

Enhanced Digital Image Security Using Combination of Arnold Transformation and RSA Algorithm

Manoj Kumar Jangir*, Naveen Kumar Tiwari**

*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 expansion of digital media, images have become a major component of data exchanged over public networks, making their security a critical concern. Digital content often faces threats such as unauthorized access, modification, and copyright violations. To address these issues, techniques like encryption, authentication, and steganography are employed. This study focuses on RSA, an asymmetric encryption algorithm using public and private keys to ensure confidentiality and security, and Arnold Transformation, which enhances image protection through pixel scrambling based on iteration keys. The integration of RSA with Arnold Transformation provides a robust framework for secure image transmission, offering strong resistance against unauthorized access and cryptographic attacks.

Keywords: Cryptography, Image Encryption, RSA Algorithm, Arnold Transform, Public Key, Private Key.

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 are transmitted and kept 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].

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: Symmetric key cryptography and Asymmetric key cryptography.

2. Proposed Methodology

The asymmetric RSA encryption algorithm provides enhanced security, as the receiver does not need to share a different secret key with each sender to ensure secure communication. Another major advantage of RSA is that it is computationally hard to break, since its security relies on the factorization of large prime numbers a problem considered extremely difficult to solve. However, in certain cases, if an attacker somehow obtains an approximate decryption key through guessing or permutation techniques, it is possible to partially reconstruct 70–80% of the original image. This partial recovery could still provide significant information about the actual image. To address this issue, we incorporate Arnold Transformation along with RSA. The Arnold transformation scrambles the positional space of image pixels, effectively changing their locations while preserving their gray levels. The greater the pixel displacement, the higher the scrambling effect, resulting in a visually chaotic image. Although pixel values remain unchanged, the visual appearance of the scrambled image becomes highly disordered, making it incomprehensible to unauthorized users. Thus, even if an attacker recovers part of the decrypted image before applying the inverse Arnold transformation, the result will still be a disordered image that is extremely difficult to interpret.

Another strength of the Arnold transformation is its use of modulo operations, which require knowledge of the exact number of iterations applied. An incorrect prediction of the iteration count leads to an even more scrambled image, further enhancing security. Additionally, Arnold transformation is computationally efficient, requiring less time than many other scrambling techniques.

Therefore, combining RSA with Arnold Transformation improves the robustness of encryption without significantly increasing computational overhead.

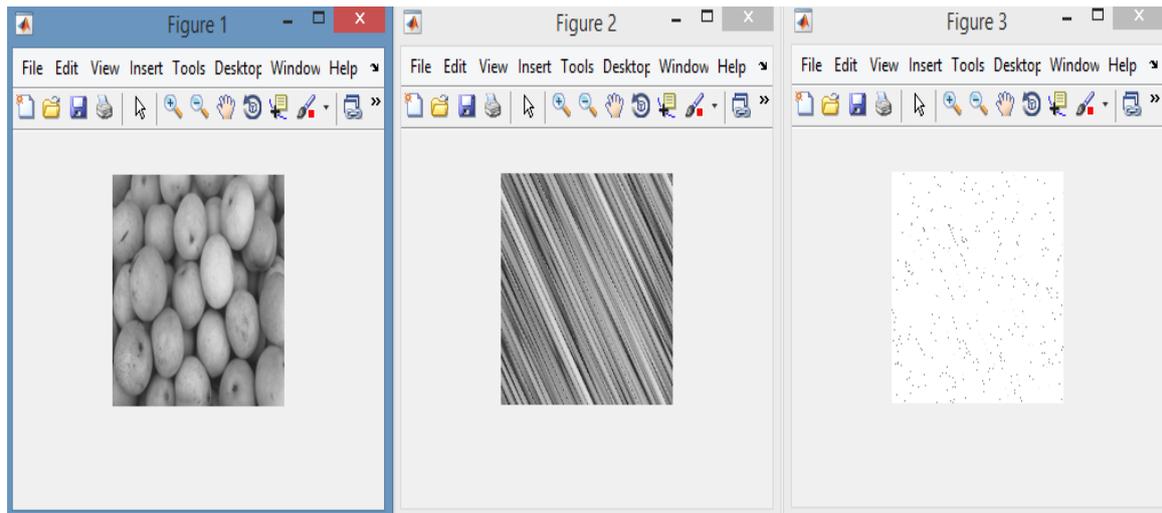
Furthermore, in RSA, when prime numbers are chosen such that their coprime values are close to the maximum pixel value, the encrypted image may visually resemble the original. Arnold transformation resolves this issue by transforming the encrypted output into a completely different, unrecognizable image.

Hence, our proposed hybrid approach, which combines Arnold Transformation with RSA, provides stronger and more robust digital image encryption, ensuring higher security against potential attacks.

3. Results and Discussion

In the proposed methodology, image scrambling is first performed using Arnold Transformation, followed by RSA encryption. This combined approach significantly enhances the robustness of image encryption, offering improved resistance against cryptographic attacks and ensuring higher security for digital images.

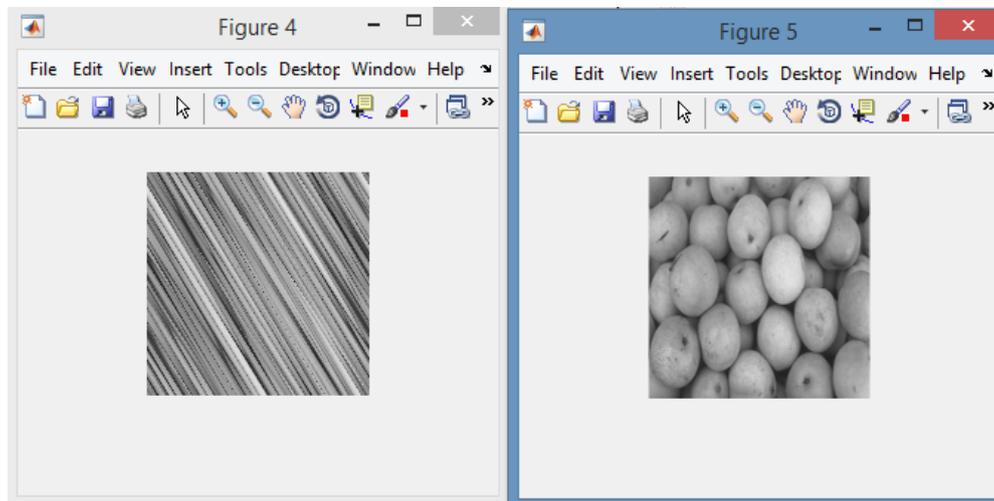
The results of the proposed method are shown in Figure 1. Figure 1(a) displays the original image, while Figure 1(b) shows the scrambled image obtained after applying Arnold Transformation. Figure 1(c) presents the encrypted image, which appears completely different from the original. Figure 1(d) illustrates the inverse Arnold Transformation applied to the encrypted image, and finally, Figure 1(e) shows the decrypted image, which closely resembles the original image. Thus, the combination of Arnold Transformation and RSA algorithm achieves improved encryption for digital images, ensuring enhanced security and robustness.



(a) Original Image

(b) Image after Arnold Transformation

(c) Proposed Encrypted Image Arnold with RSA



(d) Inverse Arnold

(e) Decrypted Image

Figure 1: Encryption and Decryption of image using Arnold Transformation and RSA Algorithm

6. Conclusion

The integration of RSA encryption with Arnold Transformation provides a secure and efficient hybrid approach for image protection. While RSA ensures strong key-based security, Arnold Transformation adds an extra layer of scrambling, making decryption without authorization extremely difficult. This combination enhances robustness against attacks while maintaining low computational overhead, offering a reliable solution for secure image transmission.

References

- [1]. 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.

- [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]. Dr. H. Arora, G. K. Soni, and D. Arora, "Analysis and Performance Overview of RSA Algorithm," *International Journal of Emerging*

- Technology and Advanced Engineering, vol. 8, pp. 9–12, 2018.
- [4]. G. K. Soni, H. Arora, and B. Jain, “A Novel Image Encryption Technique Using Arnold Transform and Asymmetric RSA Algorithm,” in Springer Int. Conf. on Artificial Intelligence: Advances and Applications – Algorithm for Intelligence System, pp. 83–90, 2020.
- [5]. V. Singh, M. Choubisa, and 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–Jun. 2020.
- [6]. 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,” in Springer Smart Systems and IoT: Innovations in Computing, Smart Innovation, Systems and Technologies, vol. 141, pp. 483–492, 2020.
- [7]. H. Arora, M. Kumar, and S. Tiwari, “Improve Image Security in Combination Method of LSB Steganography and RSA Encryption Algorithm,” International Journal of Advanced Science and Technology, vol. 29, no. 8, pp. 6167–6177, 2020.
- [8]. R. Misra, “A Novel Approach to Enhanced Digital Image Encryption Using the RSA Algorithm,” in International Conference on Engineering & Design (ICED), 2021.
- [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,” in Proc. IEEE 6th Int. Conf. on Communication and Electronics Systems (ICES), 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]. 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.
- [12]. P. Jha, D. Dembla, and 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.
- [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,” in Proc. 2025 Int. Conf. on Electronics and Renewable Systems (ICEARS), pp. 1009–1012, 2025.