RESEARCH ARTICLE OPEN ACCESS

RSA-Based Encryption for Color Image Security: A Comprehensive Review

Girdhari Jangid*, Dr. Rajeev Yadav**
*M.Tech Student, Department of CSE, Arya College of Engineering, Jaipur, Rajasthan, India
**Professor, Department of CSE, Arya College of Engineering, Jaipur, Rajasthan, India

Abstract:
The exponential growth of digital communication and multimedia applications has intensified the need for secure image transmission and storage. Color images, widely used in medical imaging, defense, social media, and e-commerce, are vulnerable to unauthorized access, tampering, and cyberattacks. Cryptographic solutions play a vital role in ensuring confidentiality, integrity, and authenticity. Among these, the RSA algorithm an asymmetric encryption technique has gained attention for its ability to provide high security based on complex mathematical computations involving large prime numbers. This paper presents a comprehensive review of RSA-based encryption techniques for color image security. It explores their theoretical foundations, applications, strengths, limitations, and integration with hybrid approaches. Furthermore, the study highlights research challenges and future directions in improving computational efficiency, key management, and real-time implementation of RSA in secure image processing.

Keywords: Cryptography, Encryption, Decryption, RSA Algorithm, Digital Image, Colour Image, Gray Image.

1. Introduction

Since Digital images have become a cornerstone of modern communication systems, playing a vital role in diverse fields such as personal photo sharing, healthcare diagnostics, satellite imaging, surveillance, and military intelligence. Their extensive use across both civilian and mission-critical applications underscores the importance of ensuring the security and integrity of image data. As the world continues to transition into the digital age, the volume of visual data transmitted and stored through online platforms, cloud services, and wireless networks has grown exponentially. This rapid expansion has also increased the risks of unauthorized access, data breaches, and malicious cyberattacks, making image security a pressing concern.

Traditional protection mechanisms, including watermarking and steganography, have been employed to safeguard digital images. While these techniques provide certain levels of authenticity, copyright protection, and covert communication, they fall short when it comes to ensuring full confidentiality and resilience against sophisticated attacks. Watermarking primarily protects intellectual property rights, whereas steganography focuses on hiding information within other media; neither method alone offers robust encryption capabilities. In contrast, encryption has emerged as the most reliable approach for maintaining data privacy and security, as it directly transforms the image content into an unintelligible form that is inaccessible to unauthorized users.

Among various encryption algorithms, Rivest–Shamir–Adleman (RSA) encryption stands out due to its asymmetric cryptographic framework, which relies on public and private key pairs for secure communication. RSA provides robust security by making use of complex mathematical operations involving large prime numbers, ensuring resistance against brute-force and cryptanalytic attacks. Its application in the domain of color image encryption is particularly significant, as color images often contain a higher density of sensitive information compared to grayscale

images, thereby requiring advanced encryption schemes. By leveraging RSA, image encryption achieves strong protection for both authentication and privacy, addressing the dual challenges of secure transmission and storage in today's interconnected digital ecosystem.

2. Cryptography and Image Encryption

Encryption is the study and application of techniques designed to ensure secure communication between a sender and a receiver, even in the presence of potential adversaries or unauthorized entities. At its core, encryption transforms data into an unintelligible format using mathematical functions, protocols, and algorithms rooted in disciplines such as mathematics, computer science, and electrical engineering. The process of reversing this transformation, known as decryption, restores the original data using a cryptographic key. In modern communication systems, encryption plays a pivotal role in safeguarding sensitive information, whether in the form of text, data files, images, or videos, against unauthorized access, tampering, or interception.

Modern cryptography is generally classified into two broad categories:

Symmetric Key Cryptography

In symmetric encryption, a single secret key is used for both encryption and decryption. This key must be securely shared between the sender and the receiver, as the security of the system entirely depends on its confidentiality. Symmetric encryption techniques are computationally efficient and suitable for encrypting large amounts of data. However, the challenge lies in securely distributing the secret key.

Asymmetric Key Cryptography

Asymmetric cryptography, also known as public-key cryptography, uses a pair of keys: a public key for encryption and a private key for decryption. The public key is openly available, while the private key remains confidential with the receiver. This approach eliminates the problem of secure key distribution, making it widely used for secure communication. The RSA algorithm is one of the most prominent examples of asymmetric cryptography, offering strong security based on the computational hardness of factoring large prime numbers.

Importance of Image Encryption

The encryption of images is essential to guarantee the safe transfer of visual data over the internet and other communication channels. With the rapid growth of digital communication, applications such as video conferencing, cloud storage, social media sharing, telemedicine, and military surveillance require robust mechanisms to protect image data from unauthorized access or misuse. Encryption ensures that only authorized users can access the image, making it unreadable to third parties.

In fields like telemedicine, encryption secures sensitive medical images, thereby maintaining patient confidentiality. In military communications, it prevents adversaries from intercepting and interpreting critical surveillance or intelligence images. Similarly, in multimedia transmission and cloud-based storage, encryption safeguards personal or proprietary image data from cyberattacks.

From a technical perspective, digital images pose unique challenges for encryption. Images typically consist of a large amount of data with properties such as high frequency, large storage capacity, and strong pixel correlation. These characteristics make conventional text-based encryption methods less effective for images. Thus, specialized encryption techniques are required to handle the complexities of image data while ensuring both security and efficiency.

3. Literature Review

Singh et al. (2025) proposed a robust multilayer image encryption scheme combining the RSA algorithm with chaotic maps, enhancing both confusion and diffusion for grayscale and color images. Their approach demonstrated strong resistance to brute-force and statistical attacks. Similarly, Pavani et al. (2024) developed a multilayer encryption framework for medical images, integrating AES with RSA-based digital signatures to ensure confidentiality, integrity, and authentication. Ali et al. (2024) introduced

a chaos–wavelet hybrid encryption method tailored for healthcare applications, which outperformed AES and RSA in speed and key sensitivity while maintaining image quality.

Huang et al. (2024) advanced optical image encryption by integrating computational ghost imaging with RSA and wavelet transforms, achieving reduced key requirements and high reconstruction quality. Dong et al. (2023) combined a 4D hyperchaotic system with RSA to secure color images, applying scrambling and diffusion techniques that improved efficiency and robustness.

Karthikeyan et al. (2023) highlighted the synergy of cryptography and steganography, embedding RSA-encrypted data into images for dual-layer protection. Ganesamoorthy et al. (2023) compared RSA with an enhanced cryptography principle (EICP), showing improved resilience against unauthorized access. Rao et al. (2023) recommended a hybrid RSA–Chaos approach to balance encryption speed and strength.

Earlier, Edan et al. (2022) optimized RSA for image encryption by adopting a block-based mechanism, which reduced computational overhead while preserving data integrity. Collectively, these studies highlight RSA's adaptability and its effectiveness when combined with chaotic systems, wavelet transforms, or steganography, underscoring its continuing relevance in secure image transmission.

4. Conclusion

The security of digital images has become increasingly critical in today's interconnected digital environment, where images are extensively used in domains ranging from healthcare and defense to social media and e-commerce. This review highlighted the pivotal role of encryption, particularly RSA-based techniques, in safeguarding color image data against unauthorized access, tampering, and cyberattacks.

RSA, as a widely recognized asymmetric encryption algorithm, offers strong security grounded in complex mathematical computations. However, due to its high computational overhead and limitations in handling large image data directly, researchers have explored hybrid approaches that combine RSA with chaos theory, wavelet transforms, steganography, and other cryptographic methods. These integrations not only enhance confusion and diffusion but also address efficiency challenges, making RSA-based schemes more practical for real-time applications.

The reviewed literature confirms that RSA-based image encryption provides robust security and adaptability across multiple applications. Nonetheless, key challenges remain in optimizing computational efficiency, reducing processing time, managing key distribution effectively, and ensuring scalability for high-resolution color images. Addressing these challenges is essential for future advancements in RSA-based image security.

In conclusion, RSA-based encryption continues to serve as a foundational technique in secure image transmission and storage. Its integration with hybrid methods has shown promising improvements in resilience against modern attacks, proving its relevance in both current and emerging multimedia security applications. Future research should focus on enhancing lightweight RSA implementations, parallel processing techniques, and post-quantum adaptations to meet the evolving demands of digital security.

References

[1]. G. Sharma, N. Hemrajani, S. Sharma, A. Upadhyay, Y. Bhardwaj, and A. Kumar, "Data management framework for IoT edge-cloud architecture for resource-constrained IoT application," Journal of Discrete Mathematical Sciences and Cryptography, vol. 25, no. 4, pp. 1093–1103, 2022.

[2]. A. Maheshwari and R. Ajmera, "Unmasking embedded text: A deep dive into scene image analysis," in Proc. IEEE Int. Conf. on Advances in Computation, Communication, and Information Technology (ICAICCIT), 2023.

[3]. N. Tiwari, D. Goyal, and N. Hemrajani, “A hybrid method for image watermarking,” International Journal of Advanced Research in Computer Engineering and Technology (IJARCET), vol. 6, no. 6, pp. 894–898, 2017.

[4]. G. K. Soni, H. Arora, B. Jain, "A Novel Image Encryption Technique Using Arnold Transform and Asymmetric RSA Algorithm", Springer International Conference on Artificial Intelligence: Advances and Applications 2019 Algorithm for Intelligence System, pp. 83-90, 2020.

[5]. Dr. Himanshu Arora, Gaurav Kumar Soni, Deepti Arora, "Analysis and Performance Overview of RSA Algorithm", International Journal of Emerging Technology and Advanced Engineering, Vol. 8, pp. 9-12, 2018.

[6]. V. Singh, M. Choubisa, G. K. Soni, "Enhanced Image Steganography Technique for Hiding Multiple Images in an Image Using LSB Technique", TEST Engineering Management, vol. 83, pp. 30561-30565, May-June 2020.

[7]. N. Tiwari, D. Goyal, and N. Hemrajani, “A hybrid method for image watermarking,” International Journal of Advanced Research in Computer Engineering and Technology (IJARCET), vol. 6, no. 6, pp. 894–898, 2017.

[8]. P. Jha, D. Dembla, W. Dubey, "Implementation of Transfer Learning Based Ensemble Model using Image Processing for Detection of Potato and Bell Pepper Leaf Diseases", International Journal of Intelligent Systems and Applications in Engineering, Vol. 12, pp. 69-80, 2024.

[9]. G. K. Soni, A. Rawat, S. Jain and S. K. Sharma, "A Pixel-Based Digital Medical Images Protection Using Genetic Algorithm with LSB Watermark Technique", Springer Smart Systems and IoT: Innovations in Computing. Smart Innovation, Systems and Technologies, Vol. 141, pp. 483-492, 2020.

[10]. H. Arora, G. K. Soni, R. K. Kushwaha and P. Prasoon, "Digital Image Security Based on the Hybrid Model of Image Hiding and Encryption," IEEE 2021 6th International Conference on Communication and Electronics Systems (ICCES), pp. 1153-1157, 2021.

[11]. R. Ajmera and N. Saxena, “Face detection in digital images using color spaces and edge detection techniques,” Int. J. of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 6, pp. 718–725, Jun. 2013.

[12]. Himanshu Arora, Mr. Manish Kumar and Mr. Sanjay Tiwari, "Improve Image Security in Combination Method of LSB Stenography and RSA Encryption Algorithm", International Journal of Advanced Science and Technology, vol. 29, no. 8, pp. 6167-6177, 2020.

[13]. H. Kaushik, H. Arora, R. Joshi, K. Sharma, M. Mehra and P. K. Sharma, "Digital Image Security using Hybrid Model of Steganography and Cryptography," 2025 International Conference on Electronics and Renewable Systems (ICEARS), pp. 1009-1012, 2025.

[14]. R. Misra, "A Novel Approach to Enhanced Digital Image Encryption Using the RSA Algorithm", International Conference on Engineering & Design (ICED), 2021.

[15]. D. Singh, S. Kumar, "Image authentication and encryption algorithm based on RSA cryptosystem and chaotic maps", Expert Systems with Applications, Vol. 274, 2025.

[16]. B. V. Pavani, C. S. Bhumika, D. V. S. Jagadeesh and C. R. Kavitha, "Comparative Image Analysis of Chest X-RAY Image Encryption using Symmetric and Asymmetric Key Encryption Algorithms," 2024 8th International Conference on Electronics, Communication and

Aerospace Technology (ICECA), pp. 478-483, 2024.

[17]. H. M. Ali, P. N. Reddy, S. G. Rao, K. K. Dixit, G. B. Santhi and S. R. Kurukuntla, "Developing an Efficient Image Encryption Algorithm for Secure Data Transmission in Healthcare Systems," 2024 International Conference on IoT, Communication and Automation Technology (ICICAT), pp. 981-985, 2024.

[18]. H. Huang, Z. Han, "Computational ghost imaging encryption using RSA algorithm and discrete wavelet transform", Results in Physics, Vol. 56, 2024.

[19]. Z. Dong, Z. Zhang, H. Zhou and X. -B. Chen, "Color Image Encryption Based on 4D Hyperchaotic System and RSA Algorithm Combined Scrambling and Diffusion," 2023 5th International Conference on Industrial Artificial Intelligence (IAI), pp. 1-5, 2023.

[20]. B. Karthikeyan, B. Bharathkumar, G. Manikandan and R. Seethalakshmi, "A Combination of RSA Algorithm with Image Steganography to Ensure Enhanced Encryption," 2023 Second International Conference on Electronics and Renewable Systems (ICEARS), pp. 773-777, 2023.

[21]. Ganesamoorthy R, P. G, S. B, R. Krishnaprasanna, V. G and V. S. Pandi, "A Novel Design of an Image Encryption and Decryption Scheme Using Enhanced Cybersecurity Principles," 2023 International Conference on Emerging Research in Computational Science (ICERCS), pp. 1-6, 2023.

[22]. D. Venkata Rao, S. Pavan Kumar 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.

[23]. S. J. Edan, M. N. Rasoul and A. A. Aljarrah, "RSA-based Encryption Algorithm for Digital Images," 2022 Iraqi International Conference on Communication and Information Technologies (IICCIT), pp. 303-308, 2022.