ISSN 2277 – 8322

RSA-Based Color Image Encryption for Secure Authentication and Privacy Preservation

Rahul Misra[1], Neeraj Sharma[2]

[1]Department of Engineering & Technology, Jagananth University, Jaipur

[2]School of Computer Application, JECRC University, Jaipur

rahul.misra@jagannathuniversity.org, neeraj.sharma@jecrcu.edu.in

Abstract: The rapid advancement of digital imaging technologies and the increasing exchange of visual information across communication networks have raised significant concerns regarding image security, privacy, and data integrity. Color images often contain sensitive information that is vulnerable to unauthorized access, manipulation, and cyberattacks during storage and transmission. To address these challenges, robust cryptographic techniques are required to ensure confidentiality, authenticity, and protection against malicious activities. This paper presents a comprehensive review of RSA-based encryption techniques for securing color images. The RSA algorithm, a widely adopted public-key cryptographic scheme, utilizes asymmetric key pairs to provide secure encryption and decryption while supporting authentication mechanisms. By transforming image pixel data into encrypted representations, RSA significantly enhances the protection of image content against unauthorized disclosure and tampering. The study examines the fundamental principles of RSA cryptography, its implementation in image encryption systems, and its effectiveness in preserving data privacy and integrity. Furthermore, the paper discusses performance considerations, computational challenges, security advantages, and potential vulnerabilities associated with RSA-based image encryption. Various application domains, including secure communication networks, medical image management, military intelligence systems, cloud storage environments, and digital forensics, are also explored. The review concludes that RSA remains a reliable and effective approach for achieving secure image transmission and authentication, while future research should focus on improving computational efficiency and integrating RSA with advanced hybrid cryptographic frameworks.

Keywords: RSA Algorithm, Image Encryption, Cryptography, Public-Key Cryptography, Color Images, Authentication, Privacy Protection, Data Security, Encryption, Decryption.

1. Introduction

ISSN 2277 – 8322

The rapid advancement of digital imaging and multimedia technologies has significantly increased the generation, storage, and transmission of color images across various communication networks [1]. As images often contain sensitive and confidential information, ensuring their security and privacy has become a critical requirement. Unauthorized access, data manipulation, and cyberattacks during image transmission can lead to serious privacy breaches and information loss. Therefore, robust image encryption techniques are essential to protect image data from unauthorized users and malicious activities [2], [3].

Image encryption has become increasingly important in a wide range of applications, including web communications, multimedia systems, healthcare imaging, telemedicine, military communications, digital forensics, and cloud-based storage services. With the widespread use of the Internet and wireless communication networks, large volumes of color images are transmitted daily, making them vulnerable to interception and tampering. Consequently, the development of secure cryptographic methods for image protection has emerged as a major research area in information security [4], [5].

Cryptography plays a fundamental role in securing digital information by ensuring confidentiality, integrity, authentication, and non-repudiation. Since the pioneering work of Claude Shannon in 1949, numerous cryptographic algorithms have been developed to address evolving security challenges. Well-known encryption techniques such as the Advanced Encryption Standard (AES), Data Encryption Standard (DES), RSA, and International Data Encryption Algorithm (IDEA) have been widely adopted for securing digital data. Among these methods, RSA has gained significant attention due to its asymmetric encryption mechanism, which provides strong security for authentication and secure key exchange.

Images have become one of the most widely used forms of information exchange in sectors such as healthcare, scientific research, industrial automation, defense, and remote sensing. However, image transmission often occurs over unsecured networks, making sensitive visual information susceptible to unauthorized access and cyber threats. Unlike text data, digital images possess unique characteristics such as high redundancy, large data volume, and strong correlation among adjacent pixels, which require specialized encryption approaches for effective protection.

To address these challenges, cryptographic image encryption techniques are employed to convert original image data into unintelligible formats that can only be accessed by authorized users possessing the correct decryption keys. Such techniques ensure the confidentiality, authenticity, and integrity of

ISSN 2277 – 8322

image information during storage and transmission. As the demand for secure digital communication continues to grow, image encryption remains a crucial component of modern cybersecurity frameworks, enabling the safe exchange of visual information across diverse applications and environments.

2. Image Encryption

Encryption is the study of techniques to guarantee the communication process between the sender and the receiver in the presence of third parties called "liabilities". Essentially, it is understood that the design of protocols based on mathematics, computer science and electrical engineering encrypt and decipher information in the form of data and images.

Modern cryptography can be classified broadly into two types:-

A. Symmetric key cryptography

In the form of encryption, there is only one key and the private key is used to encrypt and decrypt data between the sender and receiver.

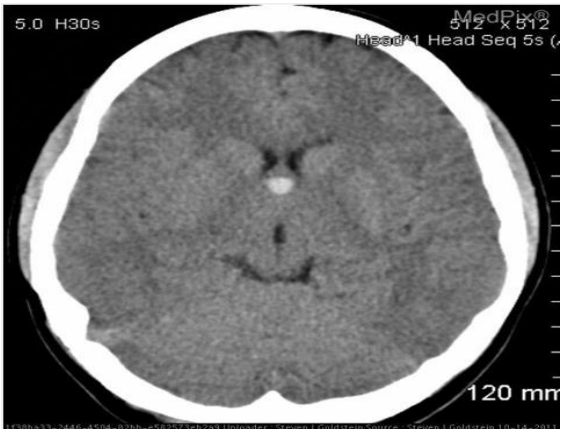
B. Asymmetric key cryptography

In this type of encryption, there are two types of keys: the public key and the private key. Both are used in encryption and decryption. The public key is available to everyone

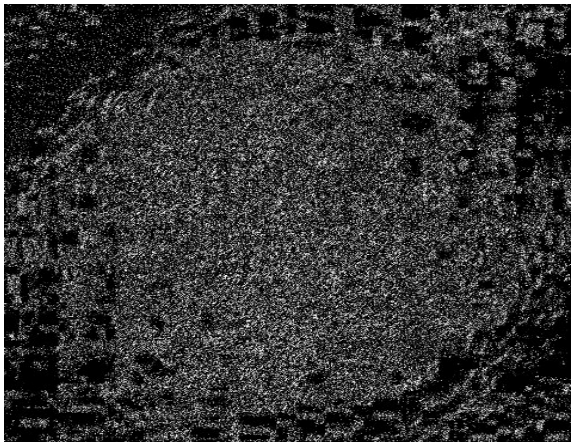
The encryption of the image is done to guarantee the safe transfer of images on the Internet. The encryption mechanism is widely used in this area of image / video transfer, since it does not provide access to unauthorized access. Encryption is also applicable in military communications and telemedicine. Up to the future point of view, the encryption has a greater scope. In the case of image security, the image contains large data, such as high frequency, large capacity and high pixel correlation. The techniques used in encryption can be considered as a tool to protect confidential data. Encryption is a mechanism that can be converted into encrypted or protected data, and can only be read by deciphering it. The process of reverse encryption is known as decryption, which uses a cryptographic key to decrypt the original data. Data encryption has become the best choice for all confidential data, including through the Internet, external networks or internal networks. Encryption is done by applying a mathematical function that generates a key later, and the key is used to obtain the encrypted data. Again, the mathematical key obtained is used for the original data. Security Manager is used to authenticate the user and accuracy in data security [8].

Image encryption is a technique used to hide data or secure image information. This is one of the most common methods that use secure image data. In this way, the image is encrypted and the encrypted image differs from the original image. The encrypted image shows no part of the original image. To obtain the original image from the encrypted image, it has been decrypted.

ISSN 2277 – 8322



(a) Original Image



(b) Encrypted Image

Figure 1: Image Encryption

3. RSA Algorithm

Public-key cryptography is also called asymmetric. It requires the use of a private key (a key that only its owner knows) and a public key (a key that both know). Public key cryptography is a fundamental technology and widely used throughout the world. It is the approach used by many cryptographic algorithms and commonly used for the distribution of software, financial transactions and in other critical security areas where it is important to protect against counterfeits and falsifications.

RSA is the most popular asymmetric digital image encryption algorithm. RSA (named for Rivets, Shamir and Adelman, who first described it publicly) is the first known algorithm for both signing and encryption, and was one of the first major advances in public-key cryptography. It uses a pair of keys, one of which is used to encrypt the digital image in such a way that it can only be verified with the other key of the pair [1].

The keys are generated through a common process, but cannot be generated in a viable manner among them. The security of RSA depends solely on finding the prime factors that are used in the process of encrypt and decrypt, the digital image and is based on the assumption that factoring a large number is difficult. "Multiplying two large prime numbers is a one-way function. It is easy to multiply the numbers to obtain a product, but it is extremely difficult to factor the product and retrieve the two large prime numbers that have been multiplied previously. it is known as a factoring problem. "

In this research, the security of the existing algorithm is improved whenever no one finds a way to solve this problem in a reasonable amount of time. RSA will be a secure encryption algorithm.

4. Mathematical Background of RSA Algorithm

ISSN 2277 – 8322

RSA (named for Rivest, Shamir and Adelman, who first described it publicly) is an algorithm for asymmetric cryptography. It is the first algorithm known to be suitable for signing and encryption, and it was one of the first great advances in public-key cryptography. It is widely believed that RSA is safe with sufficiently long passwords.

First find two prime numbers and generate a pair of keys using those two prime numbers.

p and q are different cousins

$$N = \pi * \ \theta \qquad (1)$$

Find e, d such that:

$$e * d = 1 \bmod (p-1)(q-1) \qquad (2)$$

$$\text{Private key: } = (n, d) \qquad (3)$$

$$\text{Public key: } = (n, e) \qquad (4)$$

Then, the encryption of the image and the decryption of the image are made using the key pair.

Image Encryption:

$$S(m) = m^e \bmod n = V(S) \qquad (5)$$

Image Decryption:

$$V(S) = S^d \bmod n = S(m) \qquad (6)$$

5. Digital Image Encryption Using RSA Algorithm

The RSA is the one of the most popular algorithm which is used to be digital image security or digital image encryption purpose. The encryption is one of the best techniques to secure the data or image at the time of communication. In encrypted image no one can be see the original data or image which is in it, to see the original data or image we can use the decryption technique to get the original image from the encrypted image.

The different obtained simulations result is shown in the below which is done for the image encryption purpose using the RSA algorithm.

In Figure 2 shows the different encryption and decryption of the colour image of car using RSA algorithm.

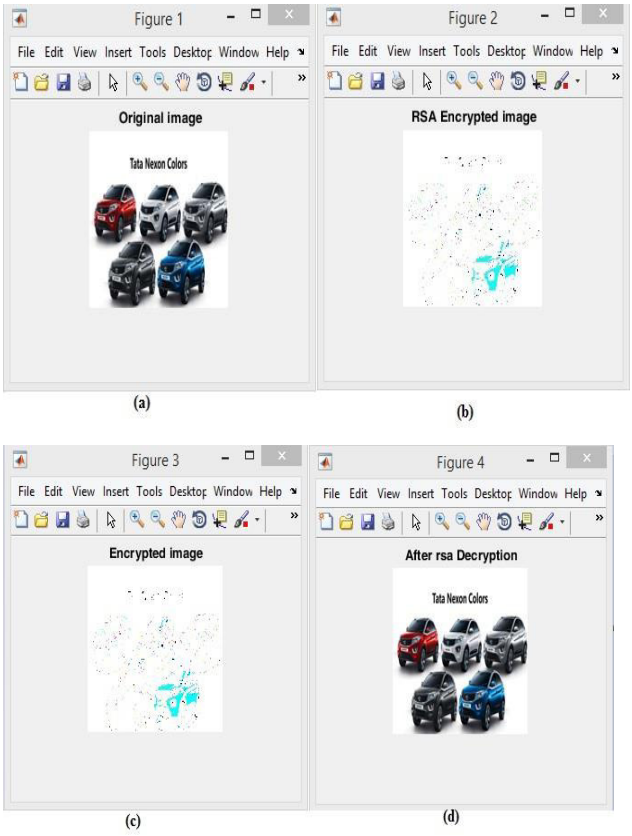


Figure 2: Color Image of the Car Encryption and Decryption Outputs (Prime number value is 107 and 109)

6. Conclusion

The asymmetric encryption algorithm of RSA makes encryption more secure and the receiver

ISSN 2277 – 8322

is not too afraid to give each sender a different key to ensure communication. And another advantage of the RSA algorithm is that the RSA algorithm is difficult to decipher because it involves the factorization of prime numbers that are difficult to factor. If in one way or another, the use of permutation or attempted piracy is able to get the decryption key is almost equal to the original key. In this paper we shown the overview of the RSA algorithm and also shown the obtained output results in the form of image encryption and decryption which is very useful to the digital image security purpose.

References

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

[2]. 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.

[3]. 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.

[4]. 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.

[5]. 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.

[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]. 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.

[9]. 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.

[10]. 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.

[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]. M. V. Lakshmi, R. Ajmera, N. Hemrajani, D. K. Dharamdasani, H. Arora and R. Joshi, "Multi-Layer Data Security using Image Embedding and RSA Encryption Technique," 2026 International Conference on Electronics and Renewable Systems (ICEARS), pp. 1597-1600, 2026.

[15]. Dr. Neeraj Sharma, "Cloud Computing Architecture: Models, Services, and Deployment Strategies", International Journal of Recent Research and Review, Vol. 18, Issue. 1, pp. 209-216, 2025.

[16]. N. Sharma, Dr. M. K. Sain, "An OOHI Analysis Approach for Distributed Data Store and Complex Event Processing of Big Data", Journal of Information and Computational Science, Vol. 11, Issue. 10, pp. 375-383, 2021.

[17]. Dr. Rahul Misra, Dr. Neeraj Sharma, "Artificial Intelligence Driven

Cybersecurity Techniques Challenges and Future Directions", International Journal of Engineering Trends and Applications (IJETA), Vol. 13, Issue. 1, pp. 11-16, 2026.

[18]. A. Upadhyay, R. Misra, S. K. Henge, Y. Bhardwaj, "Protection of Digital Image and Text Information Security Using LSB and Crossover Techniques", Computational Vision and Bio-Inspired Computing. Advances in Intelligent Systems and Computing, Vol 1439, pp. 601-608, 2023.