A Secure Image Encryption Framework Using Modified Henon Map with Integrity Verification

Smita Agrawal[1] **and Madhu B R**[2]

[1]*Department of Electronics and Communication Engineering, Jyothy Institute of Technology, Bengaluru, India*
[2]*Department of Artificial Intelligence and Machine Learning, Jyothy Institute of Technology, Bengaluru, India*

Abstract: Unsecured data communication can put the privacy and security of communication parties at risk. Data security aims to safeguard data and stop unauthorized entry and data loss. Securing the transmission of multimedia is a complex task with significant challenges in establishing the security and privacy of sensitive data. A nonlinear encryption framework is proposed here to avert unauthorized image access during transmission. Among nonlinear maps, chaotic maps show a growing and dominant role in the encryption of modern multimedia compared to traditional algorithms. The original Hénon map has a limited chaotic range, so a modified Hénon map is introduced to expand its chaotic range. This map will produce a pseudo-random number, which can be utilized as a key for image diffusion. The modified Hénon map and an image-sensitive cat map are employed in the proposed approach for encryption. Furthermore, the framework incorporates a hash based on the input image to verify its integrity. The suggested security framework provides confidentiality and integrity during transmission. This encryption scheme is simulated on MATLAB, and comparisons are made based on standard performance metrics. Simulation and theoretical examination exemplify the usefulness of the suggested algorithm and prove that this method can be an acceptable choice for secure image transmission.

Keywords: Cryptography, Encryption, Hénon map, Network Security

1. Introduction

Unsecured data communication may compromise the privacy and security of communication parties. As secure communication is vital, coding the messages in an unidentifiable form can be a way to maintain the secrecy and confidentiality of data, even if it falls into the hands of criminals. Confidentiality is critical when safeguarding image content from unauthorized access or disclosure over insecure communication channels [1]. It is vital since shared images may contain sensitive or private information such as personal health details or confidential documents. Therefore, preventing unauthorized entities from accessing and exploiting such information is essential. Encryption is one of the confidentiality measures that help maintain image content secrecy and make it difficult for eavesdroppers to intercept and monitor the transmitted data. Message integrity is another critical aspect of secure image transmission. It means that attackers must not be able to modify the transmitted image, and the received image is in its original form without any changes [2]. This is crucial in various applications such as medical imaging, security surveillance, and scientific research, where the trustworthiness of the shared images is critical. Any unauthorized modification could lead to incorrect diagnoses or unreliable research findings. Thus, maintaining message integrity builds trust in the authenticity of the received images. Cryptographic techniques are a way to achieve secure image transmission, providing confidentiality [3] and hash functions [4] to generate a fixed-size checksum that verifies the integrity or image's genuineness. Chaotic maps [5], [6] can be used to design encryption frameworks to secure image transmission. In Mathematics, chaos is a susceptible dynamical system that looks random but is deterministic [7]. Significant advantages of chaotic systems are high sensitivity to initial conditions, ergodicity, and topological mixing [8]. Many chaos-based maps are used for encryption [8]. Popular maps include the Logistic map, sine map, tent map, Hénon map, Chen chaotic map, and Chua map. However, classical chaotic maps suffer from low-key space or high complexity, leading to modified chaotic maps [9], [10], [11], [12] to expand the range of control parameters and reinforce the sensitivity of secret keys. While these encryption schemes claim to provide security for image transmission, they cannot verify whether the image is intact during transmission and no alteration happened in the image data. Integrity verification can be achieved with the help of Hash functions [13]. Numerous researchers worked on hash algorithms to secure data communication[14], [15], [16]. This paper proposes an image encryption framework with integrity verification for secure image transmission over unsecured public networks. The system uses an improved version of the Hénon map for the diffusion phase and the Discrete Cat Map in the confusion stage for encryption. The input image-based hash generated from SHA-256 verifies the integrity of the message. The improved Hénon map provides a more comprehensive chaotic range and better security when weighed against the classical Hénon map. The paper is structured in the following manner. Basic concepts of chaotic maps and Hash are introduced in Section 2. In Section 3, the paper modifies the Hénon map and analyzes its performance. Section 4 describes the newly proposed image encryption algorithm and showcases the simulation results. Lastly, the paper wraps up with a conclusion in Section 5.

2. Preliminary Concepts

A. Chaotic Maps

Chaotic maps are fascinating mathematical models that exhibit inherent complexity and unpredictability. They have a highly sensitive dependency on their initial conditions, resulting in seemingly random and unpredictable behaviour over time. These maps are often used to study chaos theory, which explores the behaviour of dynamic systems susceptible to their initial conditions. Popular maps are Logistic map, Tent map, Hénon map and many others. The inherent unpredictability of chaotic maps makes them highly usable in designing cryptographic applications[17]. Chaotic maps can be utilized in secure communication through chaos-based encryption schemes. The complex and nonlinear dynamics of chaotic systems are exploited to encrypt messages to increase transmission security. Chaotic encryption techniques improve the resilience of cryptographic systems against various attacks[18]. Despite the potential benefits, it's important to note that using chaotic maps in cryptography requires careful analysis and consideration of the map's properties to ensure robustness and security. Advanced mathematical techniques, such as bifurcation diagrams, Lyapunov exponents, and attractors are used to understand chaotic maps [19], [20], [21].

1) Cat Map

Arnold's Cat Map [22] is a 2D chaotic map used in the chaotic algorithm for encrypting images. By rotating the image continuously, the pixel's position can be changed to convert the image into an unrecognizable form. This scrambling can be achieved by the following matrix transformation :

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \mod N$$

The coordinates of the transformed point are denoted as (x_{n+1}, y_{n+1}), whereas (x, y) represents the original coordinates of a point. The size of the image determines the modulus N. ACM is an area-preserving chaotic map that stretches and folds the image to distort the image. It scrambles the position of the pixels in an image by carefully choosing the parameter p and q. ACM can be iterated to randomize the pixel positions of a square image so that it can be utilized in the confusion stage of encryption. However, if this iteration is done 3N times, the original image will be stored back [23]. Therefore, the number of iterations should be chosen less than 3N to use ACM for image scrambling.

2) Hénon Map

Hénon [24] proposed utilizing the famous two-dimensional Hénon map as a simplified approach for studying the dynamics of the Lorenz system. Equation (1) describes this map.

$$\begin{aligned} x_{n+1} &= 1 - b_1 x_n^2 + y_n \\ y_{n+1} &= b_2 x_n \end{aligned} \tag{1}$$

This nonlinear map is a discrete-time dynamical system and one of the most considered instances of evolving structures exhibiting disordered behavior. It is a nonlinear two-dimensional system, taking a point (x_n, y_n) inside the plane and putting it in a new place (x_{n+1}, y_{n+1}). It converges to a strange attractor when parameters $(b_1, b_2) = (1.4, 0.3)$ [25]. Parameter 'b1' is responsible for the amount of stretching and the parameter 'b2' is responsible for the thickness of folding. This map suffers from low-key space for usage in image encryption. A few modifications [11], [26], [27] were proposed to improve the key space of the Hénon map nevertheless there is still a large scope for improvement in the chaotic range of the map.

B. Hash

Hashing is a mathematical process that generates a fixed-length output for any input size. It is an irreversible process in which no one can recover the original message by using a hash [28]. One of the applications of hash algorithms is to ensure data integrity [29]. It verifies data is unaltered and received in intact form. The secure hashing algorithm (SHA) is a lucrative choice among different hashing algorithms explored by researchers[30], [31]. The SHA-1 algorithm was found to be vulnerable to brute force attacks, prompting the need for a more secure alternative. As a result, SHA-2, including its variants such as SHA-256, has proven to be robust and well-suited for cryptographic use [32]. In this encryption scheme, the hash will be generated using the input image with the SHA256 algorithm and sent to the receiver, which will be imbibed with the original data. While receiving the data, the hash will again calculated by the receiver, and if the calculated and received hash are the same, the integrity of the message is intact.

3. Proposed Hénon Map

As there is a need for improvement in the chaotic range of the classical Hénon map, a novel and improved Hénon map is proposed, with a more comprehensive chaotic range to provide better security to image encryption. This improved Hénon map (IHM) is defined in Equation (2).

$$\begin{aligned} x_{n+1} &= 1 - b_1 (\sin x_n^6)^3 + y_n \\ y_{n+1} &= b_2 x_n \end{aligned} \tag{2}$$

Where 'b1' and 'b2' are control parameters. Figure 2 compares the attractor of the Hénon map and IHM. The

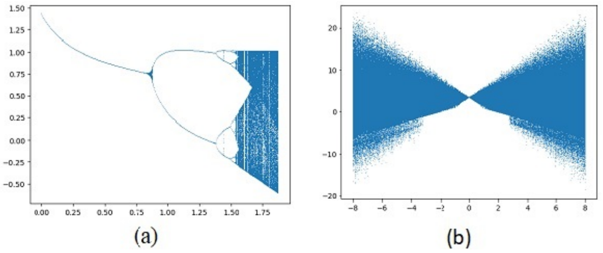

Figure 1. Bifurcation plot: (a) H´enon map, (b) Improved H´enon map

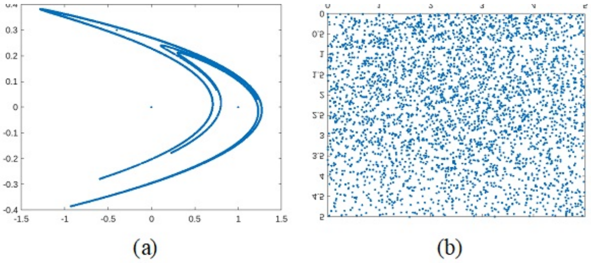

Figure 2. Attractor: (a) H´enon map (b) Improved H´enon map

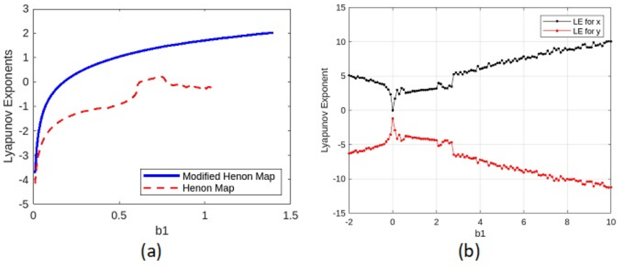

Figure 3. Lyapunov Exponent: (a) H´enon map, (b) Improved H´enon map

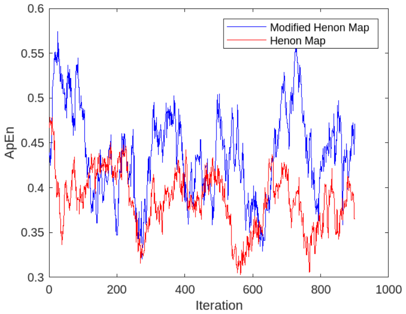

Figure 4. Comparison of approximate entropy

proposed map has a much wider and denser attractor. In this paper, this improved H´enon map will be used to generate a pseudo-random number to be used as key in image encryption. The IHM is evaluated with standard performance indicators.

4. Evaluation of Proposed Map

This section thoroughly assesses the chaotic performance of the newly proposed map through various standard tests and then compares it with the classic Hénon maps.

A. Bifurcation Diagram and Phase Space

The bifurcation diagram and phase space [19] depicts the relationship of chaotic characteristics with its control parameters. The bifurcation diagram and phase space of the H´enon map and proposed IHM is dispalyed in Figure 1 and Figure 2 respectively. Chaos is visible in the H´enon map for a narrow range of b1 $\epsilon[1.06, 1.22] \cup [1.27, 1.29] \cup [1.31, 1.4]$ and b2 = 0.3. The proposed IHM exhibits chaotic properties by varying the parameters b1 as $-8 < b1 < 8$ and b2 = 0.7. The IHM shows chaotic properties for the complete range of the parameter b1 when b2 = 0.7. Therefore proposed IHM has a much wider chaotic range when compared to the H´enon map making it desirable for usage in encryption schemes.

B. Lyapunov Exponent (LE)

In a dynamical system, Lyapunov exponent (λ) characterizes the disengagement of infinitesimally close trajectories [20]. If LE < 0, it represents periodic motion or stable fixed points. When LE > 0, adjacent points diverge exponentially. A chaotic map must have at least one positive LE to exhibit deterministic chaos. Additionally, larger LE exhibits better chaotic characteristics. LE of IHM is shown in Figure 3 with system parameter b1 lying in the range (-8, 8) and b2 = 0.7. A comparison of the Lyapunov exponent of the classical Hénon map and IHM is shown in Figure 3. It is noticed that the proposed IHM exhibits positive LE to ensure its chaotic performance, and the LE of IHM is larger than the classical map for better chaotic dynamics.

C. Approximate Entropy (ApEn)

Approximate entropy (ApEn) measures unpredictable and complex patterns in time series data. It is a metric to measure the randomness present in time series data without knowing the source of the dataset. In a predictable time series, repetitive patterns are present while the absence of repetitive patterns signifies unpredictability [33]. A higher value of ApEn ensures high randomness. A comparison of ApEn for the Hénon map and IHM is shown in Figure 4, indicating higher values for the proposed map which ensures more randomness.

D. 0-1 Test

This test is a method to differentiate between chaotic and regular dynamics. The equation (3) allows us to analyze time series data without needing to know its phase space. where $\beta(n)$ is a single-dimensional time series and n is input to the test and c is fixed in (0, 2π). The plane projected by the p–q plane shows regular dynamics if bounded trajectories are formed. While Brownian-like (unbounded) trajectories imply chaotic dynamics. The mean square displacement can be derived and then the growth rate K is calculated as described by [34]. Regular dynamics shows K = 0 and chaotic dynamics as K = 1 [35].

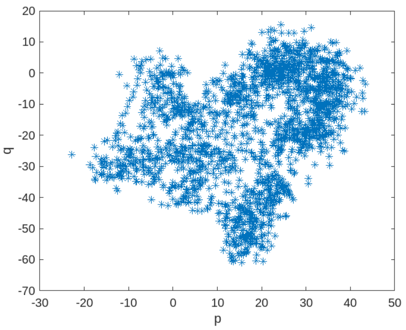

Figure 5. Brownian Motion from IHM

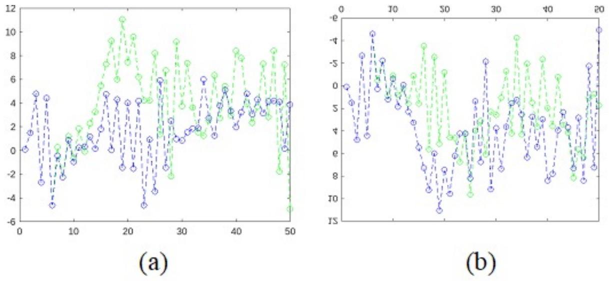

Figure 6. Sensitivity test: (a) Variation in initial conditions (b) Variation in parameter.

$$\begin{aligned} p_{n+1} &= p_n + \beta(n)\cos(nc) \\ q_{n+1} &= q_n + \beta(n)\sin(nc) \end{aligned} \tag{3}$$

The figure 5 shows Brownian-like trajectories of the IHM. The proposed map obtained K as 0.9982 which signifies chaotic dynamics.

E. *Sensitivity to Initial Conditions*

A chaotic map must exhibit high sensitivity to the initial conditions. This feature of the chaotic map can be verified by observing the iterative trajectories after making minute changes in the initial settings of the IHM. Figure 6 shows the iterative trajectory when $a0$ is changed from $a(0)$ to $a(0) + 10^{-15}$ and $x(0)$ is changed from $x(0)$ to $x(0) + 10^{-15}$. It can be observed that the proposed map with minutely different initial settings generates completely different motion trajectories as the iteration progress, ensuring high sensitivity to initial conditions.

5. Encryption Framework using IHM as PRNG Generator

The encryption process encompasses three main stages.

A. *Preprocessing*

The non-square images are converted to a square format. For colour images, the first step involves converting the image to a gray scale representation.

B. *Hash Generation*

In the secondary stage The grey scale image is taken as input to create a hash using the SHA-256 algorithm as per the following steps:

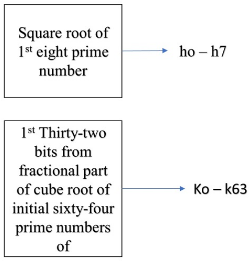
Square root of 1st eight prime number
ho – h7
1st Thirty-two bits from fractional part of cube root of initial sixty-four prime numbers of
Ko – k63

Figure 7. Initialization of Hash values

1) *Initialization*

Eight initial hash values (h_0 to h_7) and 64 additional constants (k_0 to k_{63}) are initialized and the as described in Figure 7.

2) *Processing*

The image data undergoes conversion into 512-bit long chunks and is subjected to 64 operation rounds, as detailed in Algorithm 1. The output of each round serves as the input for the subsequent round. The final hash digest H, consisting of 256 bits, is derived from the output of the last round.

C. *Permutation and diffusion*

The resulting hash H is incorporated into the image's boundary, and the image is then shuffled using a discrete cat map matrix. The shuffling matrix elements are generated by summing the input images and using prime numbers as key set 1 during this shuffling process. This makes the shuffling process dependent on the input image, enhancing the algorithm's security. Key set 2 (initial conditions and control parameter) generates a pseudo-random sequence using the IHM. The shuffled image is then XORed with the integer sequence. This process is outlined in figure 8 and detailed in the following steps:

1. Determine the dimensions of the image I, such that $[\text{row}, \text{column}] = \text{size}(I)$.
2. Compute N as the product of the image dimensions: $N = m \cdot n$.
3. Initialize two zero vectors x and y of length N.
4. For each index i from 2 to N: Update $x(i)$ and $y(i)$ using the Equation 2.
5. Find the absolute value of the integer part of the result of multiplying $x(i)$ and $y(i)$.
6. Perform modulo operation on x with 255.
7. Convert x to binary representation with 8 bits.
8. Set the pseudo-random number sequence as x.
9. Compute the sum of the image I sumI with an additional term accounting for the number of ones.
10. Compute the value a by taking the modulo of sumI with 29 and add the result to 13. Compute the value b by taking the modulo of sumI with 7 and add the result to 47. These steps ensure that the values a and b are derived by

Algorithm 1 Hash Generation Processing Steps

```
Input: Message $M$
Output: Hash value $H$
for each chunk $M_i$ do
    Create a message schedule array $M[0 \ldots 63]$
    for $n = 0$ to 15 do
        $D[n] \leftarrow M_i[n]$
    end for
    for $n = 16$ to 63 do
        $s0 \leftarrow (D[n-15] \gg 7) \oplus (D[n-15] \gg 18) \oplus (D[n-15] \gg 3)$
        $s1 \leftarrow (D[n-2] \gg 17) \oplus (D[n-2] \gg 19) \oplus (D[n-2] \gg 10)$
        $D[n] \leftarrow D[n-16] + s0 + D[n-7] + s1$
    end for
    Initialize $p, q, r, s, t, u, v, w$ with $h_0, h_1, \ldots, h_7$
    for $n = 0$ to 63 do
        $S1 \leftarrow (t \gg 6) \oplus (t \gg 11) \oplus (t \gg 25)$
        $aa \leftarrow (t \wedge u) \oplus ((\neg t) \wedge v)$
        $T1 \leftarrow w + S1 + aa + K[n] + D[n]$
        $S0 \leftarrow (p \gg 2) \oplus (p \gg 13) \oplus (p \gg 22)$
        $bb \leftarrow (p \wedge q) \oplus (p \wedge r) \oplus (q \wedge r)$
        $T2 \leftarrow S0 + bb$
        $h \leftarrow v$
        $g \leftarrow u$
        $f \leftarrow t$
        $e \leftarrow s + T1$
        $d \leftarrow r$
        $c \leftarrow q$
        $b \leftarrow p$
        $a \leftarrow T1 + T2$
    end for
    $h_0 \leftarrow h_0 + p$
    $h_1 \leftarrow h_1 + q$
    $h_2 \leftarrow h_2 + r$
    $h_3 \leftarrow h_3 + s$
    $h_4 \leftarrow h_4 + t$
    $h_5 \leftarrow h_5 + u$
    $h_6 \leftarrow h_6 + v$
    $h_7 \leftarrow h_7 + w$
end for
Return hash H $(h_0, h_1, h_2, h_3, h_4, h_5, h_6, h_7)$
```

applying a modular arithmetic operation on the sum of the elements of the image, followed by an addition of constant offsets. This technique is used to generate key-dependent parameters for subsequent steps in the encryption process.
11. Construct the permutation matrix P as follows:

$$P = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix}$$

12. For each pixel position (i, j) within the image dimensions:
a. Compute the new position M using the permutation matrix P:

$$M = 1 + \text{mod}(P \times \begin{bmatrix} i \\ j \end{bmatrix}, \text{row})$$

b. Reassign the pixel values in the shuffled image: $I(M(1), M(2)) = I(i+1, j+1)$.
13. Reshape the shuffled image to a vector of length N.
14. Convert shuffled image to 8 bit binary .
15. Perform bit wise XOR operation between pseudo random number generated in step 8 with shuffled image .
16. Convert this back to decimal.
17. Reshape back to its original dimensions $m \times n$.
18. Recalculate the sum sumI for the diffused image as in step 9.
19. Update values of a and b using prime numbers as in step 10.
20. Construct the new permutation matrix P:

$$P = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix}$$

21. Repeat step 12 to 17 with new matrix. The output is the encrypted image.

6. Decryption

The encryption process is reversed to decrypt the image outlined in the Figure 9. Subsequently, the hash is extracted from the image boundary and compared to ensure integrity at the receiver's end. When the hash matches, it signifies that the image has remained confidential and integrity is intact during transmission. Any mismatch indicates image corruption.

7. Performance Evaluation of Proposed Encryption Framework

To test the strength of the proposed encryption framework, simulations are carried out using MATLAB, using some sample images taken from the USC-SIPI database. These sample images are encrypted using the proposed encryption framework. The key set 1 used for encryption are prime numbers, and keyset 2 are initial conditions as 0.1 and 0.2, and parameters are 4.75 and 0.7. The simulation results show that all ciphered images are unrecognizable and noise-like. The encrypted images are tested against standard parameters and compared with the classical Hénon Map.

A. Visual Analysis

Figure 10 illustrates encryption and decryption results performed on sample image. It is easily visible that it is not feasible to conclude any meaningful information by using encrypted images.

B. Histogram Analysis

The graph containing the pixel intensity values of any image is called a histogram. The ciphered image must contain an invariant scattering of pixels and must be completely different from the plain image value. A good image encryption framework encrypts the plain text image to a random look alike so that the histogram for the cipher image

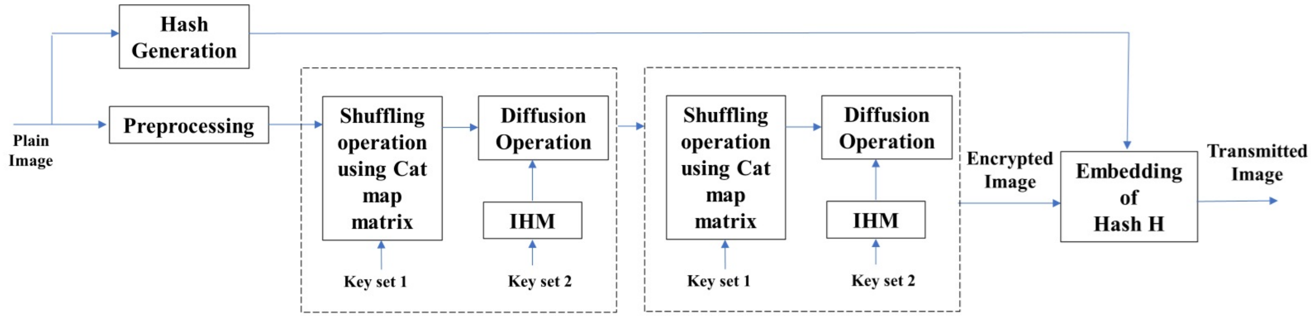

Figure 8. Flow chart for encryption

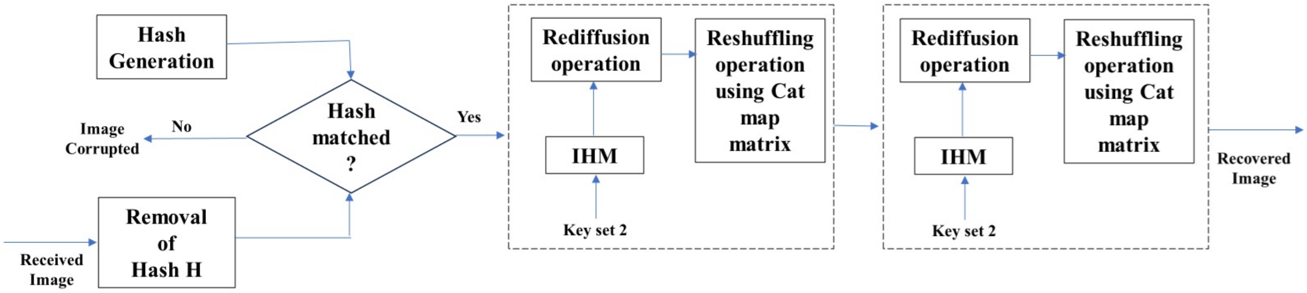

Figure 9. Flow chart for decryption

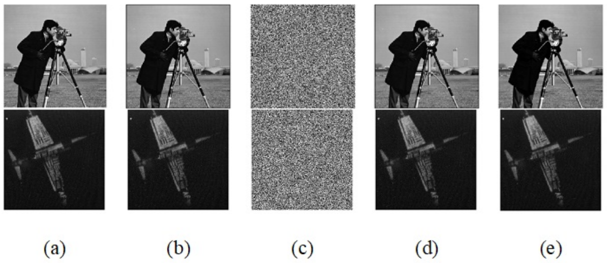

Figure 10. (a) Original image, (b) Original image with Hash, (c) Encrypted image, (d) Decrypted images with Hash, (e) Decrypted image after removal of Hash from the boundary. First-row cameraman image, second-row aeroplane image.

will be uniformly distributed [36]. Figure 11 shows the histogram of plain and encrypted images. It is evident that the histogram of the encrypted image is entirely different from the original image and pixel values are uniformly distributed therefore no attackers can use any data from the cipher image to start any statistical attack on this cryptosystem.

C. *Entropy Analysis*

The level of randomness in the image can be used to assess the strength of any encryption system. 8 is the perfect entropy value for an 8-bit image. The entropy for a robust encryption system should be as close to 8 as possible [36]. Table I illustrates the entropy of plain and encrypted images and same is compared with recent works in Table II. It is evident from the tables that the information entropy of the ciphered image is approximately approaching the ideal value. This clarifies the generation of random-looking encrypted images. Thus, it is obvious that the proposed scheme can provide security against attacks based on information entropy.

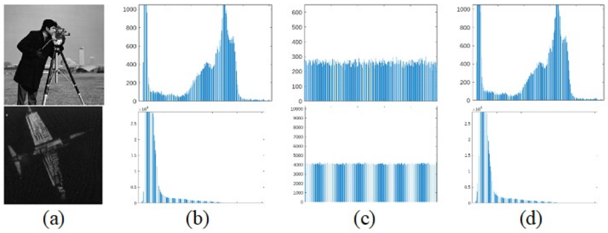

Figure 11. (a) Original image, (b) Histogram of original image, (c) Histogram of encrypted image, (d) Histogram of decrypted image. First-row cameraman image, second-row aeroplane image.

D. *Correlation Analysis*

The encryption framework must break the strong correlations among neighbouring pixels. An image with a low correlation value can resist statistical attacks[41]. Figure 12 shows a correlation graph of the plain and encrypted images in horizontal, vertical, and diagonal directions. Equation (4) calculate the correlation $\sigma(A, B)$ between two neighboring pixels A and B. where a_i and b_i are the individual data

TABLE I. Entropy of original and encrypted images

Image	Original	Encrypted
Cameraman	7.0246	7.9971
Lena	7.5749	7.9974
Peppers	7.5789	7.9994
5.01.09	6.7229	7.9976
5.01.10	6.7229	7.9976
5.01.11	6.4627	7.9969
5.01.11	6.4627	7.9969
7.01.01	6.0489	7.9994
7.01.02	4.0418	7.9993
7.01.03	5.5212	7.9993
7.01.04	6.1144	7.9993
1.03.01	7.449	7.9998
1.03.02	7.3717	7.9998
1.03.03	7.3034	7.9999
1.03.03	7.2763	7.9998

TABLE II. Comparison of entropy for Lena image

Reference	[26]	[37]	[38]	[39]	[40]	Proposed
Entropy	7.9974	7.9975	7.9980	7.9975	7.9993	7.9971

TABLE III. Comparison of correlation coefficient of original and encrypted Images

Image	Original			Encrypted		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Cameraman	0.9335	0.9592	0.9087	-0.0049	0.0008	0.003
Lena	0.9401	0.9695	0.918	-0.0055	0.0027	-0.0023
Peppers	0.9792	0.9826	0.968	-0.0019	-0.0013	0.0011
5.01.09	0.902	0.939	0.9037	0.0025	-0.0071	0.0031
5.01.10	0.902	0.939	0.9037	0.0025	-0.0071	0.0031
5.01.11	0.9571	0.9366	0.8927	0.0025	-0.0023	0.0018
5.01.12	0.9571	0.9366	0.8927	0.0025	-0.0023	0.0018
7.01.01	0.962	0.9205	0.9074	-0.003	0.0016	0.0023
7.01.02	0.9463	0.9459	0.8962	-0.0012	0.0011	-0.0017
7.01.03	0.9456	0.9321	0.9017	0.0008	0.002	0.0022
7.01.04	0.9768	0.9675	0.9559	-0.0016	-0.0016	0.0036
1.3.01	0.9126	0.9258	0.8641	-0.0013	-0.0005	0.0009
1.3.02	0.9448	0.9494	0.9162	0.0016	-0.0001	0.0015
1.3.03	0.9177	0.9682	0.8784	-0.0003	-0.0008	-0.0006
1.3.04	0.8213	0.8618	0.7748	-0.001	0.0004	-0.0002

TABLE IV. **Comparison of correlation coefficient for Lena image**

Reference	Encrypted Image		
	Horizontal	Vertical	Diagonal
[26]	0.0032	-0.0016	0.0023
[37]	0.0058	-0.0024	0.0012
[38]	0.0082	-0.0032	-0.0025
[39]	-0.0148	0.0106	0.0134
[40]	0.0048	-0.0020	-0.0027
Proposed	-0.0001	0.0004	-0.0002

points, $\overline{A}$ and $\overline{B}$ are the mean values of A and B, and M is the number of data points. Table III shows correlation coefficients of the plain image and encrypted image for some sample images for the proposed framework with IHM and compared with recently proposed work in Table IV. It can be easily observed that while the original image is tightly correlated, the correlation among neighbouring pixels in the ciphered image is completely broken.

$$\sigma(A,B) = \frac{\sum_{i=1}^{M}(a_i - \overline{A})(b_i - \overline{B})}{\sqrt{\sum_{i=1}^{M}(a_i - \overline{A})^2}\,\sqrt{\sum_{i=1}^{M}(b_i - \overline{B})^2}} \tag{4}$$

E. Key Space and Key Sensitivity

Key space is the number of possible assorted keys utilized within the encryption framework. Key space is considered the most crucial feature of the security framework. The key space must be sufficiently broad and massive to withstand the brute force attack. The proposed encryption algorithm has a vast key set that includes key set1, used at the confusion stage and key set2, used at the diffusion stage. Along with the giant key space, the encryption framework must be susceptible to encryption keys. In the proposed encryption framework, slight changes are made to the IHM keys used to decrypt the images. The figure 6 shows the resulting decrypted image using the original and slightly changed keys. It verifies that decryption of the image is not possible even with slightly different keys.

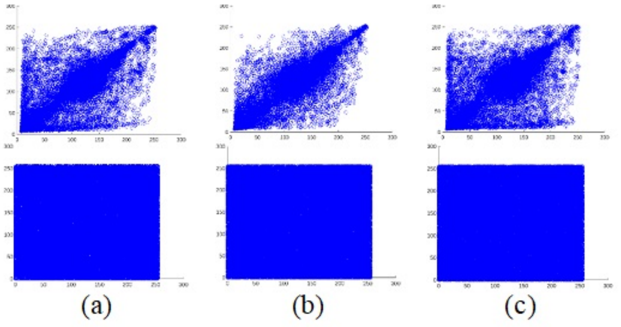

Figure 12. Correlation plot: first-row original image, second-row encrypted image in horizontal, vertical, and diagonal directions.

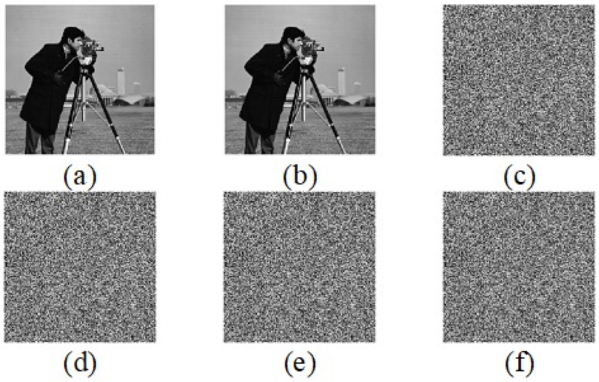

Figure 13. Sensitivity test. (a) Original image, (b) - (g) Decryption result. (b) With Correct keys (c) - (g) By altering x(0), y(0), b1, b2.

F. *Differential Attacks*

Differential attacks are prevalent in which attackers get illegal access to the cryptographic mechanism and attempt to obtain the cipher image with no information of keys. To avert the differential attack, The encryption method must ensure that even a one-pixel change in a plain image significantly alters the encrypted image. When a single pixel undergoes alteration, the impact on the original image is determined by NPCR and UACI. NPCR measures the percentage of modified pixels between the unencrypted and encrypted images. Meanwhile, UACI assesses the average difference in intensity between the plain and cipher images. It is often considered that an NPCR value exceeding 99 % and UACI approximately at 33 % indicate high resilience to differential attacks [42]. The proposed framework exhibits NPCR and UACI values that closely match the ideal requirements for various images, as illustrated in Table V, and is compared with recently suggested techniques in Table VI.

TABLE V. NPCR and UACI values for different images

Image	NPCR	UACI
Cameraman	99.5959	33.4487
Lena	99.6214	33.5681
Peppers	99.6109	33.4694
5.01.09	99.6334	33.5092
5.01.10	99.6334	33.5092
5.01.11	99.6605	33.5525
5.01.11	99.6605	33.5525
7.01.01	99.5999	33.4091
7.01.02	99.5829	33.4205
7.01.03	99.6132	33.4007
7.01.04	99.6234	33.4492
1.03.01	99.6072	33.4935
1.03.02	99.6118	33.4485
1.03.03	99.6153	33.4413
1.03.03	99.6029	33.4538

TABLE VI. Comparison of plain-text differential analysis

Method	[26]	[37]	[38]	[39]	[40]	Proposed
NPCR	99.6139	99.60	99.6150	99.5041	99.5650	99.6056
UACI	33.5316	33.45	33.4205	33.4238	33.4551	33.4975

G. *Known-Plain and Chosen-Plain Attacks*

The key is obtained by utilizing all-white or all-black images. A collection of 256*256 all-black and all-white images is utilized and encrypted using the suggested algorithm. The histogram, correlation coefficient, and information entropy are determined and displayed in Table **??** and Figure 14. The encrypted images resemble noise and do not contain understandable information, ensuring the system is sufficiently protected from known plaintext and ciphertext attacks.

8. Conclusion

This study introduces an enhanced version of the Hénon map to expand the chaotic range of the conventional Hénon Map for application in image encryption. The modified map is derived by altering the original Hénon map. The bifurcation diagram, Lyapunov exponent, correlation coefficients, and trajectory produced by this map are assessed and compared with those of the classical Hénon map. Notably, the IHM demonstrates a more extensive chaotic range, resulting in highly unpredictable outputs. This IHM is subsequently employed in creating an encryption framework, where ACM is utilized to scramble the image, and the PRN generated from IHM is XORed with the scrambled image. The framework's security is validated through standard tests and comparisons with various recently proposed schemes to assess its effectiveness against popular attack methods. The encryption framework boasts ample key space and is highly sensitive to its keys. Encrypted images exhibit a minimal correlation between neighbouring pixels and possess an entropy value close to the ideal. The histogram displays a uniform distribution, and the UACI and NPCR metrics approach their ideal values. These findings validate the potential of the suggested framework for secure image communications. It is tailored for square greyscale images and can be adapted with colour images.

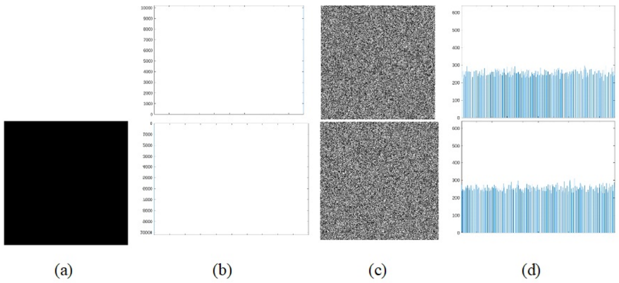

Figure 14. (a) and (b) Original image and its histogram, (c) and (d) Encrypted image and its histogram. First row all white image and second row all black image.

TABLE VII. Attacks Test Result

Image	Horizontal	Vertical	Diagonal	Entropy (Encrypted)	NPCR	UACI
All White	-0.0020	-0.0022	-0.0032	7.9969	99.6169	33.5531
All Black	0.0048	0.0012	0.0051	7.9973	99.6475	33.4281

References

[1] M. SaberiKamarposhti, A. Ghorbani, and M. Yadollahi, "A comprehensive survey on image encryption: Taxonomy, challenges, and future directions," *Chaos, Solitons & Fractals*, vol. 178, p. 114361, 2024.

[2] P. Williams, I. K. Dutta, H. Daoud, and M. Bayoumi, "A survey on security in internet of things with a focus on the impact of emerging technologies," *Internet of Things*, vol. 19, p. 100564, 2022.

[3] J. Selvaraj, W.-C. Lai, B. P. Kavin, and G. H. Seng, "Cryptographic encryption and optimization for internet of things based medical image security," *Electronics*, vol. 12, no. 7, p. 1636, 2023.

[4] R. Han, "A hash-based fast image encryption algorithm," *Wireless Communications and Mobile Computing*, vol. 2022, 2022.

[5] N. Nagaraj, "The unreasonable effectiveness of the chaotic tent map in engineering applications," *Chaos Theory and Applications*, vol. 4, no. 4, pp. 197–204, 2022.

[6] A. ASHİSH, A. MALİK *et al.*, "Dynamical interpretation of logistic map using euler's numerical algorithm," *Chaos Theory and Applications*, vol. 4, no. 3, pp. 128–134, 2022.

[7] D. Blackmore, "The mathematical theory of chaos," in *Symmetry*. Elsevier, 1986, pp. 1039–1045.

[8] B. Zhang and L. Liu, "Chaos-based image encryption: Review, application, and challenges," *Mathematics*, vol. 11, no. 11, p. 2585, 2023.

[9] L. Moysis, A. Tutueva, C. Volos, D. Butusov, J. M. Munoz-Pacheco, and H. Nistazakis, "A two-parameter modified logistic map and its application to random bit generation," *Symmetry*, vol. 12, no. 5, p. 829, 2020.

[10] S. E. Borujeni, M. S. Ehsani *et al.*, "Modified logistic maps for cryptographic application," *Applied Mathematics*, vol. 6, no. 05, p. 773, 2015.

[11] H. Zhao, S. Xie, J. Zhang, and T. Wu, "A dynamic block image encryption using variable-length secret key and modified henon map," *Optik*, vol. 230, p. 166307, 2021.

[12] A. Iatropoulos, L. Moysis, A. Giakoumis, C. Volos, A. Ouannas, and S. Goudos, "Medical data encryption based on a modified sinusoidal 1d chaotic map and its microcontroller implementation," in *2021 10th International Conference on Modern Circuits and Systems Technologies (MOCAST)*. IEEE, 2021, pp. 1–4.

[13] A. M. Ali and A. K. Farhan, "A novel improvement with an effective expansion to enhance the md5 hash function for verification of a secure e-document," *IEEE Access*, vol. 8, pp. 80 290–80 304, 2020.

[14] F. E. De Guzman, B. D. Gerardo, and R. P. Medina, "Implementation of enhanced secure hash algorithm towards a secured web portal," in *2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS)*. IEEE, 2019, pp. 189–192.

[15] H. Cheng, D. Dinu, and J. Großschädl, "Efficient implementation of the sha-512 hash function for 8-bit avr microcontrollers," in *Innovative Security Solutions for Information Technology and Communications: 11th International Conference, SecITC 2018, Bucharest, Romania, November 8–9, 2018, Revised Selected Papers 11*. Springer, 2019, pp. 273–287.

[16] J. S. Teh, M. Alawida, and J. J. Ho, "Unkeyed hash function based on chaotic sponge construction and fixed-point arithmetic," *Nonlinear Dynamics*, vol. 100, no. 1, pp. 713–729, 2020.

[17] A. Belazi, S. Kharbech, M. N. Aslam, M. Talha, W. Xiang, A. M. Iliyasu, and A. A. Abd El-Latif, "Improved sine-tangent chaotic map with application in medical images encryption," *Journal of Information Security and Applications*, vol. 66, p. 103131, 2022.

[18] A. Sarkar, S. R. Chatterjee, and M. Chakraborty, "Role of cryptography in network security," *The" essence" of network security: an end-to-end panorama*, pp. 103–143, 2021.

[19] S.-N. Chow and J. K. Hale, *Methods of bifurcation theory*. Springer Science & Business Media, 2012, vol. 251.

[20] H. D. Abarbanel, R. Brown, and M. Kennel, "Lyapunov exponents in chaotic systems: their importance and their evaluation using observed data," *International Journal of Modern Physics B*, vol. 5, no. 09, pp. 1347–1375, 1991.

[21] E. Ott, "Strange attractors and chaotic motions of dynamical systems," *Reviews of Modern Physics*, vol. 53, no. 4, p. 655, 1981.

[22] V. I. Arnold and A. Avez, "Ergodic problems of classical mechanics," *(No Title)*, 1968.

[23] F. J. Dyson and H. Falk, "Period of a discrete cat mapping," *The American Mathematical Monthly*, vol. 99, no. 7, pp. 603–614, 1992.

[24] M. Hénon, "A two-dimensional mapping with a strange attractor," *The theory of chaotic attractors*, pp. 94–102, 2004.

[25] S. Amoh, X. Zhang, G. Chen, and T. Ueta, "Bifurcation analysis of a class of generalized hénon maps with hidden dynamics," *IEEJ Transactions on Electrical and Electronic Engineering*, vol. 16, no. 11, pp. 1456–1462, 2021.

[26] J. Wu, X. Liao, and B. Yang, "Image encryption using 2d hénon-sine map and dna approach," *Signal processing*, vol. 153, pp. 11–23, 2018.

[27] S. Sheela, K. Suresh, and D. Tandur, "Image encryption based on modified henon map using hybrid chaotic shift transform," *Multimedia Tools and Applications*, vol. 77, pp. 25 223–25 251, 2018.

[28] L. Chi and X. Zhu, "Hashing techniques: A survey and taxonomy," *ACM Computing Surveys (Csur)*, vol. 50, no. 1, pp. 1–36, 2017.

[29] L. V. Cherckesova, O. A. Safaryan, N. G. Lyashenko, and D. A. Korochentsev, "Developing a new collision-resistant hashing algorithm," *Mathematics*, vol. 10, no. 15, p. 2769, 2022.

[30] P. Luo, Y. Fei, L. Zhang, and A. A. Ding, "Differential fault analysis of sha3-224 and sha3-256," in *2016 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*. IEEE, 2016, pp. 4–15.

[31] B. U. I. Khan, R. F. Olanrewaju, M. A. Morshidi, R. N. Mir, M. L. B. M. Kiah, and A. M. Khan, "Evolution and analysis of secured hash algorithm (sha) family," *Malaysian Journal of Computer Science*, vol. 35, no. 3, pp. 179–200, 2022.

[32] A. W. Appel, "Verification of a cryptographic primitive: Sha-256," *ACM Transactions on Programming Languages and Systems (TOPLAS)*, vol. 37, no. 2, pp. 1–31, 2015.

[33] S. M. Pincus, "Approximate entropy as a measure of system complexity." *Proceedings of the National Academy of Sciences*, vol. 88, no. 6, pp. 2297–2301, 1991.

[34] G. A. Gottwald and I. Melbourne, "A new test for chaos in deterministic systems," *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, vol. 460, no. 2042, pp. 603–611, 2004.

[35] ——, "The 0-1 test for chaos: A review," *Chaos detection and predictability*, pp. 221–247, 2016.

[36] U. Zia, M. McCartney, B. Scotney, J. Martinez, M. AbuTair, J. Memon, and A. Sajjad, “Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains,” *International Journal of Information Security*, vol. 21, no. 4, pp. 917–935, 2022.

[37] X. Li, J. Mou, L. Xiong, Z. Wang, and J. Xu, “Fractional-order double-ring erbium-doped fiber laser chaotic system and its application on image encryption,” *Optics & Laser Technology*, vol. 140, p. 107074, 2021.

[38] D. H. ElKamchouchi, H. G. Mohamed, and K. H. Moussa, “A bijective image encryption system based on hybrid chaotic map diffusion and dna confusion,” *Entropy*, vol. 22, no. 2, p. 180, 2020.

[39] Y. Zhang, “A new unified image encryption algorithm based on a lifting transformation and chaos,” *Information sciences*, vol. 547, pp. 307–327, 2021.

[40] X. Wang, J. Yang, and N. Guan, “High-sensitivity image encryption algorithm with random cross diffusion based on dynamically random coupled map lattice model,” *Chaos, Solitons & Fractals*, vol. 143, p. 110582, 2021.

[41] L. Abraham and N. Daniel, “Secure image encryption algorithms: A review,” *International journal of scientific & technology research*, vol. 2, no. 4, pp. 186–189, 2013.

[42] Y. Wu, J. P. Noonan, S. Agaian *et al.*, “Npcr and uaci randomness tests for image encryption,” *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT)*, vol. 1, no. 2, pp. 31–38, 2011.