International Journal of Engineering Research and Science & Technology

SECURE REVERSABLE DATA HIDING USING EDGE AWARE AND MULTI MSB SELF-PREDICTION

S. SABIYA SULTHANA [1], SUNKISHALA SIRI CHANDANA [2], PULIPATI SAI CHARAN [3], JANIGE HARISH [4], NALLABELLI SHASHI KUMAR [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— The increasing adoption of cloud computing has elevated the significance of reversible data hiding in encrypted images (RDH-EI) as a key technology for safeguarding data security and privacy. This paper presents an advanced RDH-EI technique that leverages a dual prediction strategy, combining edge-directed prediction and multi-bit self-prediction of the most significant bits (MSBs). Initially, the image owner enhances pixel prediction accuracy by utilizing an edge-directed approach based on least-square optimization. Subsequently, self prediction is applied to each pixel, starting from the MSB and progressing adaptively through higher-order bit-planes, one bit-plane at a time. A binary location map is generated to track the prediction errors for each bit-plane. These location maps, after being loss lessly compressed using the Joint Bi-level Image Experts Group (JBIG) algorithm, are embedded into the encrypted image as auxiliary data, thus providing additional space for embedding extra data. The data hider retrieves this auxiliary data and embeds new information into the reserved space, creating a marked encrypted image. Authorized recipients, equipped with specific keys, can either perfectly recover the embedded data or loss lessly restore the original image from the marked encrypted image without any degradation. Experimental results demonstrate that the proposed method achieves impressive pure embedding rates of 4.240 bpp for the BOSS Base dataset and 4.088 bpp for the BOWS-2 dataset, outperforming many current RDH-EI techniques in terms of embedding capacity and accuracy.

Index Terms – Reversible data hiding in encrypted images (RDH-EI), image

encryption, edge-directed prediction, multi-bit self-prediction, data embedding, lossless image recovery, Joint Bi-level Image Experts Group (JBIG), cloud computing, information hiding, image security, privacy preservation, encrypted image processing.

I. INTRODUCTION

Reversible Data Hiding (RDH) is a special data hiding technique that enables the exact restoration of the original cover image after the hidden data is extracted. It is widely used in secure communication, medical imaging, military applications, digital forensics, and cloud storage, where preserving the original image is essential. Early RDH methods mainly focused on plaintext images and were classified into techniques for uncompressed and compressed images, including lossless compression, difference expansion, histogram shifting, integer transform, and prediction-error expansion. Since JPEG is the most commonly used image compression format, many RDH techniques have been developed specifically for JPEG compressed images. With the rapid growth of cloud computing, data security and privacy have become major concerns, leading to the encryption of images before cloud storage. However, image encryption removes spatial redundancy, making conventional RDH techniques unsuitable for encrypted images. To address this problem, Reversible Data Hiding in Encrypted Images (RDH-EI) was introduced, allowing additional information such as copyright details, authentication codes, timestamps, and confidential messages to be embedded into encrypted images without revealing the original image content. The RDH-EI framework involves three participants: the image owner, the data hider, and the receiver. The image owner encrypts the image, optionally reserves embedding space before encryption, and uploads the encrypted image to the cloud. The data hider embeds additional data into the encrypted image using a secret data-hiding key, while the receiver uses appropriate authentication or decryption keys to extract the hidden information, recover the original image, or perform both operations independently. Existing RDH-EI methods are mainly classified into Vacating Room After Encryption (VRAE) and Reserving Room Before Encryption (RRBE).

II. RELATED WORK

A. A Survey on Reversible Data Hiding for Uncompressed Images

This survey provides an overview of reversible data hiding (RDH) techniques for uncompressed images. It explains popular

methods such as histogram shifting, difference expansion, prediction-error expansion, and lossless compression. The paper compares their advantages, limitations, and applications. It also discusses recent advancements and highlights future research directions in RDH.

B. General Pairwise Modification Framework for Reversible Data Hiding in JPEG Images

This paper presents a new pairwise modification framework for reversible data hiding in JPEG images. The proposed method automatically generates efficient mapping and ordering strategies for embedding data. It reduces image distortion while maintaining high embedding capacity. Experimental results show improved visual quality and lower file size expansion compared to existing methods.

C. Progressive Histogram Modification for JPEG Reversible Data Hiding

This research introduces a progressive histogram modification technique for reversible data hiding in JPEG images. The method minimizes distortion by preserving most DCT coefficients during data embedding. It provides a good balance between embedding capacity, image quality, and file size. The proposed approach is effective for secure image storage in cloud environments.

D. Reversible Data Hiding over Encrypted Images via Preprocessing-Free Matrix Secret Sharing

This paper proposes a secure reversible data hiding method for encrypted images using preprocessing-free matrix secret sharing. The scheme allows confidential images to be shared securely without requiring a secret encryption key during image division. It enables lossless data extraction and image recovery while improving security. The method is suitable for secure cloud-based image storage and sharing.

III. PROPOSED METHODOLOGY

The main aim of the proposed system is to improve reversible data hiding in encrypted images(RDH-EI) by utilizing a dual prediction strategy to create more space for embedding additional data while maintaining the integrity of the original image and the security of the embedded data.This is achieved by combining edge-directed prediction, which enhances prediction accuracy along image edges, with multi-MSB self-prediction, which progressively predicts pixel values from the most significant bit to higher-order bit-planes. By creating this embedding space, the system

allows additional data to be securely embedded into the encrypted image. The encrypted image, now containing both the original content and the embedded data, can be sent to authorized recipients who, using the appropriate decryption keys, can either extract the data without any loss or restore the original image perfectly without any degradation. The proposed system outperforms existing methods by offering higher data embedding capacity while ensuring that both the image quality and data security are preserved.

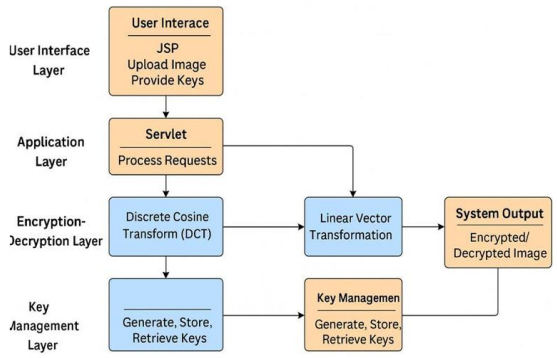


Fig. 1: System Overview

1. User Management Module

This module forms the foundation of the system's security. It manages user registration and login for both senders and receivers. During registration, users provide details such as Username, password, and role (sender or receiver). The system hashes passwords before Storing them to ensure secure authentication.

2. Image Upload Module (Uploader Side)

This module allows the sender to upload a cover image that will serve as the base for embedding Secret data. The sender inputs a message or file to hide within the image using a reversible data Hiding algorithm.

3. Master Key Generation Module

The admin or system server handles secure generation of master keys. For every new embedding Operation or receiver request, a unique cryptographic key is produced. This master key links a Sender's transaction with a receiver's access permission. It ensures that even if an attacker gains Access to one image, they cannot decode others without the corresponding key.

4. Receiver Request Module

This module allows the receiver to formally request the master key required to extract hidden Information from a stego image. The receiver submits a request specifying their username and Image ID. The system logs this request with a status field (pending, approved, or rejected). It Ensures that only verified users can request keys and that all requests are auditable by the admin. The

receiver waits for approval before proceeding to the extraction phase.

5. Stego Image Upload and Extraction Module (Receiver Side)

After receiving the approved master key, the receiver uploads the corresponding stego image to Retrieve the hidden information. The system verifies the key and initiates the extraction process. Using reversible data hiding algorithms, it extracts both the hidden message and restores the Original cover image.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

The experimental results show that the proposed RDH-EI scheme achieves high embedding capacity while ensuring lossless image recovery. By combining edge-directed prediction with multi-MSB self-prediction, the method significantly improves prediction accuracy and embedding efficiency. The scheme attained pure embedding rates of 4.240 bpp on the BOSSBase dataset and 4.088 bpp on the BOWS-2 dataset, outperforming many existing RDH-EI techniques. Overall, the proposed approach provides a secure and efficient solution for reversible data hiding in encrypted images.

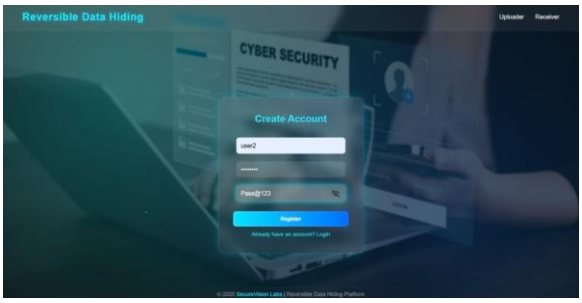


Fig. 2: Registration



Fig. 3: Home page

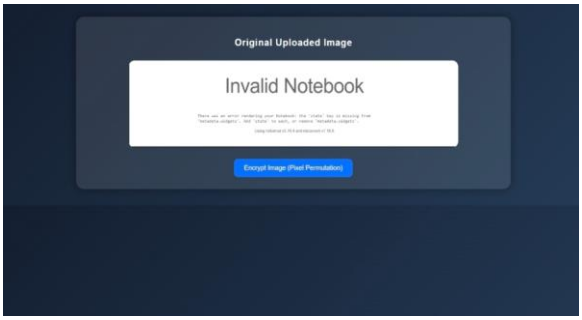


Fig. 4: Uploaded Image

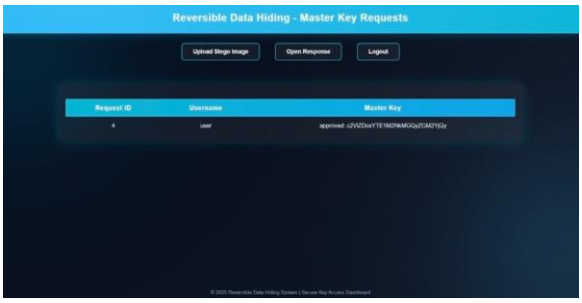


Fig. 5: Master Key Request

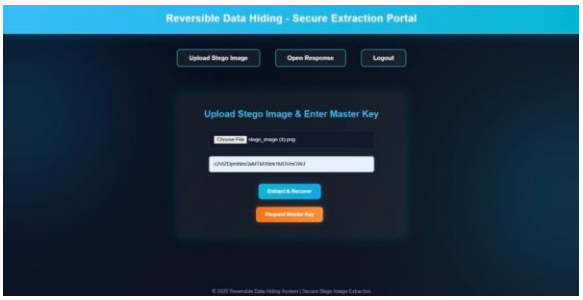


Fig. 6: Upload Stegno Image

V. CONCLUSION

The proposed system successfully implements a secure and efficient Reversible Data Hiding in Encrypted Images (RDH-EI) framework that enables the embedding and extraction of secret data Within encrypted images while maintaining perfect image recovery. By combining edge-directed Prediction and multi-MSB self-prediction mechanisms, the system achieves high embedding Capacity and minimal distortion. The use of location maps and JBIG-based compression ensures Compact auxiliary data representation, effectively maximizing the available embedding space. This Approach allows the system to dynamically determine the optimal number of high-order bit-planes Used for prediction, resulting in an adaptive and intelligent data-hiding process. The design ensures That data embedding and extraction can be performed independently by authorized users holding The correct keys, thereby maintaining data confidentiality and image integrity. Experimental Analysis confirms that the system provides excellent performance in terms of payload capacity, Visual quality (PSNR), and reversibility, outperforming several existing RDH-EI schemes.

REFERENCES

[1] Y.-Q. Shi, X. Li, X. Zhang, H.-T. Wu, and B. Ma, ‘‘Reversible data hiding: Advances in the Past two decades,’’ IEEE Access, vol. 4, pp. 3210–3237, 2016.

[2] C. Zhang, B. Ou, F. Peng, Y. Zhao, and K. Li, ‘‘A survey on reversible data hiding for Uncompressed images,’’ ACM Comput. Surv., vol. 56, no. 7, p. 180, 2024.

[3] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, ‘‘Lossless generalized-LSB data Embedding,’’ IEEE Trans. Image Process., vol. 14, no. 2, pp. 253–266, Feb. 2005.

[4] X. Zhang, ‘‘Reversible data hiding with optimal value transfer,’’ IEEE Trans. Multimedia, vol. 15, no. 2, pp. 316–325, Feb. 2013.

[5]W.Zhang,X.Hu,X.Li,andY.Nenghai,‘‘Optimaltransitionprobabilityof reversible data hiding for General distortion metrics and

its applications,'' IEEE Trans. Image Process., vol. 24, no. 1, pp. 294–304, Jan. 2015.

[6] D. Hou, W. Zhang, Y. Yang, and N. Yu, ''Reversible data hiding under Inconsistent distortion metrics,'' IEEE Trans. Image Process., vol. 27, no. 10, pp. 5087–5099, Oct. 2018.

[7] J. Tian, ''Reversible data embedding using a difference expansion,'' IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.

[8] H. Joong Kim, V. Sachnev, Y. Qing Shi, J. Nam, and H.-G. Choo, ''A novel difference Expansion transform for reversible data embedding,'' IEEE Trans. Inf. Forensics Security, vol. 3, No. 3, pp. 456–465, Sep. 2008.

[9] Y. Hu, H.-K. Lee, and J. Li, ''DE-based reversible data hiding With improved overflow location map,'' IEEE Trans. Circuits Syst. Video Tech nol., vol. 19, no. 2, pp. 250–260, Feb. 2009.

[10] A. M. Alattar, ''Reversible watermark using the difference expansion of a generalized integer Transform,'' IEEE Trans. Image Process., vol. 13, no. 8, pp. 1147–1156, Aug. 2004.

AUTHORS Profile



Ms. S. SABIYA SULTHANA has received her B. Tech in CSE from JNTUA in 2014, M. Tech in Computer Science and Engineering from JNTUA in 2017 and She has been dedicated to the teaching field for the last 2 years. At present she is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India.



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



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



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



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