ISSN 2319-5991 www.ijerst.com

Peer Reviewed, Referred & Indexed Journal

Research Paper

SMART REVERSIBLE DATA HIDING FOR ENCRYPTED IMAGES WITH SECRET SHARING

MODUKURU PRADEEP[1], BATHULA SHIVANI[2], PARAMATI ANUSHA[3], RANGA NEHA[4], POLISETTI MANOJ[5]

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus**,** Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus**,** Ibrahimpatnam, Telangana, India

ABSTRACT— Reversible data hiding in encrypted images (RDH-EI) and secret sharing-based reversible data hiding in encrypted images (SIS-RDHEI) schemes still lack diffusivity and high embedding capacity. As a result, a novel high-capacity RDH-EI scheme that combines secret sharing technology with adaptive most significant bit (MSB) prediction is proposed in this paper. First, the original image is subjected to adaptive MSB prediction, and a cryptographic feedback secret sharing strategy encrypts the spliced pixels to free up embedding space. Each encrypted image is sent to a data hider during the data hiding phase to independently embed the secret information. The original image can be recovered without loss and the secret information extracted when r copies of the image with the secret text are collected. The diffusivity, reversibility, and separability of the proposed method in this paper are demonstrated by performance evaluation.

Index Terms – Reversible data hiding in encrypted images (RDH-EI), secret sharing, secret sharing-based reversible data hiding (SIS-RDHEI), adaptive MSB prediction, image encryption, data embedding, lossless image recovery, information hiding, cryptographic feedback, image security, privacy preservation, secure data transmission.

I. INTRODUCTION

In recent years, reversible data hiding in encrypted images (RDH-EI) has attracted significant attention due to the increasing

demand for secure image transmission and confidential data embedding in cloud and network environments. Among the various approaches, secret image sharing based reversible data hiding in encrypted images (SIS-RDHEI) schemes have emerged as an effective solution to simultaneously achieve data security and reversibility. Initially, Wu et al. introduced secret sharing technology into RDH-EI, where secret data were divided into shares and embedded into encrypted images using techniques such as differential expansion and differential histogram shifting. This pioneering work opened a new direction for combining cryptographic security with reversible data hiding. Subsequently, Chen et al. improved the scheme by employing differential expansion and additive homomorphism properties to embed secret data. However, their approach supported only a single data hider and suffered from a relatively low embedding rate, which limited its practical applicability. To address the embedding capacity issue, later research introduced multiple data hiders, allowing secret data to be embedded by replacing one pixel among every n pixels. Although this improved flexibility, the embedding rate decreased as the number of data hiders increased, and when n exceeded a certain threshold, the performance became restricted. Further improvements were proposed using advanced encryption strategies. For instance, a scheme based on the Advanced Encryption Standard (AES) cryptographic feedback mechanism utilized most significant bit (MSB) prediction technology to enhance embedding efficiency and reduce encrypted image size. While this method achieved better performance compared to earlier models, the embedding capacity was still not sufficiently high for practical large-scale applications. Another notable advancement focused on utilizing redundant space generated during the encryption process. By constructing a finite field and expanding pixel pairs and polynomial coefficients to 16 bits, the embedding space was significantly increased. This approach ensured reversible extraction and achieved higher embedding capacity compared to earlier SIS-RDHEI methods. However, it lacked password feedback technology and did not fully exploit the correlation between neighboring pixels in the carrier image, resulting in limited diffusivity and suboptimal security performance. Overall, existing SIS-RDHEI schemes face a challenging trade-off among embedding rate, security, diffusivity, and reversibility. Achieving high embedding capacity while maintaining strong

encryption security and complete reversibility remains a complex research problem. To overcome these limitations, the proposed work introduces a high-capacity SIS-RDHEI scheme based on adaptive MSB prediction. This method integrates the strengths of previous secret sharing and encryption feedback strategies while innovatively applying adaptive MSB prediction to better utilize image redundancy. By expanding polynomial coefficients to 16 bits according to the characteristics of adaptive MSB prediction, the proposed scheme significantly enlarges the embedding space. At the same time, it enhances diffusivity through improved encryption feedback mechanisms and leverages pixel correlation for higher prediction accuracy. The proposed algorithm not only improves embedding capacity but also ensures reversibility and separability, meaning that secret data extraction and image recovery can be performed independently depending on the available keys. Additionally, the scheme strengthens security and supports disaster recovery backup of the carrier image, making it highly suitable for secure image storage, cloud data protection, and sensitive information transmission.

Through efficient use of image redundancy and advanced prediction techniques, the proposed SIS-RDHEI scheme achieves a balanced combination of high embedding rate, strong security, and practical applicability, offering significant improvements over existing methods and contributing valuable advancements to the field of reversible data hiding in encrypted images.

II. RELATED WORK

A. Generative Steganography Based on Long Readable Text Generation

With the rapid development of information security and artificial intelligence, steganography techniques have evolved from traditional media hiding methods to text-based content generation approaches. In this paper, the authors propose a generative steganography method based on long readable text generation. The scheme uses advanced natural language generation models to embed secret information within automatically generated meaningful text. Unlike conventional steganography methods that modify existing content, this approach generates new text that appears natural and readable while secretly carrying hidden data. The method improves concealment and reduces the risk of detection by steganalysis

tools. It also enhances security by mapping secret bits into linguistic structures during the generation process. Experimental results show that the generated texts maintain high readability and semantic coherence while ensuring reliable data extraction. The study highlights the potential of combining deep learning and steganography for secure communication. Overall, the paper presents an innovative and intelligent framework for secure text-based information hiding using generative models.

B. BOWS2 Image Dataset

The BOWS2 dataset is a benchmark image dataset widely used for research in steganography and digital image security. It provides a collection of standard grayscale images that are commonly used to evaluate data hiding and steganalysis algorithms.

The dataset helps researchers test the performance of various steganographic and reversible data hiding techniques under uniform experimental conditions. Since the images are natural and diverse, they are suitable for analyzing embedding capacity, distortion levels, and detection resistance. BOWS2 is especially useful for comparing the effectiveness of different security algorithms in terms of imperceptibility and robustness.

Researchers use this dataset to measure parameters such as PSNR, embedding rate, and visual quality after data embedding. It supports fair performance comparison among different image security schemes. Overall, the BOWS2 dataset plays an important role in validating and benchmarking image-based data hiding and encryption techniques.

C. Generative Steganography via Auto Generation of Semantic Object Contours

With the advancement of deep learning techniques, generative steganography has emerged as a powerful approach for secure information hiding. In this paper, the authors propose a novel generative steganography method based on the automatic generation of semantic object contours. Instead of modifying existing images, the proposed approach generates images where secret information is embedded within the semantic contours of objects. This method enhances concealment by integrating hidden data into meaningful visual structures. The generated images appear natural and semantically consistent, reducing the risk of detection by steganalysis methods. The framework utilizes deep neural networks to ensure accurate encoding and decoding of secret data. Experimental results

demonstrate improved security, robustness, and visual quality compared to traditional steganography techniques. The study highlights the effectiveness of combining semantic understanding with generative models for secure image-based communication. Overall, the paper presents an innovative and secure generative framework for advanced image steganography.

D. Secret-to-Image Reversible Transformation for Generative Steganography

With the rapid growth of generative models in information security, researchers have introduced advanced techniques for secure data hiding. In this paper, the authors propose a secret-to-image reversible transformation method for generative steganography. The approach transforms secret information directly into meaningful images instead of embedding it into existing cover media. This method improves concealment because the generated image itself represents the hidden data. The scheme ensures reversibility, allowing the original secret to be accurately reconstructed from the generated image. By leveraging deep learning and generative networks, the method enhances security and resistance against steganalysis attacks. Experimental results demonstrate that the generated images maintain high visual quality while ensuring reliable data extraction. The framework also improves robustness and reduces the detectability of hidden information. Overall, the study presents an innovative and secure reversible transformation technique for generative steganography applications.

III. PROPOSED METHODOLOGY

In the proposed system, a high-capacity reversible data hiding method is developed using the SIS-RDHEI scheme combined with adaptive MSB prediction. The system expands polynomial coefficients up to 16 bits, which increases the space available for embedding secret information. It makes full use of the redundancy present in the carrier image to improve embedding capacity. The method also applies secret sharing to divide the secret into multiple shares, improving reliability and backup support. Unlike traditional schemes, this approach enhances diffusivity by strengthening the encryption and sharing process. The system ensures that the original image can be perfectly recovered without any loss. It also supports separability, allowing independent data extraction and image recovery. Overall, the proposed system improves embedding rate, security, and practical usability.

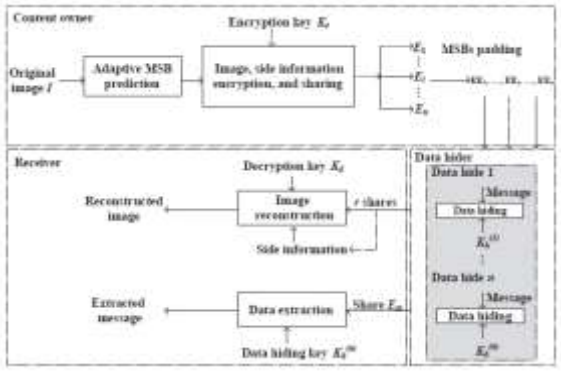
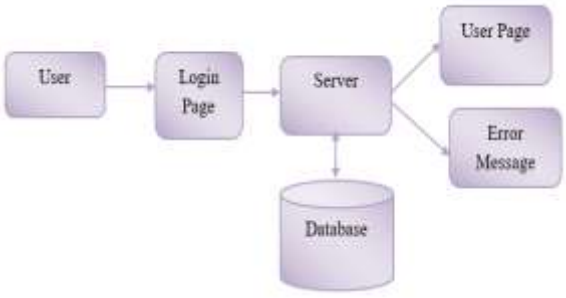


Fig. 1: System Overview

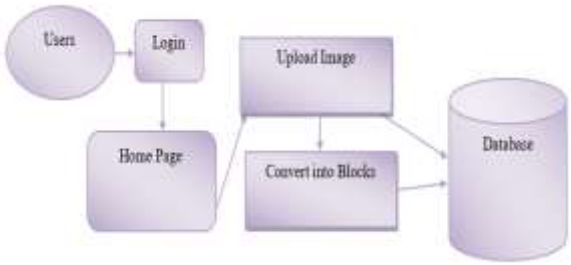
1. User Interface Design

To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password, Email id, City and Country into the server. Database will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page. It will search the query and display the query.



2. Users Module

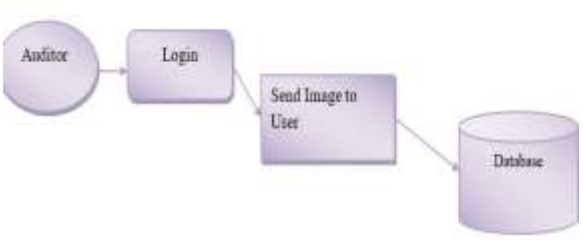
The Users module is the main working module of the system. It allows users to register and log in securely. After successful login, the user can upload an image to the system. Once the image is uploaded, the system performs adaptive MSB prediction to create embedding space. Then the image is encrypted using an encryption key to maintain confidentiality. After encryption, secret sharing is applied to divide the image into multiple shares. The user can embed secret data into these encrypted shares. The user also has the ability to recover the original image and extract the hidden message when required. This module ensures secure image processing, data hiding, and reversible recovery. It acts as the primary interaction point between the user and the system.



3. Auditor Module

The Auditor module is responsible for monitoring and verifying system activities. The auditor logs into the system using secure credentials. After login, the auditor can view encrypted image shares stored in

the database. The auditor checks whether the data is securely stored and verifies the integrity of image shares. If required, the auditor can send image shares for validation or recovery. The auditor does not modify the original image but ensures that the system follows proper security procedures. This module adds an extra layer of trust and monitoring to the system.



4. JSP Dashboard

The JSP Dashboard module acts as the main user interface of the system. It displays uploaded encrypted data along with file names, user details, and timestamps. It shows transaction status, verification results, and packet detection outcomes. The dashboard also displays pending registration requests and approved users. It allows users and auditors to monitor system activities in a clear and organized way. All important project modules and their current status are visible through this interface. It helps in tracking data flow, recovery results, and system logs. This module improves usability by providing a simple and structured view of the entire system.

5. MySQL Database

The MySQL Database module is used to store and manage all system-related data. It maintains user registration details, login credentials, roles, device metadata, encrypted data records, and system logs. It stores file details, timestamps, verification status, and transaction information. Critical encrypted data is stored securely, while supporting information like user roles and logs are also maintained for system operation. This hybrid storage approach ensures good performance and strong data security. The database supports data retrieval during verification, monitoring, and recovery processes. It acts as the central storage unit of the entire project.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

The experimental results show that the proposed secret sharing-based RDH-EI scheme achieves high embedding capacity while ensuring lossless image recovery and secure data extraction. The integration of adaptive MSB prediction and cryptographic feedback secret sharing improves embedding efficiency, image diffusivity, and security. Performance evaluation confirms

the reversibility, separability, and robustness of the proposed method compared to existing RDH-EI techniques.

Fig. 2: Login

Fig. 3: Registration

Fig. 4: Upload Image

Fig. 5: Secure Image Gallery

Fig. 6: Auditor Data

Fig. 6: Result

V. CONCLUSION

This project presents a secure and high-capacity reversible data hiding system for encrypted images using secret sharing and adaptive MSB prediction. The proposed method improves embedding capacity by expanding polynomial coefficients up to 16

bits and efficiently utilizing image redundancy. It ensures that secret data can be embedded into encrypted images without revealing the original image content to the data hider. The system achieves complete reversibility, allowing perfect recovery of the original image without any loss. It also provides separability, enabling independent extraction of hidden data and image restoration. Diffusivity is enhanced through improved encryption and sharing mechanisms, increasing overall security. The use of secret sharing supports disaster recovery backup and reliable data protection. Compared to existing schemes, the proposed approach offers better embedding rate, stronger security, and improved flexibility. Performance evaluation confirms its effectiveness in terms of embedding capacity and recovery accuracy. Overall, the project provides a practical and secure framework for confidential image transmission and storage applications.

REFERENCES

[1] X. Wu, J. Weng, and W. Yan, Adopting secret sharing for reversible data hiding in encrypted images, Signal Process., vol. 143, pp. 269–281, 2018.

[2] Y. C. Chen, T. H. Hung, S. H. Hsieh, and C. W. Shiu, A new reversible data hiding in encrypted image based on multi-secret sharing and lightweight cryptographic algorithms, IEEE Trans. Inf. Forensics Secur., vol. 14, no. 12, pp. 3332–3343, 2019.

[3] B. Chen, W. Lu, J. Huang, J. Weng, and Y. Zhou, Secret sharing based reversible data hiding in encrypted images with multiple data-hiders, IEEE Trans. Dependable Secure Comput., vol. 19, no. 2, pp. 978–991, 2022.

[4] C. Qin, C. Jiang, Q. Mo, H. Yao, and C. C. Chang, Reversible data hiding in encrypted image via secret sharing based on GF(p) and GF(2^8), IEEE Trans. Circuits Syst. Video Technol., vol. 32, no. 4, pp. 1928–1941, 2022.

[5] Z. Hua, Y. Wang, S. Yi, Y. Zhou, and X. Jia, Reversible data hiding in encrypted images using cipher-feedback secret sharing, IEEE Trans. Circuits Syst. Video Technol., vol. 32, no. 8, pp. 4968–4982, 2022.

[6] Z. X. Wang, M. Q. Zhang, and Y. J. Kong, Reversible data hiding in encrypted images based on image secret sharing, (in Chinese), Journal of

Computer Applications, vol. 42, no. 5, pp. 1480–1489, 2022.

[7] Y. Ke, M. Zhang, X. Zhang, J. Liu, T. Su, and X. Yang, A reversible data hiding scheme in encrypted domain for secret image sharing based on Chinese remainder theorem, IEEE Trans. Circuits Syst. Video Technol., vol. 32, no. 4, pp. 2469–2481, 2022.

[8] Y. Wang and W. He, High capacity reversible data hiding in encrypted image based on adaptive MSB prediction, IEEE Trans. Multimed., vol. 24, pp. 1288–1298, 2022.

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

[10] C. C. Thien and J. C. Lin, Secret image sharing, Comput. Graph., vol. 26, no. 5, pp. 765–770, 2002.

AUTHORS Profile

Mr. MODUKURU PRADEEP has received his B.Tech from JNTUK, Kakinada in 2013, M.Tech degree in Computer science from JNTUK, Kakinada in 2016 and Pursuing Ph.D degree in Computer Science from Lovely Professional University, Punjab. He is dedicated to teaching field from the last 10 years. His research area Deep Learning. At present he is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India.

Ms. BATHULA SHIVANI pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.

Ms. PARAMATI ANUSHA pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.

Ms. RANGA NEHA pursuing B.Tech degree in Computer Science and Engineering at Guru

Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.

Mr. POLISETTI MANOJ pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.