RESEARCH ARTICLE OPEN ACCESS

A Survey on Image Encryption Methods with Focus on 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:
The rapid growth of digital imaging technologies has raised critical concerns about image security and privacy in modern communication systems. This survey reviews image encryption methods with a focus on Arnold Transformation and the RSA algorithm. Arnold Transformation ensures pixel scrambling and increases image randomness, while RSA, an asymmetric cryptographic technique, provides strong authentication, confidentiality, and integrity. Together, these methods enhance resistance to cryptographic and statistical attacks. The paper highlights their strengths, limitations, and potential applications in secure communication, secure imaging, military surveillance, and digital forensics. In this paper mainly highlights the digital image security using the RSA encryption technique and Arnold transform.

Keywords: Cryptography, Encryption, Image Encryption, RSA Algorithm, Arnold Transform, Data Security.

1. Introduction

In the modern era of information technology, the Internet has become the most vital medium for communication and data exchange. Advances in IT have made digital media one of the most widely used tools for transferring data including text, images, audio, video, and software over open public networks. Among these, images form a significant portion of digital data and are heavily utilized in applications such as chats, news, websites, e-commerce, e-mails, and e-books. However, despite their widespread use, digital contents face challenges such as authentication, unauthorized modification, and copyright protection. To address these challenges, several techniques, including encryption (cryptography), authentication, and steganography, are employed. Encryption techniques, in particular, have proven to be the most effective solutions for ensuring data confidentiality and integrity. Recently, issues related to manipulation detection, protection, and authentication of digital images have gained significant attention from researchers [1].

In the field of cryptography and network security, image encryption has become a crucial research area due to its applications in secure digital communication. In this process, plain text or image data is converted into an encrypted form before transmission through a communication channel, ensuring that only authorized recipients can recover the original content. Hence, encryption algorithms must be robust enough to resist attacks by intruders. Images play an especially important role as a mode of communication in various domains such as medicine, research, industry, and the military. Since the transmission of images often occurs over insecure networks, strong protection is necessary to prevent unauthorized access to sensitive information. Unlike other data formats, images usually involve larger multimedia content, which makes their security even more critical [4].

Cryptography, as a method of image security, provides reliable ways to store and transmit images securely over the Internet. It ensures confidentiality, integrity, and authenticity of the data. However, encryption of gray-scale image data can still present challenges when the dataset is large and highly correlated [1].

With the rapid growth of digital communication, electronic data exchange, and the increasing use of cyberspace, ensuring digital image and video security has become essential. Applications such as pay-per-view services, secure videoconferencing, medical imaging, industrial systems, military communications, passwords, and legal digital signatures require strict access control and integrity verification. Unauthorized disclosure or malicious dissemination of images such as personal photographs, medical diagnostic scans, or classified government and industrial documents can lead to severe consequences for individuals, companies, or even nations.

Image encryption plays a key role in secure multimedia communication. It is widely applied in video/image transmission, medical image sharing across insecure networks, telemedicine, and military systems. Image encryption is particularly challenging because image data is characterized by high redundancy, large capacity, and strong pixel correlations. The encryption process converts original (plain) images into unintelligible encrypted data, which can only be recovered through decryption using a valid key. This ensures confidentiality even when transmitted over unsecured networks. Encryption algorithms such as AES, DES, Triple DES (3DES), RSA, Scalable Encryption Algorithm (SEA), and International Data Encryption Algorithm (IDEA) are commonly applied for securing images and videos. These mechanisms are based on mathematical functions to generate encryption keys, which are later used to encrypt and decrypt data. Effective security management ensures not only user authentication but also data confidentiality and accuracy [3].

Beyond encryption, digital information concealment techniques are also applied to secure multimedia. For instance, data-hiding methods combine steganography with encryption to ensure that both the cover image and the confidential message can be retrieved at the receiving end. For example, Siva Shankar S proposed a scheme combining Arnold transformation with randomized mapping to enhance image encryption and data hiding [16]. In this method, secret message bits are embedded in the least significant bit positions of the cover image, and a random diffusion process further encrypts the data. The Arnold transformation scrambles pixel positions multiple times, providing strong resistance against brute-force attacks. Security analysis showed high robustness, low collision probability, and the ability to recover the original image with minimal loss.

Similarly, hybrid methods combining Arnold transformation and RC4 stream encryption have been proposed [20]. In this scheme, Arnold transformation first randomizes pixel positions in the spatial domain, followed by RC4 encryption for enhanced security. A Blum Blum Shub (BBS) random bit generator is used to produce the RC4 input key. Security analysis through correlation coefficients and quality factor evaluation demonstrates improved protection compared to standalone RC4 encryption.

Information security has always been central to human communication, but with the rise of electronic devices and digital signals, it has become more critical than ever. This concern traces back to the pioneering work of Claude Shannon in 1948, who introduced the modern concept of cryptography. Cryptography, at its core, involves designing protocols that ensure secure communication between a sender and a recipient in the presence of adversaries. It integrates principles of mathematics, computer science, and electrical engineering to develop methods for encryption and decryption of digital data, including images.

Modern cryptography can be broadly classified into two main categories: symmetric key cryptography and asymmetric key cryptography:

A. Symmetric Key Cryptography

In symmetric key cryptography, a single secret key is used for both encryption and decryption, meaning that the sender and the recipient must share the same key in advance. The security of this method relies heavily on keeping the key confidential. Since only one key is involved, symmetric encryption techniques are generally faster and more

efficient, making them well-suited for encrypting large volumes of data. However, a major drawback is the challenge of secure key distribution if the key is intercepted during transmission, the entire system becomes vulnerable. Common symmetric key algorithms include Data Encryption Standard (DES), Triple DES (3DES), Advanced Encryption Standard (AES), Blowfish, and Twofish, which are widely applied in file encryption, secure data storage, and private network communications..

B. Asymmetric Key Cryptography

Asymmetric key cryptography, also known as public-key cryptography, employs a pair of keys: a public key and a private key. The public key is openly available and used for encrypting data, while the private key is kept secret by the recipient and used for decryption. This ensures that only the intended recipient can access the encrypted information, eliminating the need to share a secret key in advance and thereby solving the key distribution problem. However, asymmetric cryptography is computationally more intensive and slower than symmetric methods, which is why it is often combined with symmetric encryption for instance, to securely exchange symmetric keys that are then used for bulk data encryption. Common asymmetric algorithms include RSA (Rivest–Shamir–Adleman), Elliptic Curve Cryptography (ECC), Digital Signature Algorithm (DSA), and Diffie–Hellman Key Exchange. These methods are widely used in securing online transactions, implementing digital signatures, enabling SSL/TLS protocols, and supporting modern authentication systems.

2. 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. "

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:

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

3. Arnold Transformation

Image scrambling is a common technology with encryption fast speed and good results that is to realize the image encryption. The transformation of Arnold is one of the main methods for realize the encryption algorithm in the field of image transformation [11].

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \ mod\ 1, x, y\ \varepsilon\ \{0, 1\} \quad (7)$$

Formula (3.1) is Arnold's transformation for a unit square. In fact, we can extend pixels from one digital image to another image. For an image, its size is N × N. Then get the formula

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \ mod\ N, x, y\ \varepsilon\ \{0, 1, 2, 3, 4 \dots N - 1\} \quad (8)$$

Setting $A = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$ is transformation matrix (x,y) as a pixel of original image $(x, y)\ \varepsilon\ (0, 1, 2, 3, 4 \dots \dots N - 1), (x', y')$ as a pixel of the scrambled image, then its feedback is formula (9)

$$P_{ij}^{n+1} = AP_{ij}^{n}\ mod\ N, P_{ij}^{n} = (i, j), n = 0, 1, 2, 3, \dots \dots N - 1 \quad (9)$$

Through the substitution of discrete points, while the information of the image is transplanted, after all the points of the original image have been crossed and then a new image will be formed.

Assume that a point X in the image and a point Y in the image have corresponding relationships, such that the gray value or the RGB color value of pixel X is mapped to that of pixel Y. In this process, the gray or RGB color value undergoes a positional shift. This phenomenon is referred to as location movement, which in digital image encryption is achieved using the Arnold Transformation. The image transformation can be expressed mathematically as shown in equation (8).

When this iterative process is executed for a certain number of steps, the image appears chaotic. This behavior, based on Arnold Transformation, ensures that pixel positions are altered systematically. From equation (3.3), it is evident that Arnold Transformation performs a one-to-one positional mapping of pixels. Moreover, the transformation is periodic, meaning that after a certain number of iterations, the original image can be reconstructed. Thus, any pixel (x, y) returns to its original position after k iterations.

For an encrypted image, if the encryption algorithm is known, the original image (plaintext) can be restored within a limited number of iterations. However, such algorithms alone do not comply with Kerckhoff's principle of cryptography, as they are not inherently secure. Therefore, it is necessary to combine the Arnold Transformation with other encryption algorithms to enhance the robustness of the encryption scheme [11].

Images have always been an essential medium for representing and understanding the world, ranging from ancient murals and hieroglyphics to modern digital video. With the rapid advancement of computer networks and multimedia technology, digital image security has become a significant concern. Consequently, image encryption has emerged as a vital area of research.

Image scrambling is a widely used technique in digital image encryption. It transforms an image into a chaotic representation, ensuring that the original information cannot be directly perceived. Even exhaustive calculations of all possible combinations would be computationally expensive. Image scrambling techniques typically include randomization of pixel positions and modification of pixel intensity (gray-level interference). By altering pixel locations (permutation) or modifying gray values (substitution), encryption is achieved. Popular scrambling techniques include the Arnold Transformation, Magic Transform, Tangram Algorithm, Conway's Game of Life, Gray Code Transformation, and others.

Although the Arnold Transformation is simple and cyclic, making it useful for applications such as image hiding, it has certain limitations. The randomization effect of the traditional Arnold Transformation is weak for small iteration counts, and its periodicity does not always correspond proportionally to the image size. Furthermore, advances in computation have made it easier to calculate the periodicity

and perform reverse transformations. As a result, the traditional Arnold Transformation alone is less secure [12].

To overcome these limitations, the Arnold Transformation can be combined with strong cryptographic algorithms, such as the RSA algorithm, to improve the overall security of image encryption. In the proposed approach, Arnold Transformation is integrated with RSA to provide a more secure image encryption scheme.

4. Conclusion

Image security is vital in modern communication, and this survey reviewed encryption methods focusing on RSA and Arnold Transformation. While Arnold Transformation enhances image randomness and RSA ensures strong confidentiality, their integration offers a balanced and robust approach against cryptographic attacks. Despite challenges such as cyclic behavior in Arnold and high computational demand in RSA, hybrid models show great potential for secure communication, medical imaging, and defense applications. Future work should aim to optimize efficiency and explore advanced techniques like chaos-based and quantum cryptography to further enhance image security.

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

[3]. 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.

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

[5]. 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.

[6]. 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.

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

[8]. 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.

[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," in Smart Systems and IoT: Innovations in Computing, Smart Innovation, Systems and Technologies, vol. 141, Springer, 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," in Proc. IEEE 6th Int. Conf. on Communication and Electronics Systems (ICCES), pp. 1153–1157, 2021.

[11]. Y. Wang and T. Li, "Study on Image Encryption Algorithm Based on Arnold Transformation and Chaotic System," in Proc. IEEE Int. Conf. on Intelligent Systems Design and Applications, pp. 449–451, 2010.

[12]. Z. Shang, H. Ren, and J. Zhang, "A Block Location Scrambling Algorithm of Digital Image Based on Arnold Transformation," in Proc. IEEE 9th Int. Conf. on Young Computer Scientists, pp. 2942–2947, 2008.

[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.

[14]. R. Ajmera and N. Saxena, "Face Detection in Digital Images Using Color Spaces and Edge Detection Techniques," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 6, pp. 718–725, Jun. 2013.