A Comprehensive Review of Digital Image Security Using Cryptographic Techniques

Gaurav Garg
B.Tech Student, Department of CSE, Global Institute of Technology, Jaipur, Rajasthan, India
21egjcs046@gitjaipur.com

Harsh Raj
B.Tech Student, Department of CSE, Global Institute of Technology, Jaipur, Rajasthan, India
21egjcs047@gitjaipur.com

Kritika
Assistant Professor, Department of CSE, Global Institute of Technology, Jaipur, Rajasthan, India
kritika.rohila@gitjaipur.com

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

ABSTRACT: The extensive use of digital images in modern communication systems, including healthcare diagnostics, military and defense applications, surveillance, cloud storage, and social media platforms, has raised serious concerns regarding data security and privacy. The transmission of image data over open and public networks exposes it to various threats such as unauthorized access, interception, tampering, and illegal duplication. Cryptography has emerged as a fundamental technique for safeguarding digital images by transforming visual information into an unreadable form using mathematical algorithms and secret keys. However, the inherent characteristics of digital images such as large data size, high redundancy, and strong pixel correlation pose unique challenges that are not effectively addressed by conventional text-based encryption methods. This paper presents a comprehensive review of digital image cryptography, focusing on its fundamental principles, including confusion and diffusion, as well as commonly used symmetric and asymmetric encryption techniques. The study also discusses chaos-based image encryption methods and highlights key performance and security evaluation metrics such as histogram analysis, entropy, correlation coefficient, and key sensitivity. By examining existing cryptographic approaches and their limitations, this review emphasizes the importance of developing secure, efficient, and robust image encryption schemes to meet the growing demands of modern multimedia communication systems.

KEYWORDS: Digital Image Security, Image Cryptography, Encryption Algorithms, Data Confidentiality, Information Security.

1. INTRODUCTION

The rapid advancement of digital communication technologies and multimedia applications has resulted in the extensive use of digital images in modern information systems. Digital images are widely utilized in diverse fields such as healthcare diagnostics, military and defense communication, surveillance systems, biometric authentication, social media platforms, cloud storage, and e-commerce applications. With the increasing reliance on open

and public networks for data transmission, ensuring the security and privacy of digital image data has become a critical challenge.

Unlike textual data, digital images contain a large amount of sensitive visual information and are often transmitted in raw or compressed formats, making them vulnerable to various security threats. These threats include unauthorized access, interception, tampering, illegal duplication, and malicious manipulation. In critical applications such as telemedicine and military communication, any compromise in image security can lead to severe consequences, including privacy violations, financial loss, and threats to national security. Therefore, protecting digital images against unauthorized use and ensuring confidentiality, integrity, and authenticity are essential requirements in modern communication systems.

Traditional security mechanisms such as access control, password protection, and network firewalls provide only partial protection and are insufficient once the data is intercepted. Cryptography has emerged as one of the most effective techniques for securing digital information by transforming original data into an unreadable format using mathematical algorithms and secret keys. Image cryptography specifically focuses on protecting image data by encrypting pixel values so that the content remains unintelligible to unauthorized users.

However, digital images possess unique characteristics such as high data redundancy, strong correlation among neighboring pixels, and large data size, which distinguish them from text-based data. Conventional encryption algorithms designed for text may not always be efficient or optimal for image data. As a result, specialized image encryption techniques and optimized cryptographic schemes have been developed to address these challenges. This paper aims to review the fundamental concepts of image cryptography, discuss commonly used encryption approaches, and highlight their importance in securing digital image communication.

2. FUNDAMENTALS OF IMAGE CRYPTOGRAPHY

Image cryptography is a branch of information security that focuses on protecting digital images by converting them into an encrypted form that is unreadable without proper authorization. The primary objective of image cryptography is to ensure data confidentiality by preventing unauthorized users from accessing or interpreting the image content during transmission or storage. The encryption process transforms the original image, known as the plaintext image, into a cipher image using cryptographic algorithms and secret keys. The decryption process reverses this operation to recover the original image.

Unlike text data, digital images consist of a large number of pixels, where each pixel represents intensity or color information. Images exhibit high spatial redundancy, meaning that adjacent pixels often have similar values, resulting in strong correlations. An effective image cryptography scheme must eliminate these correlations to prevent statistical attacks. Therefore, most image encryption techniques employ two fundamental cryptographic principles: confusion and diffusion. Confusion obscures the relationship between the encryption key and the cipher image, while diffusion spreads the influence of a single pixel change across the entire image.

Image cryptographic techniques can be broadly classified into symmetric key and asymmetric key encryption methods based on key usage. In symmetric key cryptography, the same secret key is used for both encryption and decryption. Algorithms such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), and chaos-based encryption schemes are commonly used due to their high speed and suitability for large image data. Symmetric

encryption is computationally efficient; however, secure key distribution remains a major challenge.

Asymmetric key cryptography uses two different keys: a public key for encryption and a private key for decryption. Popular algorithms such as RSA and Elliptic Curve Cryptography (ECC) offer higher security and solve the key distribution problem. However, these methods require high computational resources and are generally not suitable for encrypting large image data directly. Therefore, asymmetric encryption is often combined with symmetric encryption in hybrid security systems.

In addition to conventional cryptographic algorithms, chaos-based image encryption techniques have gained significant attention due to their sensitivity to initial conditions, pseudo-random behavior, and strong diffusion properties. These characteristics make chaotic systems highly suitable for image encryption applications. Performance evaluation of image cryptography schemes typically involves metrics such as histogram analysis, correlation coefficient, entropy, key sensitivity, and resistance to cryptographic attacks.

Image cryptography plays a vital role in safeguarding digital image data. Understanding its fundamental principles is essential for developing secure, efficient, and robust image encryption systems capable of meeting the security demands of modern digital communication environments.

3. CRYPTOGRAPHIC TECHNIQUES FOR IMAGE SECURITY

Symmetric Key Cryptography

Symmetric key cryptography is a widely used encryption technique in which the same secret key is employed for both encryption and decryption of data. Due to its high processing speed and low computational complexity, symmetric encryption is particularly suitable for securing large-sized digital images. Commonly used symmetric algorithms for image encryption include the Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple DES (3DES), and Blowfish.

Among these algorithms, AES is the most preferred for image security applications because of its strong cryptographic strength, efficient performance, and resistance to known cryptographic attacks. AES operates on fixed-size data blocks and supports multiple key lengths, making it flexible and highly secure for protecting image data. In addition to conventional symmetric algorithms, chaos-based encryption techniques have gained significant attention in recent years. These methods exploit the properties of chaotic systems, such as sensitivity to initial conditions, ergodicity, and pseudo-random behavior, which make them highly suitable for image encryption by effectively reducing pixel correlation and enhancing diffusion.

Despite their advantages, symmetric encryption systems face a major challenge in secure key distribution. Since the same secret key must be shared between the sender and receiver, ensuring secure key exchange over open networks is difficult. If the secret key is compromised, the entire encryption system becomes vulnerable to unauthorized access.

Asymmetric Key Cryptography

Asymmetric key cryptography, also known as public key cryptography, utilizes two distinct keys: a public key for encryption and a private key for decryption. This approach eliminates the key distribution problem associated with symmetric encryption, as the public key can be

openly shared without compromising security. Popular asymmetric algorithms used in cryptographic systems include RSA and Elliptic Curve Cryptography (ECC).

Asymmetric cryptographic algorithms provide a higher level of security and are particularly effective for secure key exchange and digital authentication. ECC, in particular, offers strong security with shorter key lengths, making it more efficient than traditional public key algorithms such as RSA. However, asymmetric encryption involves complex mathematical operations, which result in higher computational overhead and slower processing speed.

Due to these limitations, asymmetric cryptography is generally not suitable for directly encrypting large image data. Instead, it is commonly used in hybrid encryption systems, where asymmetric algorithms securely exchange secret keys, and symmetric algorithms perform the actual image encryption. This hybrid approach combines the efficiency of symmetric encryption with the secure key management advantages of asymmetric cryptography, making it highly effective for digital image security applications.

4. PERFORMANCE AND SECURITY CONSIDERATIONS

The effectiveness of an image cryptography scheme is assessed using a set of performance and security metrics that evaluate both its robustness and computational efficiency. These metrics are essential to ensure that the encrypted image provides strong protection against unauthorized access while remaining practical for real-time and large-scale applications. Encryption speed is a critical performance metric, especially for high-resolution images and real-time communication systems. A secure image encryption algorithm should achieve fast encryption and decryption without imposing excessive computational overhead.

Histogram analysis is commonly used to evaluate the statistical properties of the encrypted image. A secure encryption scheme should produce a cipher image with a uniformly distributed histogram, which prevents attackers from extracting useful information through statistical analysis. Uniform histograms indicate that pixel values are evenly distributed and do not reveal patterns related to the original image.

Correlation coefficient analysis measures the degree of similarity between adjacent pixels in an image. In plaintext images, neighboring pixels are highly correlated due to image redundancy. A strong encryption algorithm should significantly reduce this correlation, ensuring that adjacent pixels in the cipher image exhibit minimal or no correlation. Low correlation values indicate effective diffusion and resistance to statistical attacks. Entropy is another important metric that quantifies the randomness of the encrypted image. An ideal encrypted image should have entropy values close to the theoretical maximum, indicating high unpredictability and resistance to information leakage.

Key sensitivity is a crucial security requirement in image cryptography. A robust encryption scheme should exhibit high sensitivity to the secret key, such that even a minor change in the encryption key results in a completely different cipher image. This property ensures protection against brute-force and key-related attacks by preventing attackers from approximating the correct key. In addition to these metrics, a secure image encryption algorithm must be resilient to various cryptographic attacks, including brute-force attacks, statistical attacks, known-plaintext attacks, and differential attacks. At the same time, the algorithm should maintain acceptable computational efficiency to support practical implementation. Overall, an effective image cryptography scheme must achieve a balance between strong security, high randomness, resistance to attacks, and computational feasibility, making it suitable for modern digital image communication systems.

5. CONCLUSION

Digital image security is a critical requirement in modern multimedia communication systems. Cryptography provides a powerful and reliable solution by ensuring confidentiality and protecting image data from unauthorized access. This review has presented an overview of image cryptography, including fundamental concepts, commonly used algorithms, performance considerations, and existing challenges. Although cryptographic techniques offer strong security, ongoing research is essential to address their limitations and meet the evolving demands of secure image communication in the digital era.

REFERENCES

[1] 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.

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

[3] 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.

[4] A. Maheshwari, R. Ajmera and D. K. Dharamdasani, "Unmasking Embedded Text: A Deep Dive into Scene Image Analysis," 2023 International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT), pp. 1403-1408, 2023.

[5] 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.

[6] Manoj Kumar Ramaiya, Dinesh Goyal, Naveen 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.

[7] 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.

[8] 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.

[9] 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.

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