Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol X No. Y (2025)

Image Encryption and Decryption Algorithm Based on Chaotic Systems and RSA Cryptography

Arabind Kumar[1,a)], Sanjay Yadav[2,b)], Rajni Rohila[3,c)]

[1&3] *Department of Applied Sciences The Northcap University Gurugram, India*

[2] *Alliance school of Applied Mathematics, Alliance University Bangalore, India*

[a] *arabind20asd003@ncuindia.edu*

[b] *sanjay.yadav@alliance.edu.in*

[c] *rajnirohila@ncuindia.edu*

*Corresponding Author - Sanjay Yadav

Article History:

Received: 12-01-2025

Revised: 15-02-2025

Accepted: 01-03-2025

Abstract: This paper presents a novel image encryption and decryption algorithm that combines chaotic systems and RSA cryptography to enhance the security of digital images. In this hybrid approach, a chaotic system generates a pseudo-random key for pixel-level encryption, while RSA cryptography is employed to securely exchange the encryption key between the sender and receiver. The proposed algorithm leverages the unpredictability and sensitivity of chaotic systems to obfuscate image patterns, ensuring high security against potential attacks. RSA cryptography, known for its robust public-key infrastructure, guarantees secure key management and protects the encryption key during transmission. Experimental results show that the algorithm offers strong encryption, high resistance to common cryptographic attacks, and efficient performance. The proposed method demonstrates the effectiveness of combining chaotic systems and RSA for digital image protection, making it a promising solution for applications requiring secure image communication and storage.

Keywords: Image Encryption, Chaotic Systems, Security, RSA Cryptography, Key Generation.

1. INTRODUCTION

In the modern digital era, the proliferation of multimedia data, particularly images, has led to increased concerns about privacy and security. Images, as a form of sensitive information, are often transmitted over the internet or stored in digital systems, where they are vulnerable to unauthorized access, manipulation, and misuse. Securing digital images is, therefore, a critical aspect of maintaining confidentiality, integrity, and authenticity, especially in sectors like healthcare, defence, and digital forensics. Traditional encryption methods like the Advanced Encryption Standard (AES) and Data Encryption Standard (DES) are commonly used to protect data, but these algorithms are often not tailored for image data, which has unique characteristics such as large size, high redundancy, and specific pixel patterns. As a result, image encryption algorithms require specialized techniques to effectively obscure these patterns and protect against potential cryptographic attacks [1-2].

With the growing need for data security in digital communication, the protection of image data is crucial. Image encryption involves transforming an image into an unreadable format that can only be

restored by authorized decryption. Chaotic systems, known for their randomness and sensitivity, have become increasingly popular for encryption. RSA cryptography, a well-established public-key algorithm, provides robust key security. This paper aims to develop an image encryption algorithm combining chaotic systems and RSA cryptography for enhanced security. In an era where digital information is increasingly vulnerable to unauthorized access, effective methods of securing data have become paramount. The integration of image encryption techniques plays a crucial role in safeguarding visual content from prying eyes, particularly in applications spanning from secure communications to medical imaging [3-5].

The complex nature of image data necessitates the development of advanced algorithms that not only protect the integrity of imagery but also ensure that the decryption process is both efficient and reliable. Among the myriads of encryption strategies, chaotic systems paired with RSA cryptography present a promising solution, offering dual-layered security that capitalizes on the strengths of both methodologies. This essay will delve into the intricacies of these algorithms, exploring how they leverage the unpredictability of chaotic systems alongside the robustness of RSA, ultimately aiming to provide a comprehensive understanding of their applications and effectiveness in modern cybersecurity frameworks [6].

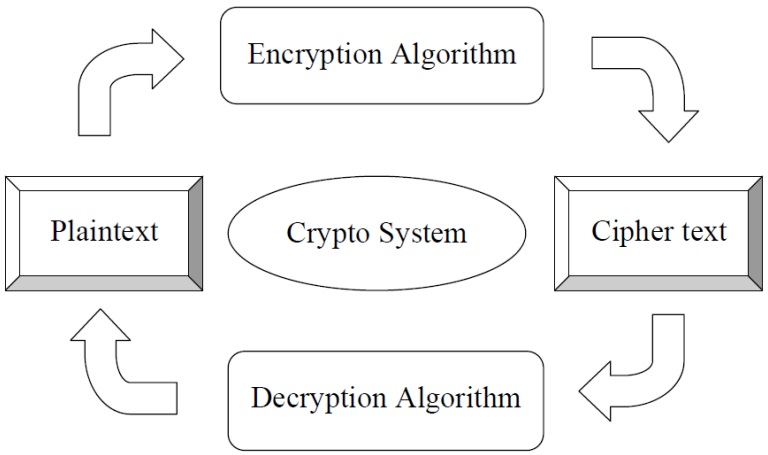


Figure -1 General Block Diagram of Cryptosystem

Chaotic systems and RSA cryptography have emerged as promising tools for addressing these challenges. Chaotic systems, known for their sensitive dependence on initial conditions and pseudo-random behaviour, offer an ideal foundation for generating complex encryption keys. On the other hand, RSA cryptography, a widely recognized asymmetric encryption algorithm, provides robust key management and secure transmission of keys, making it suitable for ensuring the confidentiality of the encryption process [7].

This paper proposes an innovative image encryption and decryption algorithm that combines chaotic systems and RSA cryptography. The chaotic system generates a pseudo-random key to encrypt the image, while RSA cryptography is employed for secure key exchange. The aim is to design an algorithm that enhances the security of image data while maintaining the efficiency and practicality of the encryption/decryption processes.

2. LITERATURE REVIEW

A review of existing encryption techniques reveals the growing importance of combining chaos theory with conventional cryptographic algorithms. Studies indicate that chaotic systems, when combined with RSA, offer improved security by making the encryption process highly unpredictable. However, the challenge remains in designing algorithms that are both computationally efficient and secure [8]. In an increasingly digital world, the protection of sensitive visual data has become paramount, as unauthorized access to image information can result in significant privacy breaches. Encryption methods serve as a critical line of defence, transforming accessible images into indecipherable formats for anyone without the decryption key [9]. By employing sophisticated techniques such as chaotic systems and RSA cryptography, researchers have developed advanced algorithms that ensure the security and integrity of image data. Furthermore, the link between fractal sets and public-key cryptography demonstrates the potential for innovative approaches to encryption, aimed at safeguarding images during transmission and storage. With ongoing advancements in encryption technologies, the significance of robust image security will continue to grow, underscoring the necessity for effective protective measures [10].

Traditional encryption techniques for image data typically rely on block ciphers or stream ciphers. For example, the AES algorithm has been widely used for encrypting images. However, AES is designed for general data encryption and may not fully exploit the spatial and statistical properties of images. Liu et al. (2015) [11] proposed an image encryption scheme using AES combined with a pixel shuffling technique, where image pixels are rearranged before encryption. Although effective in certain cases, these schemes are vulnerable to known-plaintext attacks and may not be sufficient for high-security applications. To address the shortcomings of traditional encryption methods, researchers have increasingly turned to chaotic systems, which offer more robust security features. Chaotic maps, such as the Logistic map and Henon map, have been utilized to generate pseudo-random sequences for encryption. Chaotic systems exhibit sensitive dependence on initial conditions, making it difficult to predict or reverse the encryption without knowledge of the initial system state [12]. Xun Yi (2013) [13] introduced a chaotic encryption method that uses the Logistic map to generate keys for pixel scrambling, achieving higher levels of security compared to traditional methods. The application of chaotic systems in image encryption has garnered significant attention in recent years. Tao et al. (2016) [14] demonstrated how the Logistic map can be employed for pixel-level permutation and diffusion in image encryption. This method achieves a high level of confusion and diffusion, which are essential principles in cryptography for securing image data. Similarly, Chen et al. (2014) explored the use of the Arnold cat map in combination with a chaotic key generator to perform encryption in the frequency domain, providing both spatial and frequency domain security for image data [15].

3. MATHEMATICAL BACKGROUND

The combination of chaotic systems and RSA cryptography has gained significant attention to exploit the advantages of both approaches. Zhou et al. (2018) proposed a hybrid encryption scheme that combines RSA and a chaotic system for encrypting medical images. In their approach, the chaotic system generates a sequence of pseudo-random numbers for pixel shuffling, and RSA is used to encrypt the key. The hybrid system exhibited high resistance to various attacks, including differential and statistical attacks [16].

3.1 CHAOTIC MAP FOR ENCRYPTION:

A chaotic map, such as the Logistic Map or Tent Map, is used to generate a pseudorandom sequence. The chaotic sequence is employed to shuffle the image pixel positions and modify pixel values. Understanding the principles of chaotic systems is crucial in enhancing the security of cryptographic methods. Chaotic systems are characterized by their sensitivity to initial conditions, leading to unpredictable outcomes while adhering to deterministic rules. This property is particularly beneficial in cryptography, as it introduces complexity and randomness into the encryption process [17].

The integration of chaotic systems with traditional cryptographic algorithms, such as RSA, can significantly strengthen security measures by implementing unpredictable key generation methods. As noted, the hybrid approach benefits from the unpredictability of chaos in key management, while also leveraging the established security of RSA algorithms through the difficulty of integer factorization. Furthermore, by incorporating principles of diffusion and confusion, as suggested in previous studies, encryption algorithms can achieve higher levels of security, effectively protecting sensitive data from unauthorized access. Ultimately, the synergy between chaotic systems and established cryptographic techniques offers a promising avenue for developing robust encryption systems [18].

Chaotic systems are deterministic but appear random due to their sensitive dependence on initial conditions. For this algorithm, the Logistic Map is used to generate a pseudo-random sequence. In this work, we use a Logistic Map to generate chaotic sequences. The Logistic Map is defined by the equation:

$$x_{n+1} = r \, . \, x_n(1 - x_n) \qquad (1)$$

where:

- x_n is the state of the system at iteration n,
- r is the control parameter (typically $3.57 \leq r \leq 4$ for chaotic behaviour),
- x_0 is the initial condition (a number between 0 and 1).

This system generates a chaotic sequence that can be used for pixel permutation [19].

3.2 RSA ALGORITHM

The RSA algorithm is used for key generation, encryption, and decryption. The application of RSA cryptography in image decryption represents a significant advancement in data security, particularly in safeguarding sensitive visual information. By leveraging the mathematical complexity of prime factorization, RSA creates a secure framework for decrypting images that have been encrypted for confidentiality [20]. This method allows for the successful transmission and retrieval of image data, ensuring that only authorized users can access the original content. Additionally, the integration of chaotic systems further enhances the robustness of RSA by introducing unpredictability and diversity in key generation, which complicates potential attacks. As observed, the main strength of the proposed system is the chaotic variable key generator that changes the value of encrypted message whenever a different number of keys is used. Moreover, combining RSA with chaos theory not only improves encryption strength but also increases both performance and security in image decryption tasks, solidifying its role in modern cryptographic techniques [21-22].

RSA cryptography is a well-known asymmetric encryption algorithm that has been widely adopted for secure data exchange. In RSA, a pair of keys a public key and a private key—are used for encryption and decryption, respectively. The primary advantage of RSA is that it allows the secure exchange of keys over an insecure communication channel, ensuring that only authorized users can access the encrypted data [24-25].

The RSA key generation process is as follows in detail:

Step 1. Two large prime numbers can be selected randomly, p and q.

Step 2. One key member N and Euler's totient function $\varphi(N)$ can be

calculated by:

$$N = p \times q, \qquad \varphi(N) = (p-1) \times (q-1) \tag{2}$$

Step 3. The encryption keys can be selected randomly that meet the

following two conditions:

$$1 < e < \varphi(N), \qquad \gcd(e, \varphi(N)) = 1 \tag{3}$$

where the logic expression $\gcd(e, \varphi(N))$ presents the great common divisor

between e and $\varphi(N)$, that is, e and $\varphi(N)$ are prime numbers.

Step 4. The decryption key d can be calculated by the following

formula:

$$e \cdot d = 1 (\mathrm{mod}\ \varphi(N)), \quad 0 \leqslant d \leqslant N \tag{4}$$

where mod $\varphi(N)$ represents the modulo operation. Given the above, the public key (e, N) and the private key d can be computed. In the encryption process, the plaintext string information is represented as a plurality of groups, and is set to a decimal number string M which is shorter than the bit length of N.

First, the encryption operation is performed on each plaintext group M using the public key (e, N):

$$C = E(M) \equiv M^e \bmod N \tag{5}$$

where C denotes the ciphertext and $E(M)$ is the encryption operation.

The decryption operation using the private key (d, N) is as follows:

$$M' = D(C) \equiv C^d \bmod N \tag{6}$$

where $D(C)$ is the decryption operation, when the decryption is completed,

$M' = M$.

RSA operates on integer values and requires significant computational resources, making it slow for encrypting large data like images directly. RSA encryption/decryption involves large prime number operations and modular exponentiation, which is computationally expensive. Images, being large, contain many pixel values that require processing. Directly encrypting each pixel using RSA would not only be inefficient but would also require considerable time and resources [26].

4. PROPOSED IMAGE ENCRYPTION AND DECRYPTION ALGORITHM

Figure 2 illustrates that in the event that a cryptanalyst is able to crack the RSA algorithm's key, the second encryption algorithm the Chaos-based algorithm must be solved in order to retrieve the original image. This will ensure that the cipher's strength is guaranteed.

4.1 Image Encryption Using Chaotic System and RSA

Step 1: Chaotic Pixel Permutation

- Given an image I with $M \times N$ pixels, apply the Logistic Map to generate a chaotic sequence $\{c_1, c_2, c_3 \dots \dots, c_{M.N}\}$. This sequence is used to permute the pixels of the image.
- Let P denote the permutation matrix derived from the chaotic sequence. The permuted image I_{perm} is obtained by rearranging the pixels in I based on the order provided by c_i:

$$I_{perm}[i] = I[c_i]$$

where $I[i]$ represents the pixel at position i in the original image.

Step 2: RSA Encryption of the Image or Key

- After the chaotic permutation, the resulting image can be encrypted further using RSA. This can be done either by directly encrypting the permuted image or encrypting a key (e.g., the chaotic sequence) used to permute the image.
- Let K be the key (which could be the permuted image or a secret value), and (n, e)be the RSA public key. The RSA encryption of K is:

$$K_{enc} = K^e (mod\ n)$$

Step 3: Final Encrypted Image

- The final encrypted image is the result of both chaotic pixel permutation and RSA encryption:

$$I_{enc} = RSA\_Encrypt\big(I_{perm}, (n, e)\big)$$

4.2 Image Decryption Using RSA and Chaotic System

Step 1: RSA Decryption

- Given the encrypted image I_{enc}, the first step in decryption is to use the private RSA key (n, d) to decrypt the image data:

$I_{perm} = I_{encd} (mod\ n)$,

This gives the permuted image I_{perm}.

Step 2: Reverse Chaotic Pixel Permutation

- The next step is to reverse the chaotic pixel permutation. The chaotic sequence $\{c_1, c_2, c_3 \dots \dots, c_{M.N}\}$used to permute the image can be reversed by using the inverse of the chaotic system, which can be achieved by sorting the chaotic sequence in reverse order to obtain the original pixel positions.

- Let $\{c_1, c_2, c_3 \dots \dots, c_{M.N}\}$be the chaotic sequence. The inverse chaotic sequence $\{{c_1}^{-1}, {c_2}^{-1}, {c_3}^{-1} \dots \dots, {c_{M.N}}^{-1}\}$is computed by sorting the chaotic values in reverse order. Using this inverse sequence, the original image is restored by applying the inverse permutation:

$$I = P^{-1}(I_{perm})$$

where P^{-1} represents the inverse permutation matrix.

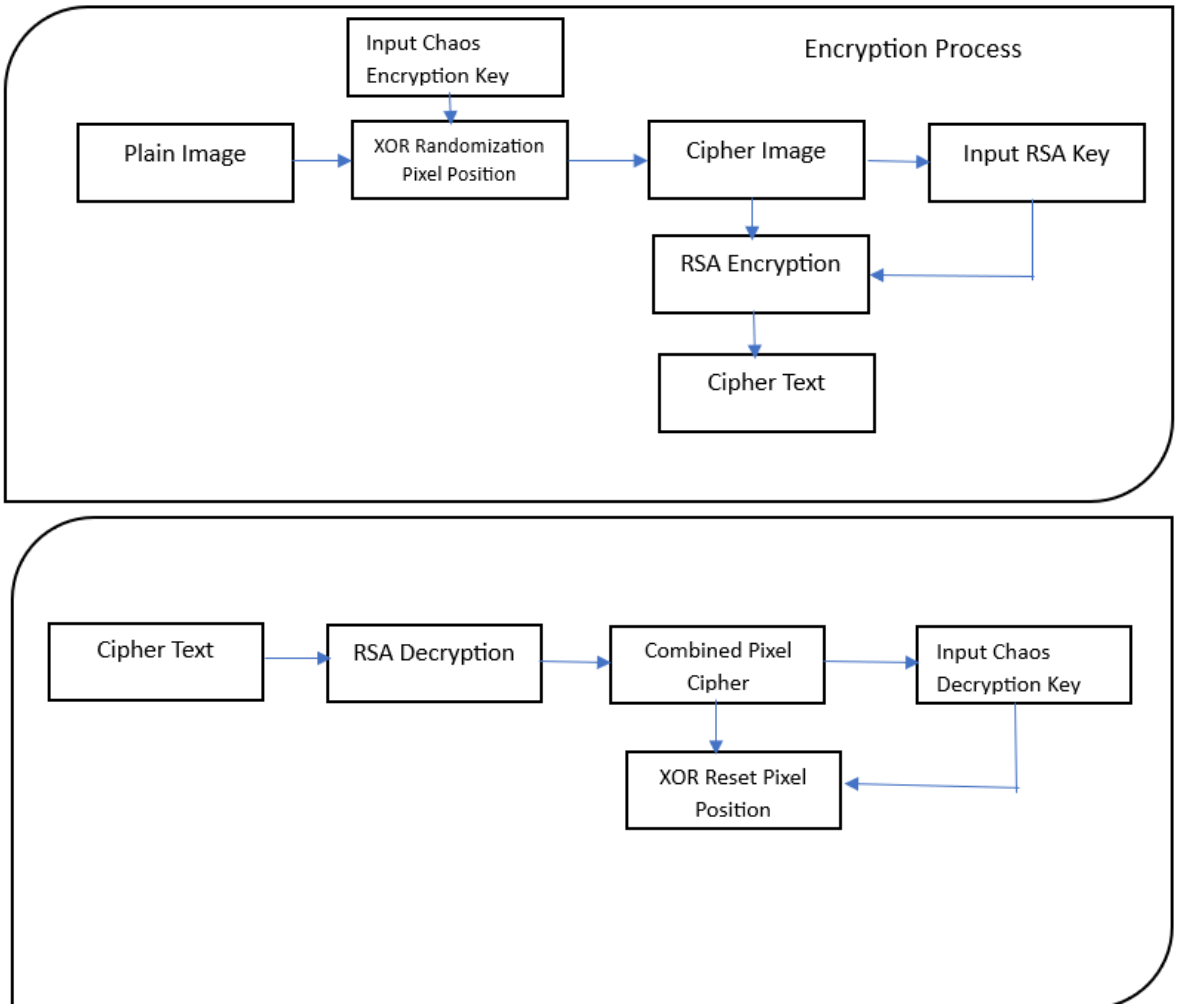


Figure-2. Flowchart of Proposed Scheme

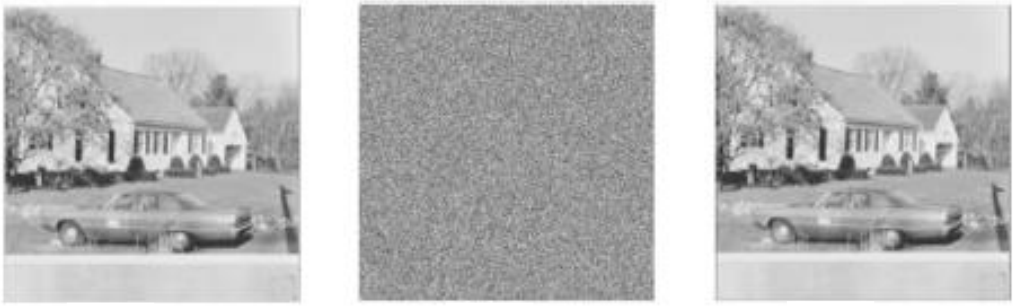
5. RESULTS AND DISCUSSION

Our impressions of the results confirm that the RSA calculation, one of the most remarkable encryption computations available today, is the calculation used in this framework. By passing through a crucial length of up to 2048 pieces, the calculation's strength is increased and the likelihood of key breaking by intruders is reduced. In the main scenario, we were gradually developing the keys and storing them on the computer as documents so that we could use them again without having to input data and make calculations again. Additionally, this development reduces the framework's lengthy key age calculations, so we briefly summarize the time spent on encryption and unscrambling, which is one of the primary drawbacks of the RSA calculation.

The algorithm is evaluated based on the following criteria:

5.1. Validation of the Scheme

The combination of RSA with chaotic maps makes it difficult to break the encryption without the keys. To be called a secure encryption algorithm, the keys should have high sensitivity to any change. That is to say, when the decryption key changes slightly, the original plain image cannot be decrypted and result is absolutely different from that of the plain image. As shown in Fig. 3, we choose the plain image for the test. It can be observed from Figs. 3(a), 3(b), and 3(c) that when the secret key changes 10^{-14}, the decrypted images are like white noise image. Therefore, it shows that the algorithm has high key sensitivity and can resist brute force attacks.



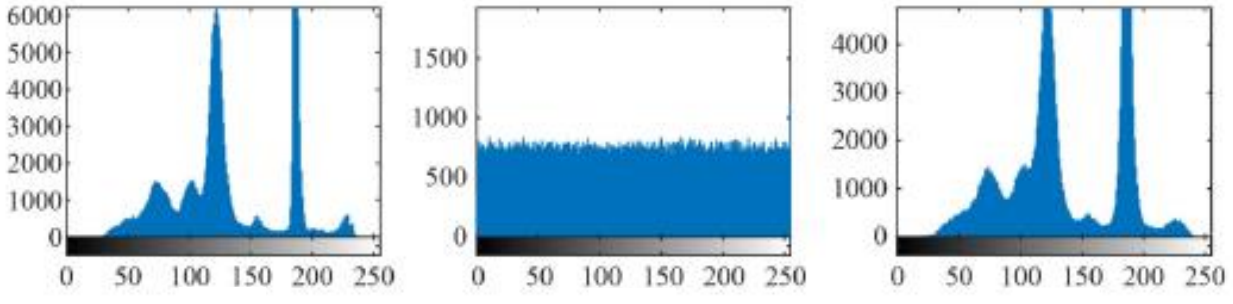
(a) (b) (c)

Figure 3: Results of the test images (a) original image, (b) encrypted image (c) original

The encryption and decryption times are compared with conventional methods. Image quality is evaluated by comparing the original and decrypted images.

5.2. Histogram analysis

Histogram is commonly used to show the distribution of pixels in an image. For a meaningful plain image, the distribution of pixels is relatively concentrated, so the histogram is uneven. For a good meaningful encryption scheme, the histograms of the original carrier image and the carrier image containing secret image should keep the same to show good performance. is set in our test. As shown in Fig. 4, the plain images, i.e., 256 × 256 grayscale image Art and color image Boat are selected, the carrier images, i.e., 512×512 grayscale images Baboon, Peppers, and color image Sun are also selected. Figures. 4(a) and 4(c) are the carrier images with their corresponding histograms.



(a) (b) (c)

Figure 4. Histogram Analysis of (a) Input Image, (b) Encrypted Image, (c) Decrypted Image

5.3. Noise Attacks

Noise Attacks are typically used to test the robustness of encryption systems by adding random noise to the encrypted data, potentially corrupting it and making decryption difficult. In an image encryption system based on chaotic systems and RSA, the analysis would involve introducing various types of noise (e.g., Gaussian noise, salt-and-pepper noise) and then examining the effect on the decrypted image. The goal is to analyze how resilient the encryption scheme is to such attacks. Ideally, a good encryption scheme should make the decrypted image appear as random noise when the encryption key or the image data is tampered with. Furthermore, the image should still be recoverable once the noise is removed or corrected.

Advantages and Challenges

- **Advantages:**

o Combining chaotic systems and RSA encryption leverages both the unpredictable nature of chaos and the mathematical security of RSA, making it hard for attackers to decrypt the image without access to the secret key.

o Histogram analysis helps assess the encryption's robustness by ensuring the image's pixel distribution is well-randomized.

- **Challenges:**

o Computational Complexity: The use of both chaotic systems and RSA encryption can increase the complexity, especially for larger images.

o Key Management: Proper management of the keys (especially the RSA private key) is essential to ensure the system remains secure.

o Performance: The use of chaotic systems and RSA may lead to slower encryption/decryption times compared to simpler encryption methods.

6. CONCLUSION

This research presents an image encryption and decryption algorithm that leverages both chaotic systems and RSA cryptography. The hybrid approach offers strong security and practical implementation for protecting image data. Future work includes optimizing the algorithm for faster encryption and exploring other chaotic maps for improved performance.

In conclusion, the integration of chaotic systems with RSA cryptography significantly enhances the security and efficiency of image encryption and decryption algorithms. The study demonstrates that employing Chebyshev polynomials not only introduces desirable properties into the cryptographic process but also creates a more robust framework against potential attacks, as indicated by the introduction of complex intermediate Furthermore, the combination of Dependent-RSA and chaotic mappings offers a dual-layer of security, where attackers face two levels of reverse engineering to compromise the encryption This approach not only minimizes the computational overhead but also ensures that the rapid development of digital image sharing remains protected from evolving cybersecurity threats. Ultimately, the findings underscore the necessity for continuous innovation in cryptographic methods to maintain data integrity and confidentiality in an increasingly digital world.

Acknowledgements: I would like to express my heartfelt gratitude to my research supervisor Dr. Sanjay Yadav, & Dr. Rajni Rohila for their invaluable guidance, expertise, and support throughout the course of this research.

I want to extend my sincere gratitude to my colleagues for their support and collaboration.

References

1. Stallings, William, Cryptography and Network Security: Principles and Practice. Prentice-Hall, New Jersey, 2004.
2. Taki, A. E., Deen, E., & Gobran, S. N. "Digital Image Encryption Based on RSA Algorithm," *9*(1), 69–73, 2014.
3. Arabind Kumar, Sanjay Yadav and Tarul Garg, "Phase-Image-Encryption-Based Elliptic Curve and Double-Random-Phase Encoding" in Engineering Proceedings MPDI, January 2024.
4. Zhang Y, Xu B, Zhou NR, "A novel image compression-encryption hybrid algorithm based on the analysis sparse representation" Opt Commun 2017; 392:223–33.
5. Gaur, E. A., & Gupta, E. M., "Review: Image Encryption Using Chaos Based algorithms", International Journal of Computer Applications *4*(3), 904–907, 2014.
6. Arabind Kumar, Sanjay Yadav, "A New Image Encryption Scheme Using RSA Cryptosystem and Arnold Transformation" in Advances in Computational Intelligence, Algorithms for Intelligent System, 2023, pp. 187-198
7. Pahrul Irfan, Yudi Prayudi, Imam Riadi, "Image Encryption using Combination of Chaotic System and Rivers Shamir Adleman (RSA)" International Journal of Computer Applications (0975 – 8887) Volume 123 – No.6, August 2015
8. A. M. T. Othman, "Chaotic encryption systems for image data," International Journal of Computer Applications, vol. 92, no. 14, pp. 28–33, 2013.
9. Zhao TY, Ran QW, Chi YY, "Image encryption based on nonlinear encryption system and public-key cryptography" Opt Commun 2015; 338:64–72.
10. L. S. Z. Wang, Z. Y. Wang, and C. M. Zhang, "A novel image encryption algorithm based on chaotic system and DNA sequence," International Journal of Security and Its Applications, vol. 9, no. 7.
11. Ying Liu, Wei Zhang, Xinxia Peng, Yan Liu, Sida Zheng, Tongjia Wei, "Design of password encryption model based on AES algorithm" International Conference on Civil Aviation Safety and Information Technology (ICCASIT), January 2020.
12. Bowen Zhang and Lingfeng Liu, "Chaos-Based Image Encryption: Review, Application, and Challenges", Chaos-Based Secure Communication and Cryptography, June 2023.
13. Ziaur Rahman, Xun Yi, Ibrahim Khalil, Mousumi Sumi "Chaos and Logistic Map Based Key Generation Technique for AES-Driven IoT Security" Lecture Notes of the Institute for Computer Sciences, November 2021.
14. Tao, X., et al. (2016). "Image encryption based on chaotic maps," Journal of Mathematical Imaging and Vision.
15. Young-Long Chen, Chung-Ming Cheng, "Combining a chaos system with an Arnold cat map for a secure authentication scheme in wireless communication networks", Engineering Computations ISSN: 0264-4401, February 2014.

16. Zhou, X., et al. "Hybrid image encryption using RSA and chaotic systems," International Journal of Computer Science and Applications 2020.
17. Amin, M., Faragallah, O. S., & Abd El-Latif, A. A. (2010) “A chaotic block cipher algorithm for image cryptosystems. Communications in Nonlinear Science and Numerical Simulation” 15, 3484–3497.
18. Awad, A. dan Saadane, A. “New Chaotic Permutation Methods for Image Encryption.” International Journal of Computer Applications Volume 123 - Number 6, 2015.
19. Jakub Oravec, Lubos Ovsenik, Jan Papaj, “An Image Encryption Algorithm Using Logistic Map with Plaintext-Related Parameter Values” Entropy (Basel). 2021 Oct 20;23(11):1373.
20. Gaur, E. A., & Gupta, E. M., “Review: Image Encryption Using Chaos Based algorithms”, International Journal of Computer Applications *4*(3), 904–907, 2014.
21. Aradhana Sahoo, Pratyasha Mohanty, Purna Chandra Sethi, “Image Encryption Using RSA Algorithm” Intelligent Systems, Proceedings of ICMIB 2021.
22. Arabind Kumar, Sanjay Yadav, “A New Image Encryption Scheme Using RSA Cryptosystem and Arnold Transformation” in Advances in Computational Intelligence, Algorithms for Intelligent System, 2023, pp. 187-198.
23. Radhakrishna M, Shridevi K S, Sowmya B S, Sushmitha T J, “Digital Image Encryption and Decryption based on RSA Algorithm” International Journal of Scientific Research in Science Engineering and Technology, July 2022.
24. Shantappa G Gollagi, R Srividya, G Santhosh Kumar, Piyush Kumar Pareek, “A New Method of Secure Image Encryption by Using Enhanced RSA Algorithm” International Conference on Forensics, Analytics, Big Data, Security (FABS), 2021.
25. Yujia Liu, Zhaoguo Jiang, Xiping Xu, Fuqi Zhang, Jiahong Xu, “Optical image encryption algorithm based on hyper-chaos and public-key cryptography” Optics and Laser Technology 127 (2020) 106171.
26. Zhang, Y., et al. (2017). "A hybrid image encryption algorithm using RSA and chaotic systems," Security and Privacy.