International Journal of Information Technology & Computer Engineering

ISSN 2347–3657
Volume 13, Issue 4, 2025

A Multi-Layer Secure and Quality-Preserving Image Sharing Framework Using LSB Steganography, AES Encryption, and Shamir's Secret Sharing

Bilal Ahmed Siddique [1], Dr Md. Zainlabuddin [2]
[1] PG Scholar, [2] Associate Professor
[1,2] Department of Computer Science and Engineering, ISL Engineering College, Hyderabad, Telangana, India

bilalahmsiddique@gmail.com, zainlab2007@gmail.com

ABSTRACT
The growing use of digital images in sensitive applications demands secure transmission and storage mechanisms. Conventional encryption protects data confidentiality but reveals the existence of secret communication, while steganography conceals information without strong protection once detected. Secret sharing schemes provide distributed security but often generate image-based shares with increased overhead.
This paper proposes a multi-layer secure image sharing framework that integrates LSB steganography, AES encryption, and Shamir's Secret Sharing Scheme. Secret data is first embedded into a cover image using LSB steganography, encrypted using AES, and then divided into threshold-based binary shares using Shamir's scheme. The proposed approach ensures imperceptibility, strong confidentiality, and threshold-based access control while preserving image quality and reducing storage overhead, making it suitable for secure image communication and distributed storage applications.

Keywords: *Image Security, LSB Steganography, AES Encryption, Shamir's Secret Sharing, Threshold Cryptography, Secure Image Sharing.*

I. INTRODUCTION

With the widespread adoption of the Internet and digital media technologies, the secure exchange of sensitive information has become a critical concern. Images are commonly used to store and transmit confidential data such as personal identity information, medical records, and classified documents. Protecting such information from unauthorized access, interception, and tampering is essential in modern communication systems.

Traditional cryptographic techniques are effective in protecting data content but do not conceal the existence of secret communication. Encrypted data is easily identifiable and may attract malicious attacks. Steganography provides a complementary solution by hiding secret information within digital media, making communication covert. Among various steganographic techniques, Least Significant Bit (LSB) steganography is widely used due to its simplicity, high embedding capacity, and minimal impact on image quality.

Secret sharing schemes offer another layer of security by dividing a secret into multiple shares such that only a predefined number of shares can reconstruct the original secret. This approach provides fault tolerance and prevents single-point failure. However, many existing secret image sharing schemes generate image-based shares, which increase storage requirements and may degrade visual quality.

To address these challenges, this paper proposes a hybrid framework that combines steganography, encryption, and secret sharing. Unlike conventional approaches, the proposed system performs secret sharing on encrypted binary data rather than image-based shares. This design preserves image quality, enhances security, and reduces storage overhead.

II. LITERATURE SURVEY

Image security has been an active area of research due to the increasing use of digital images in sensitive applications such as healthcare, defense, forensics, and secure communication. Researchers have explored various techniques including cryptography, digital watermarking, and steganography to ensure confidentiality, integrity, and authenticity of image data. This section reviews significant contributions relevant to image encryption, watermarking, and steganography.

2.1 SD-EI: A Cryptographic Technique to Encrypt Images

S. Dey proposed SD-EI, a specialized cryptographic technique designed exclusively for image encryption. Unlike traditional text-based encryption algorithms, SD-EI addresses the unique characteristics of image data such as high redundancy, large data size, and strong pixel correlation. The technique combines cryptographic algorithms with image processing

operations to enhance security and resistance against attacks. The approach ensures confidentiality and integrity while maintaining efficient encryption and decryption processes. Presented at an international conference on cybersecurity and digital forensics, this work highlights the importance of domain-specific encryption techniques for multimedia security applications.

2.2 Cryptographic Technique for Security of Medical Images in Health Information Systems

Q.-A. Kester et al. presented a cryptographic technique tailored for securing medical images within health information systems. The study emphasizes the sensitivity of medical image data and the strict privacy requirements in healthcare environments. The proposed approach integrates encryption algorithms with key management and access control mechanisms to ensure secure storage, transmission, and retrieval of medical images. The work addresses challenges related to data confidentiality, integrity, and controlled access in health informatics. This research underscores the necessity of strong cryptographic frameworks for protecting medical images against unauthorized access and data breaches.

2.3 Digital Watermarking for Image Security Using Discrete Slantlet Transform

M. Mundher et al. explored digital watermarking techniques based on the discrete slantlet transform to enhance image security. The proposed method focuses on embedding imperceptible watermarks into images to provide copyright protection, authentication, and tamper detection. The use of the slantlet transform improves robustness against common image processing attacks while maintaining visual quality. The study discusses watermark embedding and extraction processes, as well as performance evaluation under different attack scenarios. This work contributes to multimedia security by demonstrating the effectiveness of transform-domain watermarking techniques.

2.4 Digital Watermarking Techniques for Image Security: A Review

A. Mohanarathinam provided a comprehensive review of digital watermarking techniques for image security. The paper surveys spatial domain, frequency domain, and transform domain watermarking methods, comparing their advantages and limitations. It discusses key performance factors such as imperceptibility, robustness, capacity, and security. The review also highlights recent advancements and the integration of watermarking with cryptographic techniques to strengthen image protection. This work serves as a valuable reference for researchers seeking to understand the evolution and current trends in image watermarking.

2.5 Digital Image Steganography: Survey and Analysis of Current Methods

A. Cheddad et al. presented an extensive survey of digital image steganography techniques. The paper analyzes various data hiding methods, including least significant bit (LSB) embedding, frequency-domain approaches, and adaptive steganography. It discusses the strengths and weaknesses of each technique in terms of capacity, imperceptibility, and resistance to detection. The study also examines steganalysis challenges and real-world applications such as covert communication and data hiding. This survey provides a strong foundation for understanding steganographic methods used in image security.

2.6 An Extensive Survey of Digital Image Steganography: State of the Art

M. Idakwo et al. presented a detailed survey on the state of the art in digital image steganography. The paper traces the evolution of steganographic techniques and highlights recent advancements aimed at improving robustness and hiding capacity. It discusses challenges posed by modern steganalysis techniques and explores emerging trends in multimedia security. The survey consolidates contemporary research efforts and identifies open research problems, making it a useful resource for researchers working on advanced steganographic systems.

III. PROBLEM STATEMENT

Despite significant progress in image security, existing approaches face several limitations:

- Encrypted images reveal the existence of secret communication.
- Steganographic methods lack strong cryptographic protection once detected.
- Image-based secret sharing schemes increase storage and transmission overhead.
- Single-layer security mechanisms are vulnerable to partial compromise.

Therefore, there is a need for a secure image sharing mechanism that preserves image quality, conceals secret existence, provides cryptographic confidentiality, and supports threshold-based reconstruction with minimal overhead.

IV. PROPOSED SYSTEM

The proposed system employs a three-layer security architecture:

1. **LSB Steganography** – Conceals secret data inside an image
2. **AES Encryption** – Encrypts the stego-image
3. **Shamir's Secret Sharing** – Divides encrypted data into binary shares

4.1 Encoding Phase (Sender Side)

Step 1: Input Acquisition
The sender selects a **cover image** and the **secret data** to be transmitted. The secret data may be textual or image-based. The cover image acts as a carrier to conceal the secret information.

Step 2: Binary Conversion of Secret Data
The secret data is converted into its binary representation. This step ensures compatibility with the LSB steganographic embedding process.

Step 3: LSB Steganographic Embedding
The binary secret data is embedded into the least significant bits of selected pixels of the cover image. Since LSB modification introduces minimal changes to pixel values, the resulting image, known as the **stego-image**, appears visually identical to the original cover image.
Purpose:
To conceal the existence of secret data while preserving image quality.

Step 4: AES Encryption of Stego-Image
The stego-image is encrypted using the Advanced Encryption Standard (AES) with a secret symmetric key. This process converts the stego-image into encrypted form, ensuring cryptographic confidentiality.
Purpose:
To protect the hidden data even if the stego-image is intercepted.

Step 5: Binary Encoding of Encrypted Image
The AES-encrypted stego-image is converted into a binary data stream. This prepares the encrypted image for secret sharing operations and avoids the generation of image-based shares.
Purpose:
To enable efficient data-level secret sharing and reduce storage overhead.

Step 6: Shamir's Secret Sharing Scheme
The binary data stream is divided into multiple shares using Shamir's Secret Sharing Scheme with a predefined (t,n)(t, n)(t,n) threshold. Each share is generated as a binary file and distributed to different participants or transmission channels.
Purpose:
To provide threshold-based access control and eliminate single-point failure.

Step 7: Secure Transmission of Shares
The generated binary shares are transmitted independently. Reconstruction is possible only when the minimum threshold number of shares is available.

4.2 Decoding Phase (Receiver Side)

Step 8: Collection of Shares
At the receiver end, the required minimum number of shares (ttt) is collected. Shares fewer than the threshold reveal no information.

Step 9: Reconstruction Using Shamir's Scheme
Using polynomial interpolation, the encrypted stego-image is reconstructed from the collected shares.
Purpose:
To recover the encrypted data securely and reliably.

Step 10: AES Decryption
The reconstructed encrypted stego-image is decrypted using the AES key shared securely between authorized users.
Purpose:
To restore the original stego-image.

Step 11: Secret Extraction Using Reverse LSB
The secret data is extracted from the decrypted stego-image by reversing the LSB embedding process. The extracted binary data is converted back into its original format.
Purpose:
To accurately retrieve the hidden secret data.

4.3 Key Features of the Proposed System

- Multi-layer security using steganography, encryption, and secret sharing
- High image quality preservation
- Threshold-based access control
- Binary share generation instead of image shares
- Fault tolerance and resistance to partial compromise

4.4 System Workflow Summary

1. Secret data → Binary conversion
2. Binary data → LSB steganographic embedding
3. Stego-image → AES encryption
4. Encrypted image → Binary encoding
5. Binary data → Shamir's Secret Sharing
6. Binary shares → Transmission
7. Threshold shares → Reconstruction
8. AES decryption → Stego-image
9. Reverse LSB → Secret recovery

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 4, 2025

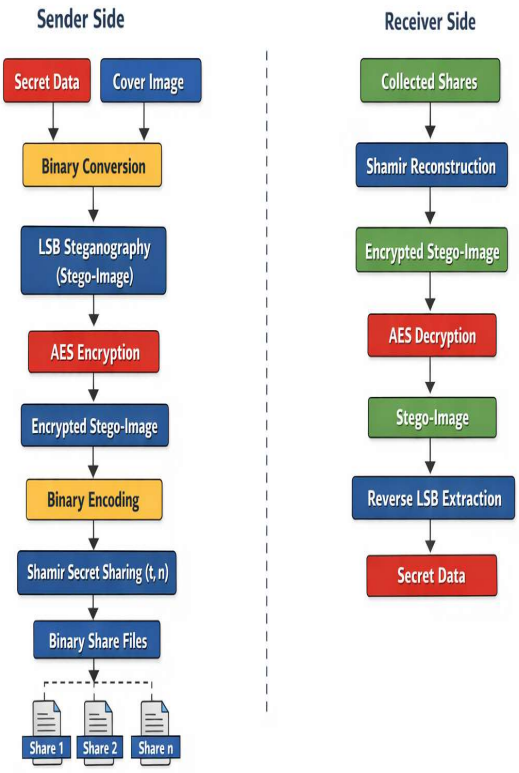

Fig 1: System-Flow

V. CONCLUSION

This paper presented a secure and quality-preserving image sharing framework that integrates LSB steganography, AES encryption, and Shamir's Secret Sharing Scheme. The proposed approach ensures imperceptible data hiding, strong cryptographic confidentiality, and threshold-based access control. By generating binary shares instead of image-based shares, the system reduces storage overhead while maintaining high image quality.

Furthermore, the layered security design improves robustness against unauthorized access and partial compromise, making the framework suitable for applications such as secure image transmission, cloud storage, and sensitive data protection. The proposed system demonstrates that combining steganography, encryption, and secret sharing provides an effective and practical solution for modern image security requirements.

VI. REFERENCES

[1]. [1] S. Dey, ‘‘SD-EI: A cryptographic technique to encrypt images,’’ in Proc. Int. Conf. Cyber Secur., Cyber Warfare Digit. Forensic (CyberSec), Jun. 2012, pp. 28–32.

[2]. Q.-A. Kester, L. Nana, A. C. Pascu, S. Gire, J. M. Eghan, and N. N. Quaynor, ‘‘A cryptographic technique for security of medical images in health information systems,’’ Proc. Comput. Sci., vol. 58, pp. 538–543, Jan. 2015.

[3]. M. Mundher, D. Muhamad, A. Rehman, T. Saba, and F. Kausar, ‘‘Digital watermarking for images security using discrete slantlet transform,’’ Appl. Math. Inf. Sci., vol. 8, no. 6, pp. 2823–2830, Nov. 2014.

[4]. A. Mohanarathinam, ‘‘Digital watermarking techniques for image security: A review,’’ J. Ambient Intell. Humanized Comput., vol. 11, no. 8, pp. 3221–3229, 2020.

[5]. L.K.Suresh Kumar , Mohammed Abdul Bari , Zero-Day Attack Detection In Multi-Tenant Cloud Environments Using Variational Autoencoders ,” International Journal of Applied Mathematics, ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)Volume 38 No. 3s, 2025. (Scopus -Q3 Journal) – Impact factor : 0.89

[6]. Mrs. Misbah Kousar , Dr. Sanjay Kumar , Dr. Mohammed Abdul Bari,” Design of a Decentralized Authentication and Off-Chain Data Management Protocol for VANETs Using Blockchain”, Communications on Applied Nonlinear Analysis, ISSN: 1074-133X, Vol 32 No. 2(2025) Scopus -Q4

[7]. A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, ‘‘Digital image steganography: Survey and analysis of current methods,’’ Signal Process., vol. 90, no. 3, pp. 727–752, Mar. 2010.

[8]. M. Idakwo, M. Muazu, E. Adedokun, and B. Sadiq, ‘‘An extensive survey of digital image steganography: State of the art,’’ ATBU J. Sci., Technol. Educ., vol. 8, no. 2, pp. 40–54, 2020.

[9]. A. Shamir, ‘‘How to share a secret,’’ Commun. ACM, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[10]. G. R. Blakley, ‘‘Safeguarding cryptographic keys,’’ in Proc. Int.Workshop Manag. Requirements Knowl. (MARK), 1979, pp. 313–318.

[11]. M. Mignotte, ‘‘How to share a secret,’’ in Proc. Workshop Cryptogr. Cham, Switzerland: Springer, 1982, pp. 371–375.

[12]. C. Asmuth and J. Bloom, ‘‘A modular approach to key safeguarding,’’ IEEE Trans. Inf. Theory, vol. IT-29, no. 2, pp. 208–210, Mar. 1983.

ISSN 2347–3657
Volume 13, Issue 4, 2025

[13]. C. S. Chum, B. Fine, G. Rosenberger, and X. Zhang, ‘‘A proposed alternative to the Shamir secret sharing scheme,’’ Contemp. Math., vol. 582, pp. 47–50, Jan. 2012.
[14]. K. E. Atkinson, An Introduction to Numerical Analysis. Hoboken, NJ, USA: Wiley, 2008.
[15]. B. Fine, A. I. S. Moldenhauer, and G. Rosenberger, ‘‘A secret sharing scheme based on the closest vector theorem and a modification to a private key cryptosystem,’’ Groups-Complex.-Cryptol., vol. 5, no. 2, pp. 223–238, Jan. 2013.
[16]. C.-C. Thien and J.-C. Lin, ‘‘Secret image sharing,’’ Comput. Graph., vol. 26, no. 5, pp. 765–770, Oct. 2002.