368	-0.0050	-0.0001
Reference [15]	-	-	-	-0.0049	0.0067	0.0006
Reference [14]	0.965935	0.936620	0.915342	0.002383	-0.008576	0.040242

4.7 Info Entropy Examination

Information entropy is a security metric used in encryption methods that measures the randomness and unpredictability of an image's pixel distribution. Greater confusion and improved security are indicated by a higher entropy value, which is produced by a more uniform gray value distribution. According to Shannon [16], the information entropy E (x) is computed as:

$$E(x) = -\sum_{i=0}^{2N-1} q(x_i) \log_2 \left(\frac{1}{q(x_i)}\right) \quad (23)$$

Table 8

(NPCR) evaluation

File Name	NPCR							
	Ref. [17]	Ref.[18]	Ref.[14]	Ref.[19]	Ref.[20]	Ref. [21]	Ref.[22]	Formulated
5.1.09.tiff	99.6064	49.8093	99.6658	99.60	97	-	-	99.78%
5.1.10.tiff	99.6154	99.6140	99.6475	99.61	97	-	-	99.63%
5.1.11.tiff	99.6244	49.8138	99.6674	99.64	96	-	-	99.67%
5.1.12.tiff	99.5703	49.8280	99.5941	99.60	97	-	-	99.80%
5.1.13.tiff	99.6109	99.5972	99.6445	99.63	98	-	-	98.49%
4.2.07.tiff	-	-	-	-	-	-	-	99.76%
Baboon.tiff	-	-	-	-	-	99.63%	-	99.64%
lenna.jpg	-	-	-	-	-	99.62%	99.59%	99.70%
7.1.01.tiff	99.5992	49.8005	99.6273	99.59	-	-	-	99.75%
cameraman	-	-	-	-	-	99.59%	99.69%	99.53%

Table 9
Unified Average Changing Intensity (UACI) evaluation

File Name	UACI							
	Ref. [17]	Ref.[18]	Ref.[14]	Ref.[19]	Ref.[20]	Ref. [21]	Ref.[22]	Formulated
5.1.09.tiff	33.4456	16.6687	33.4425	33.14	96/99	-	-	29.55%
5.1.10.tiff	33.4946	33.5374	33.5366	33.24	99/100	-	-	31.39%
5.1.11.tiff	33.5541	16.7015	33.4398	33.24	97/98	-	-	34.79%
5.1.12.tiff	33.4302	17.0621	33.4228	33.56	96/99	-	-	36.43%
5.1.13.tiff	33.4438	33.6419	33.4205	33.56	97/100	-	-	49.08%
4.2.07.tiff	-	-	-	-	-	-	-	39.17%
Baboon.tiff	-	-	-	-	-	33.41%	-	30.38%
lenna.jpg	-	-	-	-	-	33.45%	33.46%	32.01%
cameraman	-	-	-	-	-	33.40%	33.46%	33.37%

where $q(x_i)$ is the chance that a pixel value x_i will occur; this is calculated by dividing the frequency of mi by the total number of pixels, and for an 8-bit grayscale picture, $N = 8$. High randomness is indicated by an entropy value near 8 bits, which makes it hard for invaders to extract beneficial material. The entropy of encrypted pictures (like Lena) is much greater than that of plain photos in the suggested technique, which makes use of the Lorenz chaotic system and sine map. It also gets near to the ideal rate of 8. This proves that the procedure is very hardy to numerical assaults by exhibiting superior unpredictability when compared to other techniques.

4.8 Generation Peak signal-to-noise ratio (PSNR)

One important measure for evaluating picture quality is the Peak Signal-to-Noise Ratio (PSNR); a lower PSNR value denotes more distortion between the plain and encrypted images, improving security. The following are the definitions of the PSNR and Mean Square Error (MSE):

$$\text{Peak} = 20 \times \log_{10}\left(\frac{255}{\sqrt{\text{Mean}}}\right) \quad (24)$$

$$\text{Mean} = \frac{1}{W \times H}\sum_{i=1}^{W}\sum_{j=1}^{H}\big(P(m,n) - C(m,n)\big)^2 \quad (25)$$

where P(m,n) indicates the pixel value of the plain picture, $C(i, j)$ indicates the picture element of the converted picture, and $W \times H$ is the image's size. To guarantee expressive changes among the basic and encrypted pictures, the suggested technique, which uses the sine map for diffusion and the Lorenz hyperchaotic system for scrambling, requires a large MSE and consequently low PSNR. The results are exposed in Table 10.

Table 10
PSNR and MSE of encrypted image

Image	MSE	PSNR
Lenna	9876.1750	8.1849
Cameraman	10853.6279	7.7751
Baboon	8660.8644	8.7552

VI. Conclusion

The suggested picture encryption technique offers a reliable and effective way to transmit data securely by utilizing the sine map and Lorenz hyperchaotic system. The approach ensures a huge key space of 2^{512} by generating sensitive beginning conditions and parameters using SHA-512, so successfully thwarting brute-force assaults. The beginning conditions and parameters of the Lorenz system and the Sine map, as well as the size of the picture blocks, are intrinsically reliant on the plaintext since the key is formed using the plaintext information. The overall security of the encoding scheme is significantly enhanced by this

high sensitivity to the original picture. While the diffusion phase uses sine map sequences and DNA operations to assure high randomness and uniform pixel distribution, the scrambling phase, which is powered by Lorenz system sequences, creates severe confusion through inter-block rearrangements. The algorithm's resistance to statistical and differential assaults is confirmed by security evaluations, which include histogram uniformity, low correlation coefficients, high NPCR and UACI values, and near-ideal information entropy. Furthermore, substantial distortion is indicated by low PSNR values, which improves security. The algorithm offers a viable method for protecting sensitive visual data in contemporary communication systems due to its computational efficiency and strong performance, which make it appropriate for real-world applications.

REFERENCES

[1] P. G. Baines, "Lorenz, E.N. 1963: Deterministic nonperiodic flow. Journal of the Atmospheric Sciences 20, 130–41.1," 2008. doi: 10.1177/0309133308091948.

[2] S. H. Strogatz, "Notes on the videotape Nonlinear Dynamics and Chaos: Lab Demonstrations."

[3] A. Wilkinson, "What are lyapunov exponents, and why are they interesting?," *Bulletin of the American Mathematical Society*, vol. 54, no. 1, pp. 79–105, 2017, doi: 10.1090/bull/1552.

[4] A. Ur Rehman *et al.*, "A color image encryption algorithm based on one time key, chaos theory, and concept of rotor machine," *IEEE Access*, vol. 8, pp. 172275–172295, 2020, doi: 10.1109/ACCESS.2020.3024994.

[5] X. Wu, H. Kan, and J. Kurths, "A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps," *Applied Soft Computing Journal*, vol. 37, pp. 24–39, Dec. 2015, doi: 10.1016/j.asoc.2015.08.008.

[6] A. Firdous, A. U. Rehman, and M. M. Saad Missen, "A Gray Image Encryption Technique Using the Concept of Water Waves, Chaos and Hash Function," *IEEE Access*, vol. 9, pp. 11675–11693, 2021, doi: 10.1109/ACCESS.2021.3049791.

[7] G. Qi, M. A. van Wyk, B. J. van Wyk, and G. Chen, "On a new hyperchaotic system," *Physics Letters, Section A: General, Atomic and Solid State Physics*, vol. 372, no. 2, pp. 124–136, Jan. 2008, doi: 10.1016/j.physleta.2007.10.082.

[8] I. A. Ismail, M. Amin, and H. Diab, "A Digital Image Encryption Algorithm Based A Composition of Two Chaotic Logistic Maps," 2010.

[9] B. Norouzi and S. Mirzakuchaki, "A fast color image encryption algorithm based on hyper-chaotic systems," *Nonlinear Dyn*, vol. 78, no. 2, pp. 995–1015, Oct. 2014, doi: 10.1007/s11071-014-1492-0.

[10] W. Yu, Y. Liu, L. Gong, M. Tian, and L. Tu, "Double-image encryption based on spatiotemporal chaos and DNA operations," *Multimed Tools Appl*, vol. 78, no. 14, pp. 20037–20064, Jul. 2019, doi: 10.1007/s11042-018-7110-2.

[11] M. Zhou and C. Wang, "A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks," *Signal Processing*, vol. 171, Jun. 2020, doi: 10.1016/j.sigpro.2020.107484.

[12] L. Moysis, I. Kafetzis, C. Volos, A. V. Tutueva, and D. Butusov, "Application of a Hyperbolic Tangent Chaotic Map to Random Bit Generation and Image Encryption," in *Proceedings of the 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus 2021*, Institute of Electrical and Electronics Engineers Inc., Jan. 2021, pp. 559–565. doi: 10.1109/ElConRus51938.2021.9396395.

[13] X. Gao, "Image encryption algorithm based on 2D hyperchaotic map," *Opt Laser Technol*, vol. 142, Oct. 2021, doi: 10.1016/j.optlastec.2021.107252.

[14] Z. Hua, Y. Zhou, C. M. Pun, and C. L. P. Chen, "2D Sine Logistic modulation map for image encryption," *Inf Sci (N Y)*, vol. 297, pp. 80–94, Mar. 2015, doi: 10.1016/j.ins.2014.11.018.

[15] X. Wang and M. Zhao, "An image encryption algorithm based on hyperchaotic system and DNA coding," *Opt Laser Technol*, vol. 143, Nov. 2021, doi: 10.1016/j.optlastec.2021.107316.

[16] C. E. Shannon, "Communication Theory of Secrecy Systems*."

[17] Z. Hua and Y. Zhou, "Image encryption using 2D Logistic-adjusted-Sine map," *Inf Sci (N Y)*, vol. 339, pp. 237–253, Apr. 2016, doi: 10.1016/j.ins.2016.01.017.

[18] X. Liao, S. Lai, and Q. Zhou, "A novel image encryption algorithm based on self-adaptive wave transmission," *Signal Processing*, vol. 90, no. 9, pp. 2714–2722, Sep. 2010, doi: 10.1016/j.sigpro.2010.03.022.

[19] Y. Zhou, L. Bao, and C. L. P. Chen, "Image encryption using a new parametric switching chaotic system," *Signal Processing*, vol. 93, no. 11, pp. 3039–3052, 2013, doi: 10.1016/j.sigpro.2013.04.021.

[20] A. ur Rehman, X. Liao, A. Kulsoom, and S. A. Abbas, "Selective encryption for gray images based on chaos and DNA complementary rules," vol. 74, no. 13, pp. 4655–4677, 2015, doi: doi.org/10.1007/s11042-013-1828-7.

[21] Xiuli Chai, Zhihua Gan, and Miaohui Zhang, "A fast chaos-based image encryption scheme with a novel plain image-related swapping block permutation and block diffusion," vol. 76, pp. 15561–15585, Sep. 2017, Accessed: Jun. 03, 2025. [Online]. Available: https://doi.org/10.1007/s11042-016-3858-4

[22] T. Hu, Y. Liu, L. H. Gong, S. F. Guo, and H. M. Yuan, "Chaotic image cryptosystem using DNA deletion and DNA insertion," *Signal Processing*, vol. 134, pp. 234–243, May 2017, doi: 10.1016/j.sigpro.2016.12.008.