Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
DOI : 10.47974/JIOS-2160

A multi-layered image encryption framework using Henon chaos and Reframed RSA

Abhishek *
Ruchi Sehrawat †
University School of Information, Communication & Technology
Guru Gobind Singh Indraprastha University
Dwarka 110078
New Delhi
India

Abstract

The exponential rise of multimedia data transmission in the digital era highlights the imperative for robust security protocols to safeguard sensitive information against unauthorized access and cyber threats. Conventional cryptographic techniques, while effective for text, often face challenges when applied to image data due to its inherent redundancy and high pixel correlation. To solve these challenges, this research presents a multi-layered encryption framework that integrates steganography for secure embedding, Henon chaotic mapping for shuffling, and a Reframed RSA (RRSA) algorithm for encryption. The framework was assessed using severe security metrics, including entropy analysis, correlation analysis, encryption quality assessment and NIST randomness tests. Results showed that the encrypted images exhibited high randomness, indicating strong diffusion properties. Correlation and histogram analyses confirmed the effective disruption of statistical dependencies and patterns. Additionally, NIST randomness tests validated the robustness of the encryption. Compared to existing methods, the proposed approach demonstrated significant improvements in diffusion, resistance to statistical attacks and computational efficiency. This study presents a scalable and adaptable hybrid encryption solution, addressing key limitations of conventional techniques while ensuring secure multimedia data transmission in an increasingly digital world.

Subject Classification: *68M25, 68P25, 68P27, 94A60.*

Keywords: *Chaotic, Image encryption, RSA, Steganography.*

* *E-mail:* **abhisheksaini348@gmail.com (Corresponding Author)**
† *E-mail:* **ruchi.sehrawat@ipu.ac.in**

1. Introduction

Rapid expansion of digital communication has revolutionized the way information is shared, processed, and stored. This evolution has increased the importance of securing sensitive data, particularly multimedia content like images, which are frequently used in personal, governmental, and industrial applications. These images are often targeted for unauthorized access, interception, and manipulation. While conventional encryption algorithms such as AES, DES, and RSA are highly effective for text-based data, their application to images presents unique challenges [1]. The distinct features of images, such as significant redundancy and high pixel correlation, limit the efficiency and security of traditional cryptographic methods [2], [3].

As computational capabilities continue to advance, particularly with the potential of quantum computing, the vulnerabilities in existing encryption systems become more pronounced. While classical encryption methods may be effective against current computational capabilities. To address these limitations, researchers are increasingly exploring hybrid methods that combine multiple layers of security, such as chaos-based techniques, steganography, and advanced cryptographic algorithms, to enhance the robustness of image encryption.

Chaos theory, known for its deterministic randomness and sensitivity to initial conditions [4], [5], [6], [7], has proven highly effective in cryptographic applications. By introducing non-linearity and unpredictability, chaotic maps like the Henon map create encrypted data that resists cryptanalytic attacks. Additionally, steganography enhanced security by embedding confidential data within innocuous cover images [8], [9], effectively concealing its existence. These two techniques, when combined with robust cryptographic algorithms such as RSA [10], [11], [12], [13], [30], can create a formidable encryption framework capable of addressing the limitations of traditional methods.

This research, introduces a hybrid framework for image encryption, integrating steganography, Henon chaotic mapping [14], a Reframed RSA (RRSA) algorithm utilizing prime palindrome numbers and XOR encryption. The process begins by embedding a secret image into a cover image using steganography, ensuring confidentiality and concealment. The resulting steganographic-image is then shuffled using the Henon chaotic map, disrupting pixel correlation and enhancing diffusion. The shuffled image is subsequently encrypted using RRSA, as illustrated in algorithm 1. This improved version of RSA employs prime palindromes to increase encryption complexity and resist factorization attacks. Finally, the RRSA-encrypted image is further protected through an XOR operation with a key image, producing the final cipher image.

The innovative use of prime palindromes in RRSA introduced a unique dimension to the encryption process, increasing its complexity and resistance to cryptographic attacks. This comprehensive framework addressed key challenges in image encryption, such as high pixel correlation, scalability, and computational efficiency. Extensive evaluations demonstrate its robustness, efficiency, and ability to provide a secure solution for protecting image data.

By integrating multiple security layers, the proposed framework offers a comprehensive solution to the evolving challenges of image encryption. It fills existing research gaps, such as the limited usage of hybrid approaches and the underutilization of prime palindromes and offers a scalable solution capable of resisting modern and future cryptographic challenges.

Algorithm 1. RRSA Encryption

Input:

- Two prime numbers P_1, P_2
- One Palindrome Prime number PL
- Public exponent e
- Plaintext M

Output: Public key (e, N_F), Private key (d, N_F) and Cipher text C

Key Generation

- Compute $N_F = P_1 \times P_2 \times PL$
- Euler's totient function:
  $\emptyset(N_F) = (P_1 - 1) \times (P_2 - 1) \times (PL - 1)$
- Ensure e is coprime with $\emptyset(N_F)$:
  $gcd\ (e, \emptyset(N_F)) = 1$
- Private key d:
  $d = e \wedge -1 \bmod \emptyset(N_F)$

Encryption

- Encrypt plaintext M using public key (e, N_F):
  $C = M \wedge e \bmod N_F$

Decryption

- Decrypt ciphertext C using private key (d, N_F):
  $M = C \wedge d \bmod N_F$

2. Related Work

Several researchers have explored the integration of RSA encryption with various cryptographic and steganographic techniques to enhance image security. These studies incorporate different strategies, such as chaotic maps, wavelet transforms, and singular value decomposition, to improve encryption strength, reduce computational complexity, and ensure visual imperceptibility.

Kalaichelvi et al. [15] improved RSA encryption by using two key pairs instead of one. Their approach employed Canny edge detection to differentiate image regions, embedding two bits in edge pixels and four bits in non-edge pixels via the Least Significant Bit (LSB) method. This adaptive embedding-maintained image quality while ensuring effective data concealment. To address computational efficiency, Zhu, Lin, and Ding [16] introduced an RSA-based encryption scheme using Singular Value Decomposition (SVD). Instead of encrypting the entire image, they focused only on diagonal elements within three decomposed matrices, significantly reducing processing time while maintaining encryption strength.

Wavelet-based approaches have also been widely explored. Bhargava and Mukhija [17] combined LSB, Discrete Wavelet Transform (DWT), and RSA encryption, first securing the secret message with RSA before embedding it into an image using LSB, where DWT enhanced concealment and minimized distortion. Similarly, Wahab et al. [18] combined RSA encryption, Huffman coding, and DWT-based steganography. Their method first encrypted the message using RSA, compressed it with Huffman coding, and embedded it into a cover image that had undergone lossy compression via DWT. Du and Ye [19] applied Integer Wavelet Transform (IWT) with RSA encryption, extracting key image features, generating random encryption parameters, and using a 3D chaotic system for scrambling. This two-stage scrambling process modified image coefficients before applying inverse IWT and a final diffusion step. Kadhem and Baawi [20] further optimized traditional LSB-based steganography by encrypting messages with RSA, compressing them using Huffman coding, and embedding them adaptively in a 24-bit color image. Their approach incorporated XOR/XNOR operations to enhance data security.

Some researchers have combined RSA with chaotic maps to enhance security. Xu, Sun, and Zhu [21] developed an asymmetric image encryption method integrating RSA with a hyperchaotic map. Their approach scrambled images using row and column transformations, encrypted the key separately with RSA and embedded both the encrypted image and key within a carrier image using DWT. Lin and Li [22] took a different approach by using the Lorenz hyperchaotic system with RSA encryption. In their method, the RSA algorithm generated initial values for the Lorenz system, which then produced a key stream for encryption. Their technique applied additive mode diffusion and a finite field diffusion algorithm to distribute pixel values across the image, ensuring better resistance to attacks. Jiao et al. [23] also incorporated chaotic transformations, integrating the generalized Arnold map with RSA. Their method generated encryption parameters via RSA, applied XOR diffusion to pixel values, and implemented cyclic confusion for additional security. Mfungo and Fu [24] further expanded on this concept by introducing a hybrid cryptosystem that combined RSA, chaotic maps and homomorphic encryption. Their method used the unpredictability of sine and logistic chaotic maps alongside the fractal properties of the Sierpinski triangle to enhance key sensitivity and expand the key space. The encryption process incorporated multiple layers of security, including RSA encryption, chaotic scrambling, and Paillier encryption.

3. Proposed Work

The proposed method employs a multi-layered framework to ensure robust image data security. It integrates steganography, chaotic shuffling, Reframed RSA encryption, and XOR-based encryption, as illustrated in Figure 1. The framework is designed to handle images of varying sizes, such as 256 × 256, 512 × 512, and 1024 × 1024, and supports different image formats, including PNG, JPG, and TIFF, ensuring adaptability to diverse security requirements.

Each step enhances the overall security and complexity, making the system highly resistant to cryptographic attacks.

Step-by-Step Procedure:

1) **Embedding Secret Image in Cover Image:** For each pixel in cover image I_C, replace its least significant b bits with the most significant b bits of secret image I_S, then then stego image I_{stego}:

$$I_{stego} = \left(I_c \wedge \sim(2^b - 1)\right) \vee \left(I_s \gg (8 - b)\right) \quad (1)$$

2) **Chaotic Shuffling of the Steganographic Image:**

a. Generate a Henon chaotic sequence S for n pixels using initial parameters x_0, y_0, a, b:

$$x_{n+1} = 1 - a \cdot x_n^2 + y_n \quad (2)$$

$$y_{n+1} = b \cdot x_n \quad (3)$$

b. Normalize sequence S to create a permutation sequence for pixel:

$$indices(S) = sort(S)\%n \quad (4)$$

c. Permute stego image I_{stego}, pixels according *indices(S)*, then the shuffled image $I_{shuffled}$ *is:*

$$I_{shuffed} = permute(I_{stego}, indices(S)) \quad (5)$$

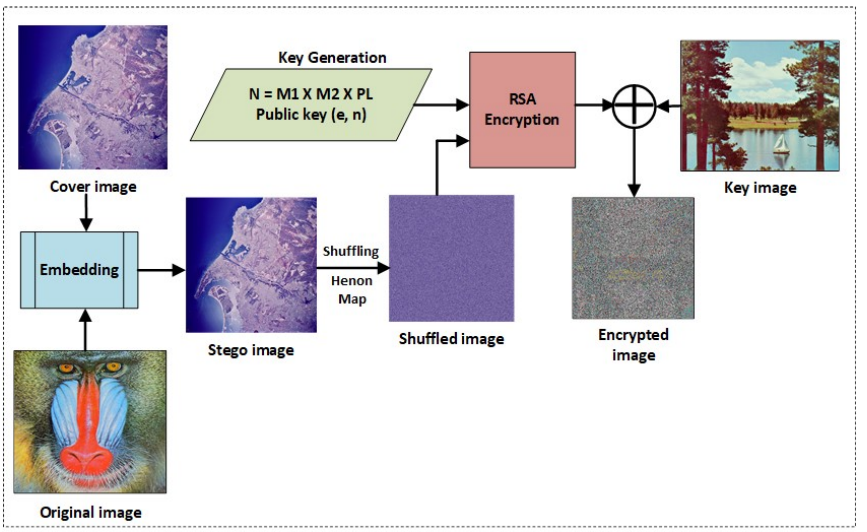


Figure 1
Process diagram of encryption framework

3) **Reframed RSA (RRSA) Encryption:**

a. Compute the RSA modulus N_F using three primes M_1, M_2 and palindrome prime number PL:

$$N_F = M_1 \times M_2 \times PL \quad (6)$$

b. Calculate the totient $\emptyset(N_F)$:

$$\emptyset(N_F) = (M_1 - 1) \times (M_2 - 1) \times (PL - 1) \quad (7)$$

c. Select public key exponent e such that $1 < e < \emptyset(N_F)$ and $\gcd(e, \emptyset(N_F)) = 1$.

d. Compute the private key d:

$$d = e^{-1} \, mod \, \emptyset(N_F) \quad (8)$$

e. Encrypt each pixel P of $I_{shuffled}$ using the public key (e,N_F):

$$I_{RRSA} = P^e \, mod \, N_F \quad (9)$$

4) XORing with a Key Image: Perform an exclusive OR operation between the RRSA encrypted image I_{RRSA} and the key image I_K, then the encrypted image I_C is:

$$I_E = I_{RRSA} \oplus I_K \quad (10)$$

4. Results and Discussions

This section analyses various metrics to assess the performance of the proposed method, including statistical analysis, encryption quality test and randomness analysis [25]. The input images used for these tests [26] are shown in Figure 2, while the encrypted images, generated using the proposed method is presented in Figure 3, illustrating the achieved visual transformation. All experiments were conducted on a system featuring an Intel Core i5-13420H CPU operating at 2.10 GHz, 16 GB of RAM and a 512 GB SSD, with Python as the implementation platform.

4.1 *Henon Map Performance Analysis*

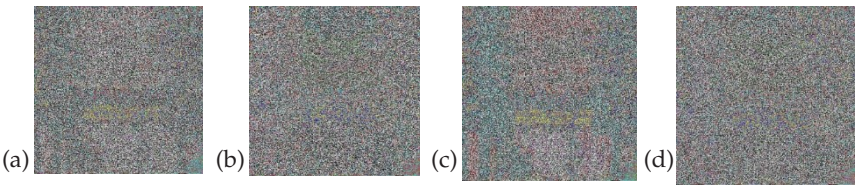
The Henon map's chaotic behavior and dynamical properties are effectively demonstrated through three key representations: phase space plot, Henon chaotic sequence and the bifurcation diagram. Figure 4, illustrates the phase space trajectory of the Henon map for a=1.4 and b=0.3, revealing the characteristic attractor structure in the x-y plane. The dense and intricate patterns highlight the system's sensitivity to initial conditions and its long-term behavior. Figure 5, presents the Henon chaotic sequence over 1000 iterations, showing the evolution of x and y values with oscillatory and seemingly random variations, which are characteristic of chaos. Lastly, Figure 6, displays the bifurcation diagram, demonstrating the dependence of the Henon map's dynamics on the parameter a. This plot illustrates the transitions from periodic behavior to chaos as a increases, with regions of stability interspersed with bifurcations and chaotic attractors. These representations offer a thorough comprehension of the intricate and varied dynamics of the Henon map.

(a) (b) (c)

(d) (e) (f)

Figure 2

Input images (a) Baboon (b) Female (c) House (d) Peppers; (e) San Diego (Cover image); (f) Boat (Key image)



(a) (b) (c) (d)

Figure 3

Encrypted images (a) Baboon (b) Female (c) House (d) Peppers

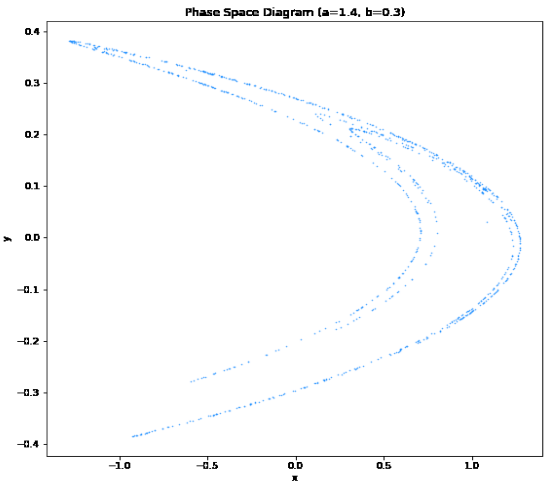


Figure 4

Phase trajectory of the chaotic system for a = 1.4, b = 0.3

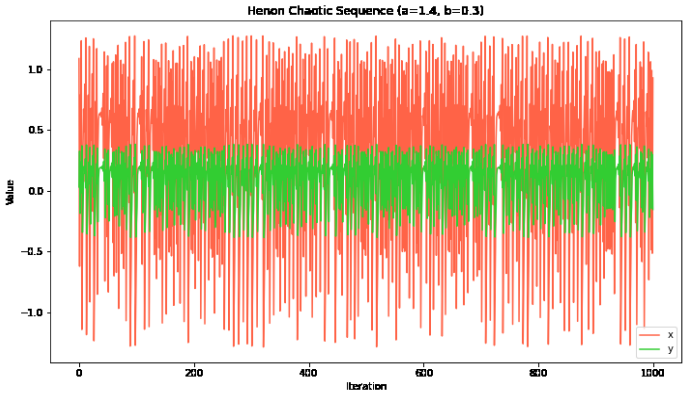


Figure 5
Time evolution of x and y values in the Henon map

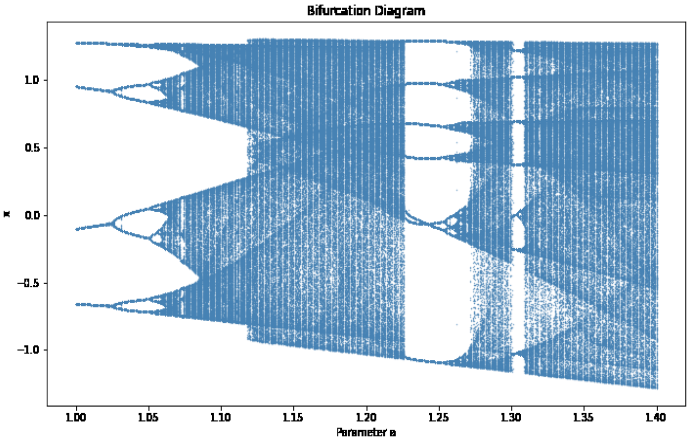


Figure 6
Analysis of periodic and chaotic regions via bifurcation

4.2 *Statistical Analysis*

The performance and efficacy of the proposed encryption technique are evaluated in this section using statistical measures like entropy analysis, correlation analysis, and histogram analysis. These analyses provide insights into how well the encryption technique obfuscates the original image's features and ensures randomness in the encrypted output.

4.2.1 Histogram Analysis

The histogram of an image represents the frequency distribution of pixel intensity values. Figure 7 illustrates the histogram of the original image, revealing distinct peaks and patterns that correspond to the pixel intensity

distribution. Figure 8 shows the histogram of the encrypted image. Unlike the original, the histogram of the encrypted image is uniformly distributed, with no discernible patterns or peaks. This uniformity indicates that the encryption process effectively conceals the statistical features of the original image, making it highly resistant to frequency-based attacks.

4.2.2 Deviation from Uniform Histogram

The divergence (deviation) from a uniform histogram serves as an indicator of the extent to which the histogram of the encrypted image aligns with an ideal uniform distribution. Table 1 presents the deviation results for various test images encrypted using the proposed method. The even distribution of the intensity of pixels in the cipher image is indicated by lower deviation values, which imply stronger encryption performance. The results show that the proposed encryption technique consistently achieves low deviation values across different test images. This outcome confirms the method's ability to obscure identifiable patterns and closely approximate a uniform histogram, thereby enhancing its robustness against statistical attacks.

Table 1

Analysis of divergence from Uniform Histogram

S. No.	Image	Proposed
1.	Baboon	0.5077
2.	Female	0.5416
3.	House	0.5029
4.	Peppers	0.5157

4.2.3 Entropy

Entropy is an important statistic for determining the randomness of pixel intensity values, which reflects the unpredictability of encrypted images. For a grayscale image, an ideal entropy value is 8, signifying maximum randomness and robust encryption. Table 2, presents a comparison of entropy values achieved by the proposed method against existing techniques for various test images. The proposed method consistently achieved entropy values above 7.98 for all test images, significantly exceeding the entropy of the original images. Furthermore, in Table 2, the results demonstrate comparable performance to referenced methods, such as Ref. [15], Ref. [22], and Ref. [23]. Thus, the entropy of the encrypted baboon image using the proposed method is 7.995, closely approaching the ideal value of 8 and matching the highest-performing method of Ref. [22]. These findings confirm the efficacy of the proposed method in concealing image details and enhancing security by generating encrypted images with near-ideal entropy.

4.2.4 Correlation Analysis

In this study, correlation analysis is used to evaluate the relationship between pixel intensity values, focusing on both adjacent pixels and the

relationship between original and encrypted images. A strong encryption scheme is expected to minimize the correlation between adjacent pixels and completely obscure any relationship between original and encrypted images.

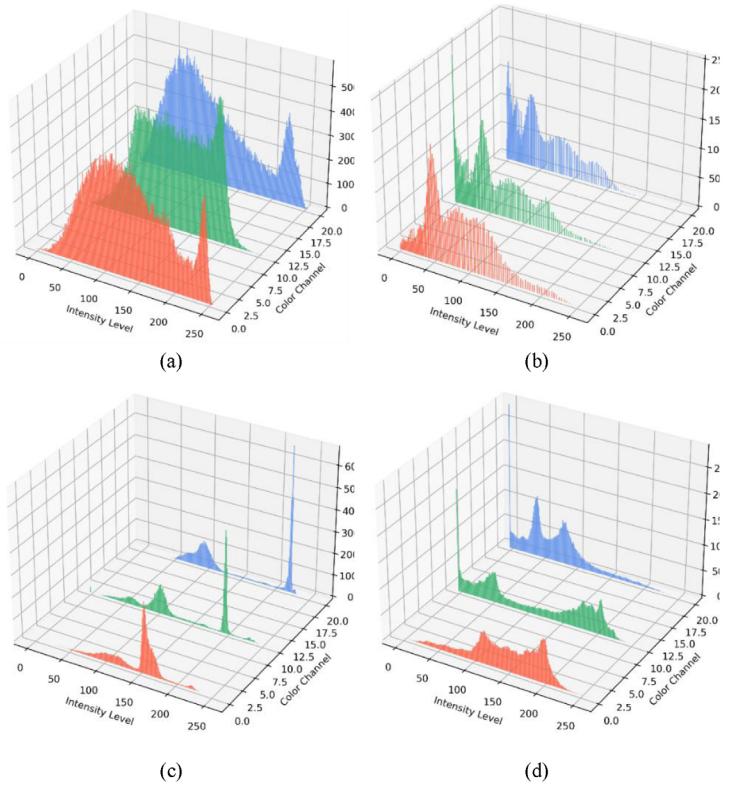
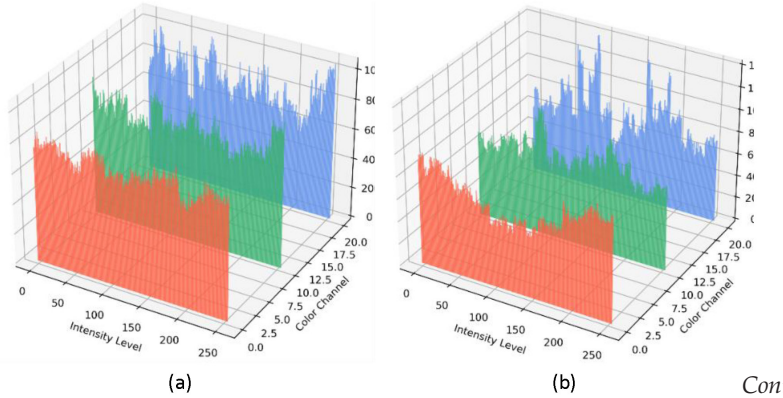
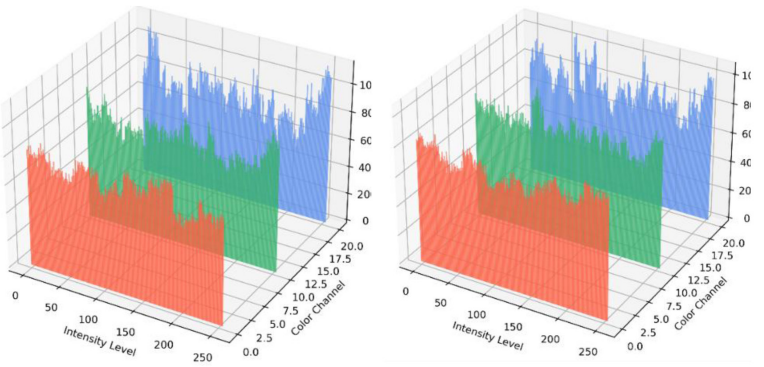


Figure 7
Histogram analysis of original images (a) Baboon (b) Female (c) House (d) Peppers



Contd...



(c) (d)

Figure 8
Histogram analysis of encrypted images (a) Baboon (b) Female (c) House (d) Peppers

4.2.4.1 Correlation Analysis within adjacent pixel

Figures 9 to 12 present scatter plots of pixel intensity correlations in the horizontal, vertical, and diagonal directions for the original and encrypted images. The original images exhibit strong positive correlations, while the encrypted images show, no discernible correlation, confirming the proposed method's ability to disrupt pixel relationships effectively. Table 3 provides a comparison of correlation coefficients for adjacent pixels in different directions. The proposed method achieved coefficients close to zero, indicating a significant reduction in pixel correlation compared to the original images. Such as, the horizontal correlation coefficient for the baboon image decreases from 0.7169 in the original image to 0.0584 in the encrypted image. Additionally, the proposed method demonstrates comparable or superior performance to referenced methods, such as Ref. [18] and Ref. [22].

4.2.4.2 Correlation between original and encrypted images.

The correlation between original and encrypted images measures the similarity between them. A correlation value close to zero indicates that the encryption method has successfully obscured the relationship between the original and encrypted images. Table 4 show the correlation values of the original and encrypted images for several test images. The results show near-zero values for all tested images, further validating the effectiveness of the proposed encryption method. The correlation value for the house image is -0.0244 and for the baboon image, it is 0.0029, indicating that the encrypted images have no statistical resemblance to the original images.

Table 2

Entropy comparison of the of proposed and existing

S. No.	Image	Original Image	Pro-posed	Ref [15]	Ref [22]	Ref [23]
1.	Baboon	6.416	7.995	-----	7.999	-----
2.	Female	5.984	7.989	-----	-----	-----
3.	House	6.112	7.994	-----	-----	-----
4.	Peppers	6.614	7.995	7.747	7.999	7.999

Table 3

Performance comparison of correlation of proposed with existing

Scheme	Test Images	Directions		
		H	V	D
Original	Baboon	0.7169	0.6091	0.6092
	Female	0.9740	0.9656	0.9514
	House	0.9782	0.9529	0.9360
	Peppers	0.9609	0.9682	0.9333
Proposed	Baboon	0.0584	0.0089	0.0062
	Female	0.1282	0.0075	-0.0033
	House	0.0453	0.0123	0.0049
	Peppers	0.0272	0.0074	-0.0041
Ref. [18]	House	0.9540	0.9759	0.9440
Ref. [22]	Baboon	-0.0179	-0.0060	0.0181
	Peppers	-0.0195	-0.0101	-0.0109

4.3 *Encryption Quality*

The encryption quality of the proposed method is evaluated using four essential metrics: Mean Squared Error (MSE), Mean Absolute Error (MAE), Peak Signal-to-Noise Ratio (PSNR), and Structural Similarity Index Measure (SSIM) [27], [28]. These metrics provide a comprehensive assessment of the encryption's effectiveness by evaluating the distortion and dissimilarity introduced during the encryption process. A high MSE and MAE indicate substantial changes in pixel intensity values, while low PSNR and SSIM values suggest minimal resemblance and structural similarity between the original and encrypted images. For the encryption technique to be secure and reliable, this combination of high distortion and low similarity is essential.

As summarized in Table 5, the proposed method demonstrates consistent performance across various test images, effectively disrupting the statistical and structural features of the original images With a PSNR of 10.561 and an SSIM of 0.0136, the baboon image has minimal visual or structural correlation with

the original image, while its MSE of 5713.983 and MAE of 61.433 demonstrate notable pixel intensity changes. Similar results are observed for other images, such as the peppers image, which achieved an MSE of 7097.655 and an SSIM of 0.0116, further confirming the strong encryption performance of the proposed method.

These results highlight the method's ability to produce encrypted images that are both statistically and visually distinct from their originals, ensuring resistance to both statistical and visual attacks The consistency in performance across diverse test images highlights the robustness and adaptability of the encryption technique, making it a reliable approach for secure image encryption.

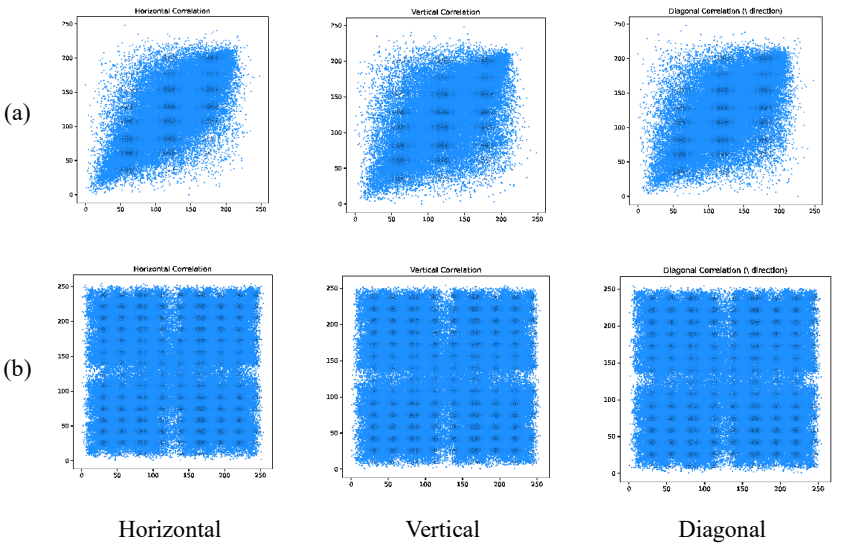


Figure 9

Correlation coefficient diagram of baboon image, (a) Original (b) Encrypted.

Table 4

Evaluation of pixel correlation between original Images and encrypted Images

S. No.	Image	Correlation Value
1.	Baboon	0.0029
2.	Female	-0.0010
3.	House	-0.0244
4.	Peppers	-0.0047

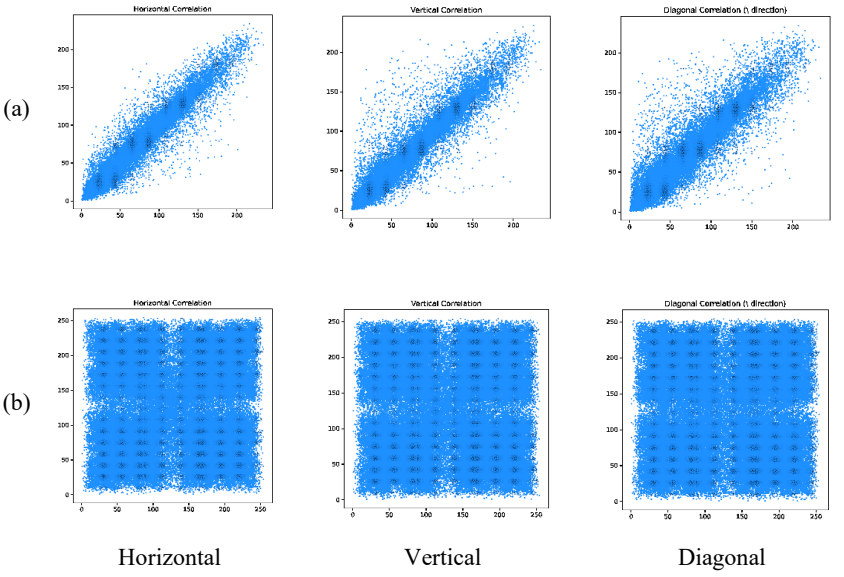
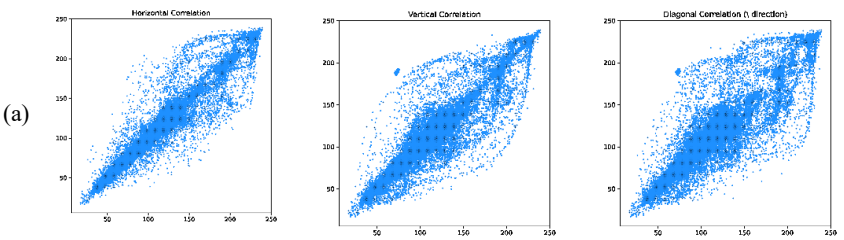


Figure 10
Correlation coefficient diagram of female image, (a) Original (b) Encrypted.

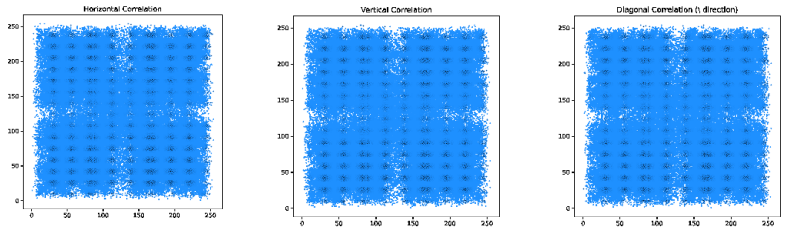
Table 5
Analysis of Encryption Quality Metrics for the Proposed Method

S. No.	Image	MSE	MAE	PSNR	SSIM
1.	Baboon	5713.983	61.433	10.561	0.0136
2.	Female	9279.430	81.239	8.455	0.0088
3.	House	5598.832	60.837	10.649	0.0129
4.	Peppers	7097.655	69.207	9.619	0.0116



Contd...

(b)

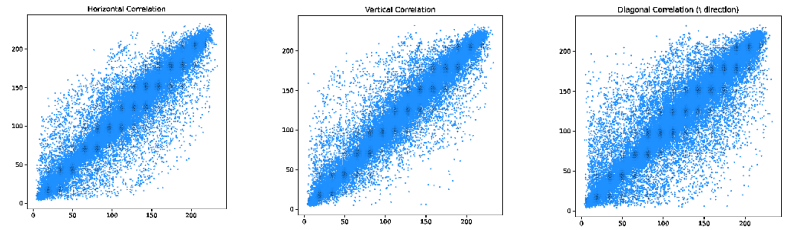


Horizontal Vertical Diagonal

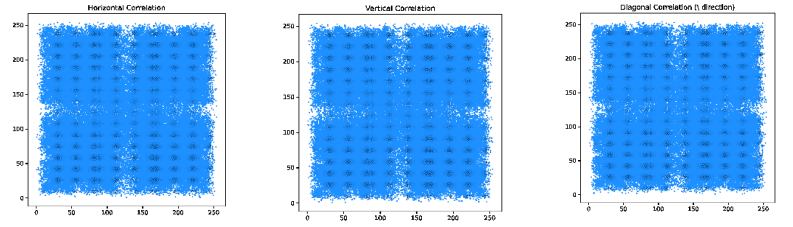
Figure 11

Correlation coefficient diagram of house image, (a) Original (b) Encrypted.

(a)



(b)



Horizontal Vertical Diagonal

Figure 12

Correlation coefficient diagram of peppers image, (a) Original (b) Encrypted.

4.4 *Randomness Analysis*

Randomness analysis is an important step in determining the strength of an encryption scheme. It assures that the created cipher images are highly random, making them resistant to cryptanalysis. In this work, two important methodologies are used to evaluate the randomness of the proposed encryption method: Gray-Level Co-Occurrence Matrix (GLCM) Analysis and the NIST Statistical Test Suite.

4.4.1 Gray-Level Co-Occurrence Matrix (GLCM) Analysis.

GLCM is a statistical method used to analyses the spatial relationships between pixels in an image. Key metrics derived from GLCM, such as homogeneity, energy, and contrast, provide valuable insights into the texture and

randomness of both original and encrypted images. Homogeneity measures the homogeneity of pixel pair distributions, with lower values in encrypted images indicating less uniformity and more unpredictability. Energy determines pixel pair repetitions, and lower energy values in encrypted images indicate greater unpredictability. Contrast assesses the intensity difference between adjacent pixels and a significant rise in contrast in encrypted images indicates successful encryption. As shown in Table 6, the encrypted baboon image exhibits a significant increase in contrast, from 1037.484 to 8362.663, as well as decreases in homogeneity and energy, confirming the strong randomness induced by the proposed method. Similar patterns are observed in other test images, validating the efficacy of the encryption technique in disrupting spatial pixel relationships and enhancing randomness.

Table 6

GLCM Analysis

S. No.	Image	Original Image			Encrypted Image		
		Homogeneity	Energy	Contrast	Homogeneity	Energy	Contrast
1.	Baboon	0.1271	0.0097	1037.484	0.0348	0.0057	8362.663
2.	Female	0.3371	0.0266	82.207	0.0485	0.0062	7567.475
3.	House	0.3232	0.0607	92.777	0.0359	0.0057	8487.513
4.	Peppers	0.3303	0.0193	222.239	0.0320	0.0058	8591.578

4.4.2 NIST Test

A well-known standard for assessing the randomness of encryption algorithms is the NIST Statistical Test Suite [29]. It includes a number of tests, including as frequency, runs, and linear complexity, that assess various aspects of randomness in encrypted data. For encryption to be considered random, the p-value from each test must exceed the threshold of 0.01. The results of the NIST tests, summarized in Table 7 and visually represented in Figure 13, confirm the high randomness achieved by the proposed encryption method. Notably, the proposed method consistently passes all 15 tests, with p-values exceeding 0.01 for all evaluated images. These findings underscore the suitability of the proposed encryption technique for secure applications, ensuring robust protection against statistical and randomness-based attacks.

Table 7

NIST Tests

Tests	P- Value				Conclusion
	Baboon	Female	House	peppers	
Frequency (Monobits) [29]	0.9238	0.7622	0.5086	0.0916	Random
Frequency within a Block [29]	0.0284	0.025	0.432	0.0325	Random
Runs [29]	0.0589	0.0169	0.031	0.023	Random

Longest Run of One in a Block [29]	0.9888	0.9998	0.9815	0.9999	Random
Binary Matrix Rank [29]	0.196	0.039	0.808	0.039	Random
Discrete Fourier Transform [29]	0.944	0.607	0.958	0.226	Random
Non-overlapping Template Matching [29]	0.8999	0.9824	0.9956	0.9871	Random
Overlapping Template [29]	0.8865	0.6330	0.3972	0.3972	Random
Universal Statistical [29]	0.259	0.267	0.223	0.154	Random
Linear Complexity [29]	0.8088	0.6093	0.1112	0.0306	Random
Serial Test (P-Value-1) [29]	0.498	0.999	0.498	0.498	Random
Serial Test (P-Value-2) [29]	0.9999	0.998	0.999	0.327	Random
Approximate Entropy [29]	0.3099	0.3098	0.3101	0.3100	Random
Cumulative Sums (Forward) [29]	0.8954	0.8994	0.9827	0.9917	Random
Cumulative Sums (Backward) [29]	0.9162	0.9153	0.9214	0.9991	Random
Random Excursions (Average) [29]	0.9625	0.9965	0.9847	0.9953	Random
Random Excursions Variant (Average) [29]	0.9687	0.7799	0.9034	0.9712	Random

5. Discussion

The proposed image encryption framework combines multiple security techniques to ensure strong protection against cryptographic attacks. A major feature of this method is the use of Henon chaotic mapping for pixel shuffling. Traditional image encryption methods often face challenges with high pixel correlations, making them prone to statistical attacks. The Henon map effectively randomizes pixel positions, reducing correlation coefficients to nearly zero and greatly enhancing randomness. Moreover, histogram analysis shows that encrypted images have a uniform pixel intensity distribution, further reducing the risk of statistical attacks.

The Reframed RSA algorithm provides another layer of security by addressing vulnerabilities in traditional RSA encryption. It used prime palindrome numbers, which introduced unique mathematical properties that make modulus factorization considerably more complex. This added complexity significantly strengthens resistance to brute-force attacks. Experimental results showed that RRSA not only enhanced security but also maintains efficient key generation, ensuring strong encryption without reducing computational performance.

To further enhance the encryption process, an XOR operation with a key image is applied after RRSA encryption. This step strengthens the diffusion and confusion properties, making it computationally infeasible for attackers to decrypt the encrypted data without the corresponding key image. The XOR

operation increased non-linearity, decreasing the possibility of effective cryptanalysis.

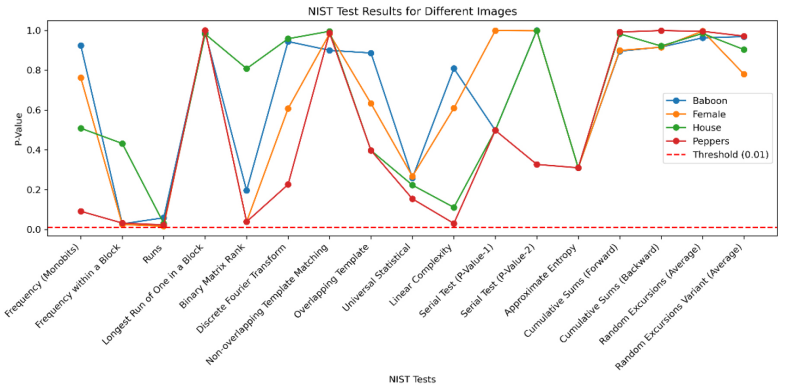


Figure 13
NIST Test

6. Conclusion

This research presented a novel multi-layered framework for secure image encryption, integrating steganography, chaotic mapping, and a Reframed RSA algorithm. The proposed method enhanced image security by embedding a secret image into a cover image, disrupting statistical patterns through chaotic pixel shuffling, and introducing randomness. Encryption was achieved using RRSA, further strengthened by XORing the encrypted image with a key image. The performance of the framework was rigorously evaluated using multiple security metrics. Entropy analysis showed values close to 7.99, indicating excellent randomness and diffusion. Correlation coefficients of encrypted images are near zero, effectively eliminating statistical dependencies among adjacent pixels. Histogram analysis revealed a uniform distribution, confirming the encryption's ability to obscure image patterns. Quality metrics highlighted the robustness of the encryption, with MSE ranging from 5598.83 to 9279.43 and MAE from 60.83 to 81.23, reflecting significant pixel alterations. PSNR values ranged between 8.45 and 10.65, while SSIM values close to zero indicated substantial visual distortion, critical for security. The NIST randomness tests validated the cryptographic strength, as all p-values surpassed the threshold of 0.01. The use of prime palindromes in RRSA introduced an innovative layer of complexity, enhancing resistance to brute-force and statistical attacks compared to traditional RSA. This scalable and efficient framework provides a robust solution for real-world applications, ensuring secure multimedia data transmission in digital environments.

Acknowledgment

Authors express their thankfulness for the IPRF award received from ‘Guru Gobind Singh Indraprastha University, New Delhi, India.’

References

[1] Z. Man, J. Li, X. Di, Y. Sheng, and Z. Liu, "Double image encryption algorithm based on neural network and chaos," *Chaos, Solitons & Fractals*, vol. 152, p. 111318 (Nov. 2021), doi: https://doi.org/10.1016/j.chaos.2021.111318.

[2] S. Kumar, K. K. Raghuvanshi, S. Kumar, and S. Kumar, "Ilmdnacnn: Intertwining logistic map and DNA encoding based Image encryption using CNN," *SSRN Electronic Journal* (2022), doi: https://doi.org/10.2139/ssrn.4117315.

[3] Kang, Y. Liang, Y. Wang, and M. V. I, "Color image encryption method based on 2D-variational mode decomposition," *Multimedia tools and applications*, vol. 78, no. 13, pp. 17719–17738 (Jan. 2019), doi: https://doi.org/10.1007/s11042-018-7129-4.

[4] L. Tu, Y. Wang, and C. Zhang, "A new image encryption algorithm based on optimized lorenz chaotic system," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 13 (Jul. 2020), doi: https://doi.org/10.1002/cpe.5902.

[5] B. V. Nair, S, Vismaya V, S. S. Muni, and A. Durdu, "Deep learning and chaos: a combined approach to image encryption and decryption," *arXiv (Cornell University)* (Jun. 2024), doi: https://doi.org/10.48550/arxiv.2406.16792.

[6] Nurnajmin Qasrina Ann, Dwi Pebrianti, Mohd Fadhil Abas, and Luhur Bayuaji, "A new hybrid image encryption technique using lorenz chaotic system and simulated kalman filter (SKF) algorithm," *Lecture notes in electrical engineering*, pp. 441–453 (Jan. 2022), doi: https://doi.org/10.1007/978-981-16-8690-0_40.

[7] S. Das, S. S. Mukherjee, and S. Mandal, "Application of chaotic neural network in cryptography," *International Journal of Computer Applications*, vol. 184, no. 13, pp. 60–64 (May 2022), doi: https://doi.org/10.5120/ijca2022922133.

[8] Q. Li, X. Wang, X. Wan, B. Ma, C. Wang, Y. Xian and Y. Shi, "A novel grayscale image steganography scheme based on chaos encryption and generative adversarial networks," *IEEE Access*, vol. 8, pp. 168166–168176 (Jan. 2020), doi: https://doi.org/10.1109/access.2020.3021103.

[9] Sanjukta Krishnagopal, S. Pratap, and B. Prakash, "Image encryption and steganography using chaotic maps with a double key protection,"

Advances in intelligent systems and computing, pp. 67–78 (Dec. 2014), doi: https://doi.org/10.1007/978-81-322-2220-0_6.

[10] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126 (1978), doi: https://doi.org/10.1145/359340.359342.

[11] M. Mumtaz and L. Ping, "Forty years of attacks on the RSA cryptosystem: A brief survey," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 22, no. 1, pp. 9–29 (Jan. 2019), doi: https://doi.org/10.1080/09720529.2018.1564201.

[12] A. Sahoo, P. Mohanty, and Purna Chandra Sethi, "Image encryption using rsa algorithm," *Intelligent Systems, Lecture Notes in Networks and Systems*, vol. 431, pp. 641–652 (Jan. 2022), doi: https://doi.org/10.1007/978-981-19-0901-6_56.

[13] W. Stallings, *Cryptography and network security : principles and practice*. Hoboken, New Jersey: Pearson Education, Inc (2020).

[14] P. N. Lone, D. Singh, and U. H. Mir, "A novel image encryption using random matrix affine cipher and the chaotic maps," *Journal of Modern Optics*, vol. 68, no. 10, pp. 507–521 (May 2021), doi: https://doi.org/10.1080/09500340.2021.1924885.

[15] V. Kalaichelvi, P. Meenakshi, P. Vimala Devi, H. Manikandan, P. Venkateswari, and S. Swaminathan, "A stable image steganography: a novel approach based on modified RSA algorithm and 2–4 least significant bit (LSB) technique," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 7, pp. 7235–7243 (Aug. 2020), doi: https://doi.org/10.1007/s12652-020-02398-w.

[16] K. Zhu, Z. Lin, and Y. Ding, "A new RSA image encryption algorithm based on singular value decomposition," *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 33, no. 01, pp. 1954002–1954002 (Jun. 2018), doi: https://doi.org/10.1142/s0218001419540028.

[17] S. Bhargava and M. Mukhija, " Hide image and text using LSB, DWT and RSA based on image steganography," *ICTACT Journal on Image and Video Processing*, vol. 9, no. 3, pp. 1940–1946 (Feb. 2019), doi: https://doi.org/10.21917/ijivp.2019.0275.

[18] O. F. A. Wahab, A. A. M. Khalaf, A. I. Hussein, and H. F. A. Hamed, "Hiding data using efficient combination of RSA cryptography,

and compression steganography techniques," *IEEE Access*, vol. 9, pp. 31805–31815 (2021), doi: https://doi.org/10.1109/access.2021.3060317.

[19] S. Du and G. Ye, "IWT and RSA based asymmetric image encryption algorithm," *Alexandria Engineering Journal*, vol. 66 (Nov. 2022), doi: https://doi.org/10.1016/j.aej.2022.10.066.

[20] Eman Lateef Kadhem and Salwa Shakir Baawi, "A secure and high capacity image steganography approach using huffman coding and RSA encryption," *Journal of Al-Qadisiyah for Computer Science and Mathematics*, vol. 15, no. 2 (Sep. 2023), doi: https://doi.org/10.29304/jqcm.2023.15.2.1231.

[21] Q. Xu, K. Sun, and C. Zhu, "A visually secure asymmetric image encryption scheme based on RSA algorithm and hyperchaotic map," *Physica Scripta*, vol. 95, no. 3, p. 035223 (Feb. 2020), doi: https://doi.org/10.1088/1402-4896/ab52bc.

[22] R. Lin and S. Li, "An image encryption scheme based on lorenz hyperchaotic system and RSA algorithm," *Security and Communication Networks*, vol. 2021, no. 1, pp. 1–18 (Apr. 2021), doi: https://doi.org/10.1155/2021/5586959.

[23] K. Jiao, G. Ye, Y. Dong, X. Huang, and J. He, "Image encryption scheme based on a generalized arnold map and RSA algorithm," *Security and Communication Networks*, vol. 2020, no. 1, pp. 1–14 (Jun. 2020), doi: https://doi.org/10.1155/2020/9721675.

[24] Dani Elias Mfungo and X. Fu, "Fractal-based hybrid cryptosystem: enhancing image encryption with RSA, homomorphic encryption, and chaotic maps," *Entropy*, vol. 25, no. 11, pp. 1478–1478 (Oct. 2023), doi: https://doi.org/10.3390/e25111478.

[25] Y. Alghamdi and A. Munir, "Image encryption algorithms: A survey of design and evaluation metrics," *Journal of Cybersecurity and Privacy*, vol. 4, no. 1, pp. 126–152 (Mar. 2024), doi: https://doi.org/10.3390/jcp4010007.

[26] University of Southern California, "SIPI Image Database," *sipi.usc.edu*. https://sipi.usc.edu/database/database.php

[27] J. Nilsson and T. Akenine-Möller, "Understanding SSIM," *arXiv.org*, Jun. 29 (2020). https://arxiv.org/abs/2006.13846

[28] R. Parameshachari and S. M. Chandramouli, "Building enhanced chaotic map encryption method for medical information system,"

Journal of System and Management Sciences, vol. 11, no. 1 (Mar. 2021), doi: https://doi.org/10.33168/jsms.2021.0111.

[29] L. E. Bassham, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, S. D. Leigh, M. Levenson, M. Vangel, N. A. Heckert, and D. L. Banks, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," (2010). [Online]. Available: https://www.nist.gov/publications/statistical-test-suite-random-and-pseudorandom-number-generators-cryptographic.

[30] N. N. H. Adenan, A. Nitaj, M. R. K. Ariffin, and N. A. Abu, "Cryptanalysis of a cubic Pell variant of RSA with primes sharing least significant bits," *Journal of Information and Optimization Sciences*, vol. 45, no. 5, pp. 1263–1280 (2024), doi: https://doi.org/10.47974/jios-1333.

Received April, 2025