Secure Image Encryption Using RSA Algorithm and Arnold Transformation

Yuvraj Pratap Singh
B.Tech Student, Department of IT, Global Institute of Technology, Jaipur, Rajasthan, India
22egjit021@gitjaipur.com

Dr. Sangeeta Soni
Associate Professor, Department of CSE, Global Institute of Technology, Jaipur, Rajasthan, India
sangeeta.soni@gitjaipur.com

ABSTRACT: The rapid proliferation of digital media has elevated images as a dominant form of data shared across public networks, thereby raising significant security concerns. Digital content is continuously exposed to threats such as unauthorized access, tampering, and copyright infringement. To mitigate these vulnerabilities, effective security techniques including encryption, authentication, and steganography are utilized. This research emphasizes RSA, an asymmetric cryptographic algorithm that employs public and private keys to ensure confidentiality and secure communication, along with the Arnold Transformation, which enhances image protection by scrambling pixel positions based on iterative keys. By integrating RSA with the Arnold Transformation, this study presents a robust framework for secure image encryption, offering strong resistance against unauthorized access and cryptanalytic attacks during transmission.

KEYWORDS: Cryptography, Image Encryption, RSA Algorithm, Arnold Transformation, Public Key, Private Key.

1. INTRODUCTION

With the rapid growth of multimedia technologies, digital imaging has become a crucial component of data communication [1]. As a result, ensuring user privacy and securing transmitted images has become increasingly important. Image encryption is essential to prevent unauthorized access and provide secure image transmission and storage. It is extensively used in various fields, including web communications, multimedia systems, medical imaging, telemedicine, and military communication [2]-[5]. Due to the widespread use of color images in internet and wireless networks, along with the rapid advancement of multimedia and communication technologies, securing visual data has become a significant concern [6]-[7].

Cryptography has played a vital role in data security since Claude Shannon laid its foundation in 1949. Over the years, several cryptographic algorithms such as AES, DES, RSA, and IDEA have been widely adopted to protect sensitive information. Images are commonly transmitted in multiple domains such as healthcare, scientific research, industry and defense [8]-[10]. However, since these transfers often occur over unsecured networks, adequate protection mechanisms are needed to safeguard confidential image data from unauthorized access. Images typically contain rich information, making them valuable but also vulnerable, thereby requiring strong protection techniques [11]-[13]. Cryptography provides secure mechanisms for image storage and transmission by ensuring integrity, confidentiality, and authenticity. Although cryptography is highly effective, certain challenges remain especially when dealing with complex image data containing numerous gray levels [14]-[15].

In general, encryption techniques ensure secure communication between the sender and receiver, preventing intrusion by unauthorized entities. These techniques rely on mathematical models and principles of computer science and electrical engineering to transform the original data into an unreadable format and retrieve it only by authorized users. Modern cryptography is broadly classified into two categories: 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.

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.

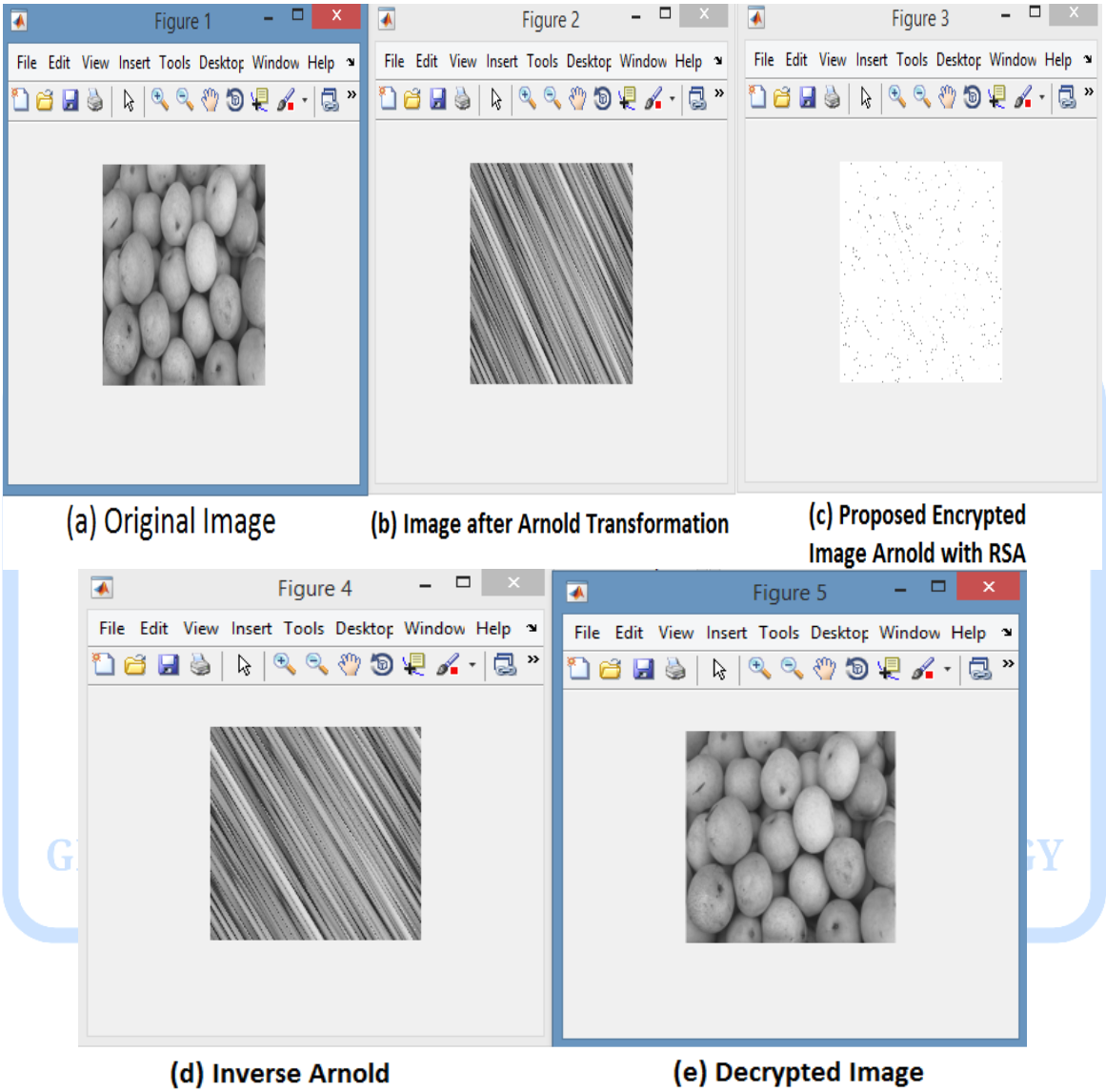

Figure 1: Encryption and Decryption of image using Arnold Transformation and RSA Algorithm

3. CONCLUSION

The integration of RSA encryption with the Arnold Transformation provides a secure and efficient hybrid approach for image protection. RSA ensures strong cryptographic security through public and private key mechanisms, while the Arnold Transformation introduces pixel scrambling to further obscure image data. This dual-layer protection significantly increases resistance against unauthorized access and cryptographic attacks. Additionally, the approach maintains relatively low computational complexity, making it suitable for real-time and secure image transmission applications.

REFERENCES

[1] V. Bhojak, K. P. Saini, N. K. Marwal, and A. Sharma, "Recent trends in Internet of Things: Applications, features and challenges," International Journal of Engineering Trends and Applications (IJETA), vol. 11, no. 6, pp. 53–57, 2024.

[2] P. Jha, K. K. Sharma, B. Jain, V. Sharma, "Digital Image Encryption Using AES Algorithm", EIJO Journal of Engineering, Technology And Innovative Research (EIJO–JETIR), Vol. 4, Issue. 2, 2019.

[3] N. Tiwari, N. Hemrajamani, D. Goyal, "Improved digital image watermarking algorithm based on hybrid DWT-FFT and SVD techniques", Indian Journal of Science and Technology, Vol. 10, Issue. 3, pp. 1-7, 2017.

[4] 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.

[5] M. K. Ramaiya, D. Goyal, N. Hemrajani, "Improved Image Steganographic System by using Multiple Encryption and DWT", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Vol. 6, Issue. 8, 2017.

[6] A. Sharma, K. Paliwal, "A Comparative Review of Steganography and Embedding Techniques for Secure Digital Media Communication", International Journal of Global Research in Science and Technology, Vol. 9, pp. 1-5, 2024.

[7] 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.

[8] 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.

[9] 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.

[10] S. P. Chaturvedi, A. Yadav, A. Kumar, R. Mukherjee, "Unlocking IoT Security: Enabling the Future with Lightweight Cryptographic Ciphers", Intelligent Computing Techniques for Smart Energy Systems, ICTSES 2023, Lecture Notes in Electrical Engineering, Vol. 1277, pp 189–199, 2025.

[11] D. Shekhawat and R. Ajmera, "Survey on security implication for the downtime of VM in cloud," IEEE 2nd World Conf. on Smart Trends in Systems, Security and Sustainability, 2018.

[12] 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.

[13] K. K. Gautam, S. Prakash, R. K Dwivedi, "Patients medical record monitoring using IoT based biometrics blockchain security system", 2023 International Conference on IoT, Communication and Automation Technology (ICICAT), pp. 1-6, 2023.

[14] H. Arora, R. Agarwal, P. Sharma, G. Shankar and D. Arora, "Image Security Utilizing Hybrid Model of Steganography and Asymmetric Cryptography Methods," 2023

International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), pp. 277-280, 2023.

[15] 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.