RESEARCH ARTICLE OPEN ACCESS

RSA-Based Encryption for Authentication and Privacy Protection of Color Images

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:

With the rapid growth of digital imaging technologies and their widespread applications, ensuring the security and privacy of color images has become a critical challenge in modern communication systems. Unauthorized access, tampering, and data breaches pose serious threats during image storage and transmission, necessitating robust encryption techniques. This paper presents a comprehensive study on the use of RSA-based encryption for authentication and privacy protection of color images. The proposed approach leverages the asymmetric nature of the RSA algorithm to provide high levels of confidentiality and integrity, ensuring that images remain secure against common cryptographic attacks. By transforming pixel values into encrypted forms, RSA enhances the impermeability of image data during transfer and storage, thereby preventing unauthorized modifications. The review highlights the effectiveness of RSA in maintaining data authenticity, protecting user privacy, and strengthening digital image security. Furthermore, the paper discusses implementation challenges, performance considerations, and potential applications in secure communication, healthcare imaging, military surveillance, and digital forensics.

Keywords: Cryptography, Decryption, Encryption, Image Encryption, RSA Algorithm.

1. Introduction

Since digital imaging plays an important role in multimedia technology, maintaining user privacy becomes even more important. To ensure such security and privacy for the user, it is very important to encrypt the image to protect against unauthorized access. Encryption of pictures and video is employed in varied fields, as well as web communications, multimedia system systems, medical imaging, telemedicine and military communications. color pictures ar transmitted and keep in massive quantities via the net and wireless networks that use the speedy development of multimedia system and network technologies. Cryptography has played an important role in security, and this is the battlefield for mathematicians and scientists from Shannon since 1949. Several cryptographic algorithms are now offered as AES, DES, RSA, IDEA, etc [5].

The image is the communication mode most used in different fields such as medical field, research field, industry, military area, etc. The important transfer of images will take place in an unsecured Internet network. Therefore, there is a need for appropriate security so that the image prevents access by the unauthorized person to important information. The advantage of the image is that it covers more multimedia data and needs protection. Cryptography is a type of image security method; It offers the secure method of transmitting and storing the image on the Internet. Security is the main concern of any system to maintain the integrity, confidentiality and authenticity of the image. Although cryptography is the efficient method, it also faces the problem of security if data with gray levels are more numerous [3].

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.

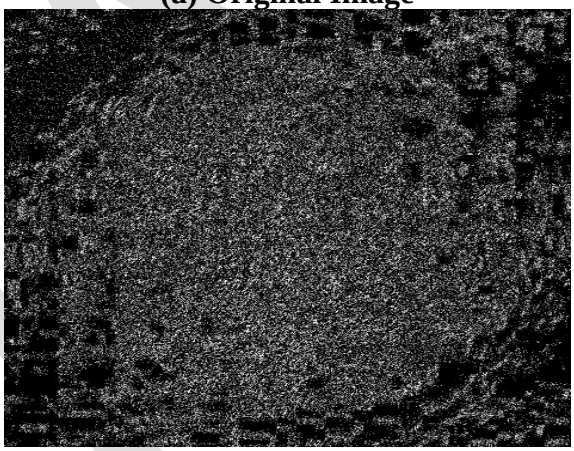
B. Asymmetric key cryptography

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.

(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

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

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

Find e, d such that:

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

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

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

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

Image Encryption:

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

Image Decryption:

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

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.

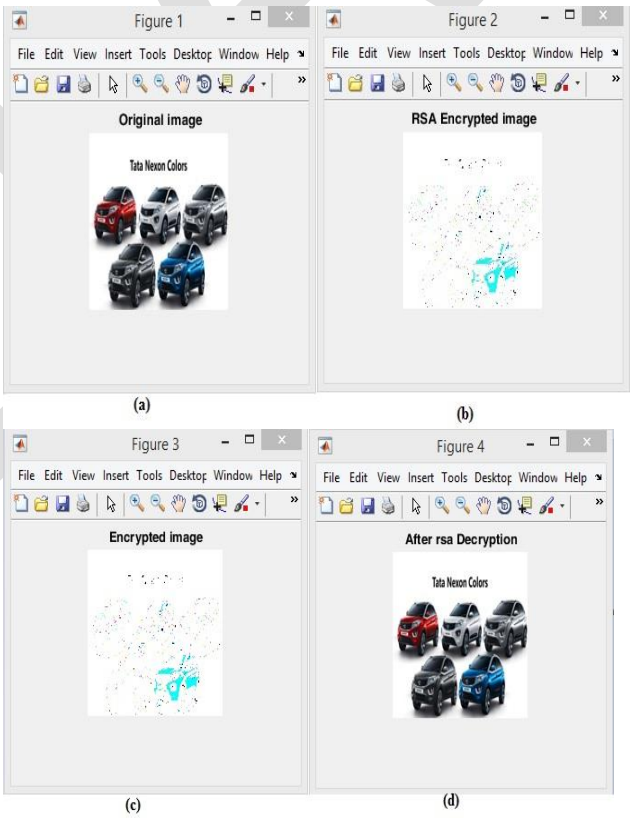


Figure 2: Color Image of the Car Encryption and Decryption Outputs (Prime number value is 107 and 109)

6. Conclusion

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

[2]. 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.

[3]. 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.

[4]. 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.

[5]. 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.

[6]. 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.

[7]. Pradeep Jha, Deepak Dembla, Widhi 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.

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