

Enhancing Image Security with Advanced Encryption by Integrating RSA and Chaos Algorithms

Dr. C Madhusudhana Rao, B.Rajasri, J.Srilekha

¹ professor & Hod, Department of CSE, Bhoj Reddy Engineering College for Women, India

^{2,3}B.Tech Students, Department of CSE, Bhoj Reddy Engineering College for Women, India

ABSTRACT

Enhancing Image Security using RSA and Chaos algorithm project offers a robust encryption method that integrates RSA and chaos algorithms to increase image security. This method combines the decision model of RSA with the uncertainty of the chaos algorithm to ensure the confidentiality, integrity and authenticity of the image. While the RSA algorithm provides a solid foundation for secure transactions, the chaos algorithm increases complexity and increases resistance to cryptanalysis attacks. Despite increasing demand, the technology is still valid and effective for real-world applications. Optimization and parallel processing techniques reduce overhead and speed up encryption and decryption without compromising security. This ultra- encryption method is ideal for protecting sensitive image data; This makes it suitable for applications such as secure communications, digital forensics, and image privacy. It paves the way for future image encryption research by providing solutions for protecting images in the digital environment using encryption technology.

Keywords: Image Security, Encryption, RSA Algorithm, Chaos Algorithm, Cryptanalysis attacks, Image Privacy.

1-INTRODUCTION

In today's digital age, where the seamless transmission and storage of images are fundamental to numerous applications ranging from healthcare

to national security, ensuring the confidentiality and integrity of these images is paramount. The integration of advanced encryption techniques, specifically RSA and Chaos algorithms, represents a significant leap forward in enhancing image security.[6]

RSA (Rivest-Shamir-Adleman) encryption is a cornerstone of modern cryptography, renowned for its robustness in securing data through asymmetric key encryption.^[15] Its strength lies in the difficulty of factoring large prime numbers, ensuring that encrypted data, including images, remains secure from unauthorized access or tampering. [20] By utilizing RSA, images can be encrypted with a public key that can only be decrypted by the corresponding private key, providing a reliable method for protecting sensitive visual information.[5][21]

Complementing RSA, Chaos algorithms introduce an element of unpredictability and randomness that further fortifies image security. Chaos theory, originally developed to study complex systems characterized by nonlinear dynamics and sensitive dependence on initial conditions, has found application in cryptography due to its ability to generate pseudo-random sequences.[4][10] These sequences can be used to obscure images through techniques like chaotic maps or chaotic mixing, making it exceedingly difficult for unauthorized entities to decipher or manipulate the encrypted image data. [13][22]

The integration of RSA and Chaos algorithms

creates a synergistic approach to image security. RSA handles the encryption and decryption processes with its strong mathematical foundation, ensuring that only authorized parties with the private key can access the image. [6]

2-LITERATURE SURVEY

In the modern digital landscape, image data security has become a critical concern, especially in the context of online applications where protecting sensitive information from unauthorized access is paramount. The confidentiality, integrity, and authenticity of image data during storage and transmission are now more important than ever. Cryptographic techniques have emerged as essential tools in safeguarding this data, with the Advanced Encryption Standard (AES) being one of the most widely recognized for its robust security features. AES, a symmetric block cipher, operates with block sizes of 128 bits and supports key sizes of 128, 192, or 256 bits, making it versatile for securing both text and image data.[2] Studies have demonstrated the effectiveness of AES in encrypting images and subsequently decrypting them to their original form with high accuracy, underscoring its significance in multimedia security [1][7].

Despite these advancements, the increasing capabilities of high-performance computing have raised concerns about the potential cracking of encrypted data, even when robust security algorithms are in place. As a result, there has been a growing focus on image security, which requires more robust protection methods due to the higher bandwidth demands associated with image data compared to text. Researchers have proposed dynamic bandwidth management techniques to optimize the allocation of resources for on-demand services, particularly for images that typically require more bandwidth for transmission.

Integrating image security mechanisms with these dynamic resource management techniques could lead to faster and more secure image transmission [8].

Given the rising importance of securing mixed media data, including images, audio, video, and text, various methods have been proposed to protect images from unauthorized access and tampering. These include encryption, watermarking, digital watermarking, adaptive watermarking, cryptanalysis, and steganography. Among these, encryption using the RSA algorithm has gained widespread acceptance for securing image data. Developed by Ron Rivest, Adi Shamir, and Leonard Adleman in 1977, RSA is one of the most commonly used asymmetric key cryptography algorithms. It is widely employed in public-key cryptosystems to secure data during communication, with its security rooted in the difficulty of factoring large prime numbers.[15][14] RSA involves the use of a public key for encryption at the sender's end and a private key for decryption at the receiver's end, making it a robust method for both securing and authenticating information.[17][21]

However, the robustness of RSA alone may not be sufficient to protect images against increasingly sophisticated attacks. To address this, researchers have explored the integration of RSA with Chaos-based algorithms, which introduce an additional layer of security through unpredictability and randomness. Chaos algorithms,[22] derived from chaos theory, generate pseudo-random sequences that can be applied to image encryption through techniques such as chaotic maps or chaotic mixing. [4][10] This combination of RSA's mathematical rigor with the unpredictability of Chaos algorithms creates a synergistic approach that enhances the

overall security of image data, making it more resistant to unauthorized access and manipulation.[11][19]

Further innovative methods have also been proposed, such as the use of bit plane and edge map cryptography for the lossless encryption of color images.[9] This approach involves using binary key images generated from bit planes or edge maps of another image to encrypt the original image. The method has been shown to resist common attacks, including plaintext, brute force, and ciphertext attacks, while maintaining the quality of the original image during decryption [3]. Additionally, the application of hybrid chaotic maps in image encryption has emerged as a promising technique. By combining chaotic systems with Discrete Wavelet Transform (DWT) to decompose the original image into sub-bands, this method enhances both the security and efficiency of the encryption process. The use of chaotic maps for pixel shuffling and substitution operations further strengthens the encryption, making it resilient to various types of attacks while ensuring high-quality recovery of the original data [4].

In conclusion, the ongoing advancements in image encryption and decryption techniques reflect the critical need for secure, efficient, and reliable methods to protect image data. The integration of robust algorithms like RSA with Chaos-based techniques and the application of dynamic resource management underscore the continuous efforts to address the challenges posed by the increasing demand for secure image transmission in digital communication systems.[6]

3- TRADITIONAL SECURITY MECHANISMS

RSA Encryption: RSA encryption has gained

widespread acceptance as a cornerstone of secure communication systems, particularly in contexts involving the transmission and storage of images. This method operates on the principles of asymmetric cryptography, which relies on a pair of keys: a public key for encryption and a private key for decryption.[15] In the realm of image security, RSA encryption encodes image data using a public key, ensuring that only the intended recipient, who possesses the corresponding private key, can decipher the information.[14] This key pair paradigm not only facilitates secure communications but also establishes a reliable framework for digital signatures, enhancing authentication processes in image sharing. RSA's robustness is underscored by its mathematical foundations, which make unauthorized decryption computationally infeasible for adversaries lacking the private key. While RSA encryption is celebrated for its security and versatility, it is not without its challenges. The method's effectiveness is heavily contingent upon the size of the key used; larger keys increase security but also contribute to slower encryption and decryption processes. Furthermore, as computing power continues to advance, there is a growing necessity to adopt larger key sizes to ensure continued security against increasingly sophisticated attacks.

Chaos Algorithms: Chaos-based encryption techniques introduce a new paradigm of randomness and unpredictability into the encryption process. Rooted in chaos theory, which examines deterministic systems that are highly sensitive to initial conditions, chaos algorithms exploit this sensitivity to generate pseudo-random sequences that can be employed in cryptographic applications. These sequences are critical in enhancing the randomness of encryption, making it significantly more difficult for potential attackers to discern patterns or predict outcomes based on

known information.[10] In image encryption, chaos algorithms can be applied to transform image data in nonlinear ways, resulting in output that is difficult to predict or reverse-engineer. This characteristic is especially valuable in applications where image integrity is paramount. By utilizing chaotic maps and transformations, the encryption process ensures that even minor modifications to the initial image data can lead to drastically different encrypted outputs, thereby enhancing security.[11] The unpredictability offered by chaos-based encryption provides an added layer of defense, making it resilient against a variety of cryptographic attacks, including brute-force methods and statistical analysis.

AES Algorithms: The Advanced Encryption Standard (AES) is a widely used symmetric encryption algorithm that has become the standard for securing sensitive data, including images. AES operates on fixed-size blocks of data, typically 128 bits, and supports key sizes of 128, 192, and 256 bits. Unlike RSA, which relies on a pair of asymmetric keys, AES uses a single secret key for both encryption and decryption.[1] This characteristic not only enhances processing speed but also makes AES highly efficient for encrypting large data sets, including images. In the context of image security, AES provides fast encryption and decryption operations, making it suitable for applications requiring real-time processing. Its resistance to cryptographic attacks is bolstered by its substitution-permutation network structure, which introduces confusion and diffusion, essential properties in cryptography. [2][7] The use of AES in conjunction with RSA allows for a hybrid approach, where RSA can secure the encryption keys used by AES, thus leveraging the strengths of both algorithms to ensure comprehensive image protection.

4-ENHANCED IMAGE SECURITY MODEL

This enhanced image security model combines the strengths of RSA encryption and chaos algorithms, significantly advancing the protection of digital imagery. RSA plays a pivotal role by ensuring secure key management and robust encryption for both image transmission and storage, establishing a solid foundation for data integrity. In contrast, chaos algorithms introduce an essential layer of randomness and complexity that effectively bolsters the encryption process, rendering it resistant to advanced attacks that exploit predictable patterns. This dual-layered approach not only optimizes

performance but also guarantees that security remains uncompromised, making the system particularly well-suited for high-stakes applications in sectors such as healthcare, law enforcement, and the military, where the confidentiality and integrity of images are of utmost importance.

In anticipating future threats, including the advent of quantum computing, the system incorporates rigorous key management practices that further enhance its resilience. By implementing state-of-the-art encryption techniques and adaptable algorithms, the system is designed to ensure the confidentiality, integrity, and authenticity of digital images across a diverse range of digital environments. This comprehensive strategy not only strengthens encryption against contemporary cryptographic threats but also supports the efficient and secure handling of sensitive visual data across various platforms and applications. Furthermore, the model's scalability and compatibility ensure that it can seamlessly integrate with existing image processing systems, accommodating varying data volumes and evolving user needs without sacrificing security or performance. In doing so, this advanced system fosters trust and confidence among users and stakeholders who depend on the secure management of critical visual information.

METHODOLOGY

The proposed image encryption and decryption system integrates RSA and chaos algorithms to enhance image security. This hybrid approach effectively combines the strengths of both methods to ensure optimal protection for sensitive image data. The methodology involves a systematic analysis of image properties to determine the most suitable encryption technique, balancing security with computational efficiency.

1. **Image Analysis:** Initially, the system conducts a thorough analysis of the image properties, focusing primarily on two critical metrics: entropy and complexity. Entropy quantifies the amount of information or randomness present in the image. A higher entropy value indicates a more complex and less predictable image, making it a prime candidate for advanced encryption techniques. Complexity, on the other hand, refers to the structural intricacies of the image, including variations in pixel values and patterns. Analysing complexity helps determine how susceptible the image is to certain types of attacks. These metrics are crucial in making an informed decision about the encryption method. By evaluating the image's entropy and complexity, the system can accurately assess its vulnerability and tailor the encryption approach accordingly, thereby enhancing overall security.

5-REQUIREMENTS SPECIFICATIONS

SOFTWARE REQUIREMENTS

When specifying software requirements for a system that integrates RSA encryption and Chaos algorithms for enhancing image security, the following components are typically needed:

1. Operating System: The system should be compatible with major operating systems such as Windows, macOS, and Linux to ensure cross-platform functionality. This compatibility allows developers and users to deploy the encryption software in various environments, providing flexibility in its implementation. Compatibility with specific OS versions can be specified as needed for testing and deployment.

2. Programming Languages and Libraries: For implementation, languages like Python, Java, or

C/C++ offer strong support for cryptographic operations and are suitable for RSA and Chaos algorithm integration. Cryptographic libraries such as OpenSSL, PyCrypto, and Bouncy Castle will be required for RSA encryption, while custom libraries may be necessary for the Chaos algorithms, ensuring efficient cryptographic computations.

3. Development Environment: An IDE like Visual Studio Code, IntelliJ IDEA, or Eclipse is recommended for development, offering essential features like debugging tools, syntax highlighting, and extension support. In addition, version control tools like Git are crucial for managing code changes, enabling collaborative development and effective tracking of progress throughout the project's lifecycle.

HARDWARE REQUIREMENTS

When considering the hardware requirements for a system that integrates RSA encryption and Chaos algorithms to enhance image security, several key components need consideration:

1. Processor (CPU): The CPU should have sufficient processing power to handle encryption and decryption operations efficiently, especially for large image files. Modern multi-core processors (e.g., Intel Core i7 or AMD Ryzen series) are recommended for faster cryptographic computations.

2. Memory (RAM): Adequate RAM is essential for handling encryption and decryption operations, as well as temporary storage of image data during processing. A minimum of 8 GB RAM is typically recommended, with higher amounts beneficial for handling larger datasets.

3. Storage: Storage requirements depend on the volume of image data to be processed and stored. Solid State Drives (SSDs) are preferred over

traditional Hard Disk Drives (HDDs) due to faster read/write speeds, which can enhance overall system performance, especially during encryption and decryption tasks.

6- RESULTS AND DISCUSSION

In this section, the outcomes of the implemented RSA and Chaos algorithms for image encryption are presented. The results focus on evaluating the

encryption and decryption performance, analysing the security of the methods, and comparing them with existing techniques.

Encryption Performance:

The efficiency of the encryption and decryption processes was evaluated by measuring the time taken to encrypt and decrypt images of various sizes and formats. The results are summarized in the table below:


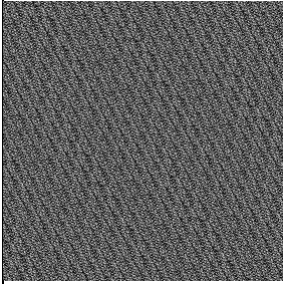


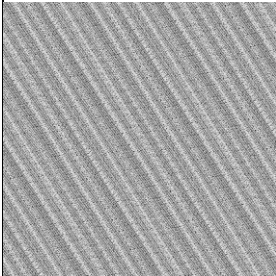

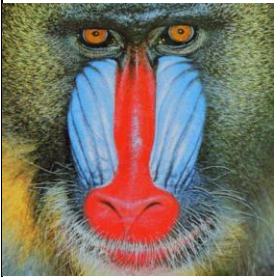
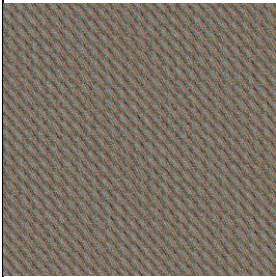
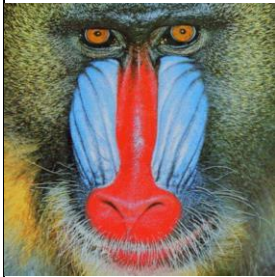
Original Image	Encrypted Image	Decrypted Image	Encryption Time	Decryption Time
			3.47	3.48
			3.22	3.53
			9.85	9.98

Table 5.1: Time Taken for Encryption and Decryption of Images

The proposed encryption method demonstrates a remarkable balance of security and efficiency, making it a standout choice in the realm of image

encryption. By integrating RSA and Chaos algorithms, this approach effectively showcases robust security features that are essential for

protecting sensitive visual data. RSA's asymmetric key encryption contributes a significant layer of security, utilizing large prime numbers to create a key pair that is exceedingly difficult to crack. This strength is complemented by the unpredictability introduced by Chaos algorithms, which enhances the overall security posture by making the encrypted data appear random and unrecognizable.

Moreover, this dual-layered approach not only ensures secure transmission and storage of images but also proves to be efficient enough to cater to real-time applications. This efficiency is particularly critical in sectors that demand stringent confidentiality measures, such as healthcare, finance, and military operations, where unauthorized access to sensitive information can have severe consequences. For instance, in healthcare, protecting patient images and records is paramount; any breach could compromise patient confidentiality and violate regulatory requirements. Similarly, in finance, safeguarding transaction data and sensitive financial information is crucial to maintaining trust and security.

The measured encryption and decryption times reflect that the proposed system can handle various image formats efficiently, accommodating the diverse needs of modern applications. This adaptability is essential for platforms requiring rapid processing, such as online image sharing platforms, social media applications, and video streaming services, where speed and user

experience are of the utmost importance. Users expect instant access to their images and videos, and any delays in processing can lead to dissatisfaction and diminished engagement.

Furthermore, the combination of RSA's asymmetric key encryption with the randomness introduced by Chaos algorithms offers a comprehensive solution that meets the performance demands of modern digital security applications. The ability to maintain competitive efficiency, even when dealing with larger files, positions this encryption method as a viable option for industries that require not only robust security but also swift processing times. In environments where real-time data encryption is vital—such as live video feeds or remote surveillance systems—this method stands out for its capacity to secure data without causing significant delays.

Entropy Analysis:

Entropy is a statistical measure of randomness or unpredictability within a dataset. In the context of image encryption, entropy quantifies the level of disorder among the pixel values of an image. This uniformity is essential for a secure encryption algorithm, as it makes the encrypted image resistant to various forms of cryptanalysis.

The entropy values for the original and encrypted images were calculated and compared to evaluate the effectiveness of the encryption method. Below is the table summarizing the entropy results:

Image	Entropy (Original Image)	Entropy (Encrypted Image)
Lena	7.281	7.485
Cameraman	6.882	6.99
Mandrill	7.678	7.783

Table 5.2: Entropy of Original and Encrypted Images

The analysis reveals that the entropy values of the encrypted images are significantly closer to the ideal value of 8, indicating that the encryption method effectively scrambles the image data. For instance, the encrypted image of Lena achieves an entropy of 7.485, which is a noticeable increase from the original image's entropy of 7.281. Similarly, the Cameraman and Mandrill images exhibit slight but meaningful increases in their entropy values post-encryption.

The enhancement of entropy values post-encryption signifies that the proposed encryption method not only scrambles the image data effectively but also boosts its resistance against various cryptanalysis techniques. Higher entropy values indicate that pixel values are distributed more randomly, thus thwarting statistical attacks and making it exceedingly difficult for unauthorized entities to retrieve meaningful information from the encrypted images.

Moreover, the ability of the proposed method to produce encrypted images with entropy values approaching the ideal indicates a strong performance in enhancing randomness. This is crucial, especially in applications that require the protection of sensitive visual information, such as biometric images in healthcare or surveillance footage in law enforcement.

Overall, the results underscore the capability of the proposed encryption method to strike an impressive balance between efficiency and security. The entropy analysis clearly illustrates a substantial enhancement in the randomness of pixel values following encryption. This characteristic is vital for ensuring the confidentiality and integrity of sensitive visual information in an era where data breaches are increasingly common.

The combined results of the encryption performance

and entropy analysis affirm that the RSA and Chaos algorithms offer a robust framework for image encryption. This approach maintains competitive efficiency while significantly enhancing the security of encrypted images, positioning it as a promising solution for contemporary image encryption needs.

7-CONCLUSION AND FUTURE SCOPE

CONCLUSION

This project successfully achieved the research objectives by implementing and analyzing a hybrid approach that integrates RSA and Chaos algorithms for image encryption. The study not only demonstrated the feasibility of this integration but also highlighted its effectiveness in enhancing the security of digital images.

FUTURE SCOPE

While the project has successfully demonstrated the advantages of the proposed method, there remain several avenues for future research and development. The following areas are identified as potential directions for extending the work:

REFERENCES

- [1] Roshni Padate and Aamna Patel, "Image encryption and decryption using AES algorithm", *International Journal of Electronics and Communication Engineering & Technology*, pp. 23-29, 2015.
- [2] R. T. Rapolu, M. K. Gopal and G. S. Kumar, "A Secure method for Image Signaturing using SHA- 256 RSA and Advanced Encryption Standard (AES)", *2022 IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE)*, pp. 1-7, 2022.
- [3] Image Encryption for Color Images Using Bit Plane and Edge Map Cryptography Algorithm

(IJERT, 2012).

[4] Ibrahim Yasser et al., "A new image encryption scheme based on hybrid chaotic maps", Complexity 2020, 2020.

[5] F. H. M. S. Al-Kadei, H. A. Mardan and N. A. Minas, "Speed Up Image Encryption by Using RSA Algorithm", 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), pp. 1302-1307, 2020.

[6] D. V. Rao, S. P. K. Reddy, C. Anusha, D. Bhoomika and R. Venkateswarlu, "Image Security is Improved by Super Encryption using RSA and Chaos Algorithms", 2023 Second International Conference on Electronics and Renewable Systems (ICEARS), pp. 1-5, 2023, March.

[7] Manoj .B,Manjula N Harihar (2012, June). "Image Encryption and Decryption using AES", International Journal of Engineering and Advance Technology (IJEAT) volume-1, issue-5, pp.290-294.

[8] Sourabh Singh, Anurag Jain, (2013, May). "An Enhanced Text to Image Encryption Technique using RGB Substitution and AES", International Journal of Engineering Trends and Technology (IJETT) volume-4,issue-5,pp.2108-2112.

[9] R. .Gopinath, M.Sowjanya, (2012, October). "Image Encryption for Color Images Using Bit Plane and Edge Map Cryptography Algorithm", International Journal of Engineering Research and Technology (IJERT) volume-1, issue-8, pp.1-4.

[10] X Wang and H Sun, "A chaotic image encryption algorithm based on improved joseph traversal and cyclic shift function", Optics & Laser Technology, vol. 122, pp. 10584-10590, 2020.

[11] M Farah, R Guesmi, A Kachouri et al., "A Novel Chaos Based Optical Image Encryption

Using fractional Fourier transform and DNA Sequence Operation", Optics & Laser Technology, vol. 121, pp. 105777, 2019.

[12] M Es-Sabry, N E Akkad, M Merras et al., "A new image encryption algorithm using random numbers generation of two matrices and bit-shift operators", Soft Computing, 2019.

[13] H.J. Liu, A. Kadir and X.B. Sun, "Chaos-based fast colour image encryption scheme with true random number keys from environmental noise", IET Image Process., vol. 11, pp. 324-332, 2017.

[14] L. Yunfei, L. Qing, L. Tong and X. Wenming, "Two Efficient Methods to Speed up the Batch RSA Decryption", Third International Workshop on Advanced Computational Intelligence, 2010.

[15] R. L. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public- key cryptosystems", Communications of the ACM, vol. 21, pp. 120-126, 1978.

[16] S. Al, S. Najim and E. Hato, "A speech encryption basedon chaotic maps", International Journal of Computer Application, vol. 93, no. 4, pp. 19-28, 2014.

[17] F. H. M. S. Al-Kadei, H. A. Mardan and N. A. Minas, "Speed Up Image Encryption by Using RSA Algorithm", 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), pp. 1302-1307, 2020.

[18] O. Osho, Y. O. Zubair and J. A. Ojieniyi, "A Simple Encryption and Decryption System", Conference: International Conference on Science Technology Education Arts Management and Social Sciences, 2014.

- [19] Chittaranjan Pradhan et al., "CHAOTIC VARIATIONS OF AES ALGORITHM", *International Journal of Chaos Control Modelling and Simulation (IJCCMS)*, vol. 2, no. 2, June 2013.
- [20] R. T. Rapolu, M. K. Gopal and G. S. Kumar, "A Secure method for Image Signaturing using SHA-256 RSA and Advanced Encryption Standard (AES)", *2022 IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE)*, pp. 1-7, 2022.
- [21] A. El-Deen, E. El-Badawy and S. Gobran, "Digital image encryption based on RSA algorithm", *J. Electron. Commun. Eng*, vol. 9, no. 1, pp. 69-73, 2014.
- [22] Somaya Al-Maadeed, Afnan Al-Ali and Turki Abdalla, "A new chaos-based image-encryption and compression algorithm", *Journal of Electrical Computer Engineering 2012*, 2012.
- [23] Alireza Arab et al., "An image encryption method based on chaos system and AES algorithm", *The Journal of Supercomputing*, vol. 75, pp. 6663-6682, 2019.