Image Security Using Cryptography and Steganography: A Comprehensive Review and Hybrid Approach

Tanishq Saini
B.Tech Student, Global Institute of Technology, Jaipur, Rajasthan, India
23egjcs819@gitjaipur.com

Tanuj Kumar Gupta
B.Tech Student, Global Institute of Technology, Jaipur, Rajasthan, India
23egjcs820@gitjaipur.com

Ayushi Shukla
Assistant Professor, Global Institute of Technology, Jaipur, Rajasthan, India
ayushi.shukla@gitjaipur.com

Kritika Paliwal
Assistant Professor, Global Institute of Technology, Jaipur, Rajasthan, India
kritika.paliwal@gitjaipur.com

ABSTRACT: With the rapid growth of digital communication and multimedia applications, secure transmission of images over open networks has become a critical concern. Digital images are highly vulnerable to unauthorized access, manipulation, and duplication during storage and transmission. Cryptography and steganography are two widely used techniques for ensuring image security. Cryptography focuses on transforming image data into an unreadable format, while steganography conceals the existence of secret information within a cover image. This paper presents a comprehensive overview of image security using cryptography and steganography, highlighting their principles, techniques, advantages, and limitations. Furthermore, a hybrid approach that combines both methods is discussed to enhance security by ensuring confidentiality as well as secrecy of communication.

KEYWORDS: Image Security, Cryptography, Steganography, Data Hiding, Encryption, Digital Image Processing.

1. INTRODUCTION

The exponential growth of digital communication technologies and multimedia applications has made digital images one of the most commonly exchanged forms of information. Images are widely used in areas such as social media, telemedicine, military communication, surveillance systems, cloud storage, and online publishing. However, the open nature of communication networks exposes digital images to various security threats, including unauthorized access, interception, tampering, duplication, and data leakage. Ensuring the confidentiality, integrity, and authenticity of image data has therefore become a critical challenge in modern information security.

Traditional security mechanisms such as access control and network firewalls provide limited protection against sophisticated cyberattacks. Cryptography has emerged as a fundamental technique for securing image data by transforming the original image into an unreadable encrypted form using mathematical algorithms and secret keys. Image cryptography ensures confidentiality by preventing unauthorized users from interpreting the image content.

However, encrypted images often appear suspicious and may attract attackers, making them vulnerable to cryptanalysis and brute-force attacks.

Steganography offers an alternative approach by concealing secret information within a seemingly innocent cover image. Unlike cryptography, steganography hides the very existence of the secret data, thereby enabling covert communication. Common steganographic techniques embed information into the spatial or transform domains of images in such a way that visual quality is preserved. While steganography effectively masks hidden data, it does not inherently protect the content if the hidden information is discovered.

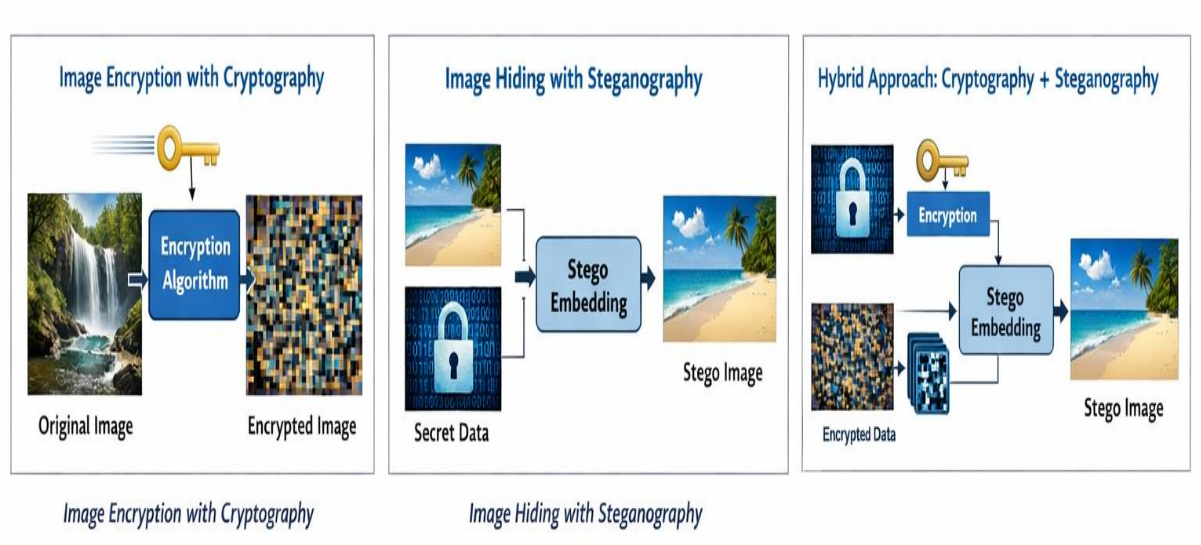
Image Encryption with Cryptography
Encryption Algorithm
Original Image
Encrypted Image
Image Hiding with Steganography
Stego Embedding
Stego Image
Secret Data
Hybrid Approach: Cryptography + Steganography
Encryption
Stego Embedding
Encrypted Data
Stego Image
Image Encryption with Cryptography
Image Hiding with Steganography

Figure 1: Image security through encryption and steganography

To overcome the limitations of individual security techniques, a hybrid approach combining cryptography and steganography has gained significant attention in recent years. In this approach, the secret image or message is first encrypted using a cryptographic algorithm and then embedded into a cover image using a steganographic method. This dual-layer security mechanism ensures that even if the hidden data is detected, it remains unreadable without the correct decryption key. The combined use of cryptography and steganography significantly enhances resistance to statistical analysis, unauthorized extraction, and cryptographic attacks.

This paper focuses on image security using cryptography and steganography, highlighting their working principles, commonly used techniques, and security benefits. The hybrid framework discussed in this study provides improved confidentiality, robustness, and secrecy, making it suitable for applications such as secure image transmission, medical data protection, military communication, and digital rights management.

2. CRYPTOGRAPHY FOR IMAGE SECURITY

Cryptography is a technique that secures image data by converting it into an unreadable format using encryption algorithms. Image cryptography can be classified into symmetric and asymmetric encryption methods.

In symmetric cryptography, the same secret key is used for both encryption and decryption. Algorithms such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), and chaotic encryption techniques are commonly used due to their high speed and efficiency. However, secure key distribution remains a challenge.

Asymmetric cryptography uses a pair of keys a public key for encryption and a private key for decryption. Algorithms such as RSA and Elliptic Curve Cryptography (ECC) provide higher security but are computationally expensive for large image data. Image cryptography ensures data confidentiality but does not hide the presence of encrypted information.

3. STEGANOGRAPHY FOR IMAGE SECURITY

Steganography is the art of hiding secret information within a digital image in such a way that the presence of hidden data is imperceptible to the human eye. Image steganography techniques are broadly classified into spatial domain and transform domain methods.

The Least Significant Bit (LSB) technique is a widely used spatial domain method in which secret data is embedded by modifying the least significant bits of image pixels. It offers high embedding capacity and simplicity but is vulnerable to image processing attacks.

Transform domain techniques such as Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), and Singular Value Decomposition (SVD) provide higher robustness against compression and noise attacks. Steganography ensures covert communication but does not encrypt the hidden information.

4. HYBRID IMAGE SECURITY APPROACH

A hybrid image security approach combines cryptography and steganography to provide multiple layers of protection. In this method, the secret image or message is first encrypted using a cryptographic algorithm and then embedded into a cover image using a steganographic technique. Even if the hidden data is detected, it remains unreadable due to encryption. This combined approach improves resistance against brute-force attacks, statistical analysis, and unauthorized extraction. It is widely applicable in secure image transmission, military communication, medical data protection, and digital watermarking systems.

5. CONCLUSION

Image security is a crucial requirement in modern digital communication systems. Cryptography and steganography individually provide effective solutions for image protection; however, each has its limitations. Cryptography ensures confidentiality but reveals the existence of encrypted data, while steganography hides information but lacks strong encryption. A hybrid approach that integrates both techniques significantly enhances image security by providing confidentiality, integrity, and invisibility. Future research can focus on integrating chaotic systems, artificial intelligence, and adaptive algorithms to further strengthen image security frameworks.

REFERENCES

[1] 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.

[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] 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] 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.

[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", Springer Smart Systems and IoT: Innovations in Computing. Smart Innovation, Systems and Technologies, Vol. 141, pp. 483-492, 2020.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

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

[14] M. K. Jha, N. Maharishi, G. K. Soni, S. Chawla, R. Yadav and S. Kaloria, "Multi-Layered Secure Framework for Digital Data Protection using Steganography, Embedding, and Cryptographic Techniques," 2025 4th International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), pp. 1572-1576, 2025.

[15] 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.

[16] 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.