International Journal of Innovative Research in Technology and Science
ISSN: 2321-1156 www.ijirts.org Volume 13 Issue 2, March 2025

A Survey on Reversible Data Hiding for Encrypted Image Based on Block Mean Difference Histogram Shifting

Jigisha Mehra, *Amit Jha, Kamini Maheshwar*
Department of CSE, University Institute of Technology Barkatullah University, Bhopal (M.P), India
mehrajigisha@gmail.com, amitkumarjha40@gmail.com, kaminimaheshwar@gmail.com

Abstract **-** Reversible data hiding in encrypted images (RDHEI) has become a critical technique for safeguarding data privacy and security in the era of digital communication and cloud computing. This paper presents a comprehensive survey of existing reversible data hiding techniques, including least significant bit (LSB) substitution, difference expansion (DE), and histogram modification. These techniques have contributed significantly to the field by enabling the embedding and extraction of hidden data while preserving the reversibility of the original image. However, they often encounter challenges such as low peak signal-to-noise ratio (PSNR) and high error rates, which can degrade the visual quality and reliability of the reconstructed images. To overcome these limitations, we propose a novel RDHEI framework based on block mean difference histogram shifting. This approach leverages the block-wise mean differences and their histogram properties to embed additional data while ensuring high payload capacity and minimal image degradation. By effectively addressing the issues of low PSNR and high errors, our proposed technique significantly improves the performance of reversible data hiding in encrypted images. We compare the existing methods in detail, outlining their strengths and weaknesses, and highlight how our framework achieves lossless recovery of the original image. Ultimately, our proposed approach ensures secure, reliable, and reversible data embedding for a wide range of digital security applications.

Keywords: Reversible Data Hiding, Encrypted Images, Histogram Shifting, Data Security, Payload Capacity

I. INTRODUCTION

A growing amount of private data is being stored on cloud servers for efficient processing due to the development of cloud computing technology. However, data privacy and security issues have also arisen from this trend. To ensure the confidentiality of sensitive images, it is common for users to encrypt images before uploading them to the server. However, there are limitations on the server's processing power for encrypted images. To solve the problem of authenticating and managing encrypted images at the cloud server side, the Reversible Data Hiding for Encrypted Images (RDHEI) technique has been proposed, which can hide and extract data losslessly in encrypted images. Data hiding is considered a promising method to achieve data security for responsible AI. Typically, data hiding involves concealing information in a specific form within another type of media. It can take different forms, such as encoding confidential information into an existing text piece or embedding audio files into a digital image. As digital assets become more diverse and ubiquitous, the importance and scope of data-hiding applications will only continue to grow [1]. In today's digital age, as digital communication and multimedia data become increasingly prevalent, the data-hiding process has become crucial. Ensuring responsible AI, such as machine learning as services, per-requisite, necessitates secure communication across all mediums, and the accountability of responsible AI, such as digital intellectual property, necessitates protection against theft and misuse. In its traditional form, the data-hiding process can be categorized into three types: watermarking, steganography, and cryptography [2]. Data hiding is the art and science of communicating secret data in an appropriate multimedia carrier, e.g., image, audio, and video files.

Digital Steganography and watermarking are the two kinds of data hiding. Reversible data hiding can be defined as an approach where the data is hidden in the host media, which may be a cover image. A reversible data hiding algorithm can recover the original image losslessly after the data has been extracted. Reversible data embedding, which is also called lossless data embedding, embeds invisible data (which is called a payload) into a digital image in a reversible fashion. As a basic requirement, the quality degradation of the image after data embedding should be low. An intriguing feature of reversible data embedding is the reversibility. That is, one can remove the embedded data to restore the original image. Data hiding is a technique for embedding information into covers such as audio, image, and video files. It can be used for copyright protection, media notation, integrity authentication, covert communication, etc. Most data-hiding methods embed messages into the cover media, such as images or videos, to generate the marked media by only modifying the least

significant part of the cover and, thus, ensuring perceptual transparency. The embedding process will usually introduce permanent distortion to the cover. That is, the original cover can never be reconstructed from the marked cover. However, in some applications, such as medical imagery, military, and law forensics, no degradation of the original cover is allowed.

We need a special kind of data hiding method for such cases, which is referred to as reversible data hiding (RDH) or lossless data hiding, by which the original cover can be lossless restored after the embedded message is extracted. The block diagram of RDH shows that reversible Steganography or watermarking can restore the original carrier without any distortion or with ignorable distortion after the extraction of hidden data. So, reversible data hiding is now becoming popular. Fig 1.1 Reversible data hiding is a basic requirement, and the quality degradation of the image after data embedding should be low. An intriguing feature of reversible data embedding is the reversibility. That is, one can remove the embedded data to restore the original image. From the information hiding point of view, reversible data embedding hides some information in a digital image in such a way that an authorized party could decode the hidden information and also restore the image to its original, pristine state. An information-hiding system is characterized by four different aspects: capacity, security, perceptibility and robustness [3].

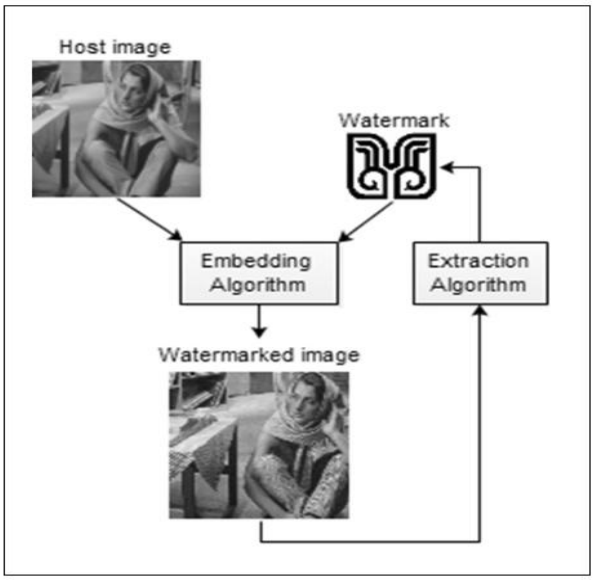

Fig.1: RIEDH in process

1.1 RDH Techniques

Reversible data hiding has been there for several years. Researchers have come up with various methods for hiding reversible data. The following are different techniques which have been proposed over the years. Circular visual cryptography was introduced in 2005. In this scheme, a circular shadow image can hide two or more confidential data sets in circular images and display them in both the inner and outer regions of the circular images. However, it can only produce a circular shadow image without the central part causing a low. Resolution on the images at the inner portion, as seen in Figure 1. It encrypts data into two ringed shadow images, allowing the hiding of two confidential data sets simultaneously.

1. Histogram block Shift Based Technique. The histogram-shifting-based reversible data hiding schemes embed data by shifting the histogram into a fixed direction. There are two important points in these schemes: peak point and zero point. The peak point corresponds to the grayscale value, which corresponds to the maximum number of pixels in the histogram of the giver image. The zero point is usually the point at which the number in the histogram is zero. The minimum number of pixels is selected as the zero point to increase the embedded capacity. In histogram-shifting-based algorithms, the pixels between the peak and zero pairs were modified in the embedding processing, the pixel in the peak point was used to carry a bit of the secret message, and the others were modified. No secret data were embedded. The hiding capacity of the histogram shifting-based data hides equals the number of pixels in the peak points; the larger the number of pixels in the peak point, the higher the hiding capacity. To increase the hiding capacity, more of the peak points and zero pairs can be used. Sometimes, it is difficult to find more pairs of peaks and zero points because the zero points are not searched [6].

2. Difference Expansion (DE) Based Technique. Difference expansion (DE) based technique for Reversible Data Hiding is proposed by Tian [2]. In the DE technique, extra storage space is discovered by exploring the redundancy in the image content. The DE technique is used to embed a payload into digital images reversibly. Both the payload capacity limit and the visual quality of embedded images of the DE method are among the best in the literature, along with a low computational complexity [5].

3. Least Significant Bit Modification Based Technique. One of the earliest methods is the modification of the LSB (Least significant bit). In this well-known method, the LSB of each signal sample is replaced (overwritten) by a secret data bit. During extraction, these bits are read in the same scanning order, and secret data is reconstructed [4].

II. RELATED WORK

Reversible data hiding has been done over the past few years. Some important techniques are discussed here. This section aims to classify the existing RDHEI techniques based on the underlying image-processing mechanisms involved. **J. Huang et al. [7]** discovered that the previously proposed algorithms for embedding secret data in the clear domain cannot be applied in the encrypted domain [37]. Indeed, classical encryption methods do not allow the correlation between neighbouring pixels to be maintained without introducing security flaws. In their work, the authors introduce a new strategy to encrypt an image, with the objective being that the conventional data-hiding algorithms designed in the clear domain can be deployed directly to embed data in the encrypted image. Specifically, the original image is split into non-overlapping blocks. Within each block, all pixels are encrypted by applying the XOR operation using the same pseudo-randomly generated byte. The encrypted blocks are then pseudo-randomly permuted. Note that pixels within the same block are not scrambled, but only the order of the blocks is changed. With this encryption method, the statistical properties of the clear image, especially the histogram of pixel differences or prediction errors, are preserved. Therefore, the conventional data-hiding algorithms in the clear domain can be applied in the encrypted domain. Still, the embedding capacity is limited by the handling of the under/overflow problem. **Yan Chen et al. [8]** This paper proposes a novel method of reversible data hiding in encrypted images (RDH-EI). We first provide an RDH-EI approach using single-level embedding, in which three parties are involved, including an image owner, a data hider, and a recipient. The image owner encrypts an original image into a ciphertext image. After dividing the original image into blocks, the owner pseudo-randomly permutes all blocks by a permutation key. With an encryption key, the image owner further encrypts the contents of all blocks using a stream cipher algorithm, during which pixels inside each block share the same stream bytes. Once the encrypted image is uploaded onto the server, a data hider embeds additional messages into the ciphertext. The data hider divides the encrypted image into blocks and selects peak pixels from each block using an embedding key. With the peak pixels, the data hider embeds an additional message using histogram shifting inside each block. On the receiver side, a recipient extracts the hidden message using the embedding key and losslessly recovers the original image with the permutation key and the encryption key. Based on the single-level algorithm, we further construct a multi-level approach. The embedding process is iteratively used to generate the marked encrypted images. Compared with state-of-the-art works, the proposed method achieves a better embedding efficiency and an error-free recovery. **Yanping Xiang et al. [9]**, This work propose a separable reversible data hiding scheme in encrypted images based on pixel value ordering (PVO). After the original image is encrypted using homomorphism encryption by the content owner, the data hider embeds the secret data in the encrypted domain. The PVO strategy realizes hiding data in each block. Additive homomorphism guarantees the performance of PVO in the encrypted domain is close to that in the plain domain. Besides, the homomorphism encryption does not cause data expansion, and the payload can be further improved. With the watermarked encrypted image, if the receiver has only the data hiding key, he can extract the additional data. If the receiver has only the encryption key, he can obtain a decrypted image similar to the original one. If the receiver has both the data hiding key and the encryption key, he can extract the additional data without any error and recover the original image losslessly. **Ranging Wang et al. [10]** Digital image sometimes needs to be stored and processed in an encrypted format to maintain security and privacy, e.g., cloud storage and cloud computing. For content notation and/or tampering detection, the cloud servers need to embed some additional information directly in these encrypted images. As an emerging technology, reversible data hiding in the encrypted domain will be useful in cloud computing due to its ability to preserve confidentiality. In this paper, a novel separable and error-free reversible data hiding scheme in encrypted images is proposed. After analyzing the property of interpolation technology, a stream cipher is utilized to encrypt sample pixels and a specific encryption mode is designed to encrypt interpolation-error of non-sample pixels. Then, the data-hider, who does not know the original image content, may reversibly embed secret data into interpolation error using a modified version of the histogram shifting and difference expansion technique. In order to adapt to different application scenarios, data extraction can be done either in the encrypted domain or the decrypted domain. In addition, real reversibility is realized. That is, data extraction and image recovery are free of any error. Experimental results demonstrate the feasibility and efficiency of the proposed scheme. **Jiang-Yi et al.**, **[11]** In this paper, we design a bit-plane block embedding (BPBE) algorithm to hide secret messages in binary images. Meanwhile, we proceed to apply BPBE for reversible data hiding in encrypted images. It embeds the part of least-significant-bit (LSB) planes into higher most-significant-bit (MSB) planes using BPBE for reserving room before encryption so that additional data can be embedded into the

LSB planes of encrypted images. If the receiver only has the data hiding key, they can extract the additional data but don't know the exact information of the original image. If the receiver is provided with only the encryption key, they can reconstruct the original image. When both keys are acquired, the data extraction and image recovery can be correctly completed. Experimental results illustrate that the proposed scheme can achieve a higher embedding rate (ER) compared to some state-of-the-art methods and maintain an acceptable image quality. **W. H. Tsai et al. [12]** proposed an image transformation technique, which selects a target image similar to the secret image, then replaces each block of the target image with a similar block of the secret image and embeds the map between secret blocks and target blocks; it forms an Encrypted image of the secret image. A greedy search method is used to find the most similar block. Although Lai et al.'s method is reversible, it is only suitable for a target image similar to the secret image, and the visual quality of the encrypted image is not so good. **Y. L. Lee et al. [13]** improve Lai et al.'s method by transforming the secret image to a randomly selected target image without any use of the database. In Lee et al.'s method, each block of the secret image is transformed into a block of the target image with a reversible colour transformation. Then, the required information for restoring the secret image, such as parameters indexes of the block, is added into the transformed blocks, which gives an Encrypted image. Lee et al.'s method can transform a secret image into a randomly selected target image and increase the quality of the encrypted image. However, in Lee et al.'s method, the transformation is not reversible. So that secret image cannot be losslessly reconstructed. **Xianquan Zhang et al. [14]**, Reversible data hiding in encrypted images (RDHEI) is an effective technique of data security. Most state-of-the-art RDHEI methods do not yet achieve desirable payload. To address this problem, we propose a new RDHEI method with hierarchical embedding. Our contributions are twofold. (1) A novel technique of hierarchical label map generation is proposed for the bit-planes of plaintext images. The hierarchical label map is calculated by using a prediction technique, and it is compressed and embedded into the encrypted image. (2) Hierarchical embedding is designed to achieve a high embedding payload. This embedding technique hierarchically divides prediction errors into three kinds: small-magnitude, medium-magnitude, and large-magnitude, which are marked by different labels. Different from the conventional techniques, pixels with small-magnitude/large-magnitude prediction errors are both used to accommodate secret bits in the hierarchical embedding technique and, therefore, contribute a high embedding payload. Experiments on two standard datasets are discussed to validate the proposed RDHEI method. **W. Zhang et al. [15]** are the first to propose an RRBE method, taking the opposite line to all of the other state-of-the-art methods developed up to this point in time. The authors start by splitting the original image into blocks. Within each block, the correlation between the pixels is evaluated by using a fluctuation function. The blocks are further partitioned into two groups, namely, A and B. Specifically, group A is composed of textured blocks, while group B is composed of relatively homogeneous blocks. The blocks in group A are placed at the beginning of the image, and those in group B are placed afterwards. In order to release space for the secret message embedding, the LSB plane of A is embedded into pixels in group B in the clear by using histogram shifting. The resulting image is then encrypted using a stream encryption algorithm, and the number of pixels that can be marked is stored in the LSBs of the first A pixels. With this information, the secret message can be embedded simply by substituting the LSBs of the remaining pixels in A. We note that the first three LSBs of each pixel can be used. **Xin Wu et al. [16]** proposed that hiding reversible data in encrypted images (RDHEI) is essential to protect data privacy. In this paper, we propose a novel RDHEI method based on block mean difference histogram shifting. The data owner divides the cover image into non-overlapping 2×2 image blocks and computes the block mean difference. To ensure the accessibility of the block mean differences, the data owner encrypts the image block using Paillier while binding the mean differences to the encrypted image block using Paillier's self-binding property. The data hider extracts the mean difference from the encrypted image blocks in the data embedding phase. The block mean difference histogram is constructed by calculating the differences based on the additive homomorphic properties of encrypted pixels within a block to enhance the density of the histogram distribution. Subsequently, the data is embedded into the encrypted image by histogram shifting to generate the encrypted marked image. Due to the homomorphic property of Paillier, the data receiver can simultaneously extract the data and restore the image from either the encrypted marked image or the plaintext marked image without loss, which achieves separability. Experimental results show that the proposed method performs great in terms of image quality and embedding rate, and its PSNR and embedding rate outperforms similar existing methods.

III. EXPECTED OUTCOME

In the field of image processing and the context of our paper on reversible data hiding, there is a need for further investigation and development of the underlying theory, frameworks, methodologies, and applications. A significant challenge lies in achieving high-quality reconstructed images while maintaining a high level of security. Moreover, it is essential to design specific systems tailored to new data formats. Our study identifies that the existing technique based on block mean difference histogram shifting often results in low peak signal-to-noise ratio (PSNR) and high error rates. However, these challenges have been addressed in our proposed technique, which improves performance by enhancing both mean squared error (MSE) and PSNR.

IV. CONCLUSION AND FUTURE WORK

Reversible data hiding (RDH) in encrypted images has recently gained significant attention due to security maintenance requirements. These techniques are becoming increasingly popular because they allow for the reversibility of carrier media at the receiving end after the extraction of secret data. In this paper, we have studied, analyzed, and compared different types of reversible data hiding techniques for digital images, including least significant bit substitution, difference expansion, and histogram modification. The survey results indicate that each technique has its advantages and disadvantages, with the primary focus across all methods being to achieve high payloads while minimizing data degradation. However, these techniques often lead to poor image clarity, inefficient data compression, and challenges in the decoding process. To address these issues, this paper proposes a novel framework for data hiding in encrypted images through reversible image transformation. This approach involves transforming a secret image into a randomly selected target image to produce an encrypted image that maintains good visual quality. Importantly, the original secret image can be perfectly restored without any loss, ensuring content protection. The field of RDH in encrypted images is promising and is expected to have a significant impact on digital security. Future work should explore how much data can be embedded while balancing the quality of the reconstructed image, the robustness of the hidden data, and properties such as separability and commutativity.

Additionally, the effectiveness of encryption strategies has been examined in this study. Notably, even when the knowledge hider does not know the original content, key data can still be embedded into the encrypted image by modifying a section of the encrypted data. Ultimately, this research highlights the potential of RDH in encrypted images for secure data transmission and proposes an effective technique to overcome limitations such as low peak signal-to-noise ratio (PSNR) in image recovery.

REFERENCES

[1]. I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, Digital watermarking and steganography. Morgan kaufmann, 2007.

[2]. W. Bender, W. Butera, D. Gruhl, R. Hwang, F. J. Paiz, and S. Pogreb, “Applications for data hiding,” IBM systems journal, vol. 39, no. 3.4, pp. 547–568, 2000.

[3]. Huang, Fangjun, Jiwu Huang, and Yun-Qing Shi. “New framework for reversible data hiding in the encrypted domain.” IEEE Transactions on Information Forensics and Security 11, no. 12: 2777-2789, 2016.

[4]. Chandramouli, Rajarathnam, and Nasir Memon. “Analysis of LSB-based image steganography techniques.” In Proceedings 2001 international conference on image processing (Cat. No. 01CH37205), vol. 3, pp. 1019-1022. IEEE, 2001.

[5]. Varsaki, Eleni, Vassilis Fotopoulos, and A. N. Skodras. “A reversible data hiding technique embedding in the image histogram.” Hellenic Open University Journal of Informatics 1, no. 2, 2006.

[6]. Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, “Reversible data hiding,” IEEE Transactions on Circuits Systems and Video Technology, Vol. 16, No.3, 2006, pp. 354–362.

[7]. J. Huang, F. Huang, Y.-Q. Shi, New framework for reversible data hiding in the encrypted domain, IEEE Transactions on Information Forensics and Security 11,2777–2789, 2016.

[8]. Ge, Haoli, Yan Chen, Zhenxing Qian, and Jianjun Wang. “A high-capacity multi-level approach for reversible data hiding in encrypted images.” IEEE Transactions on Circuits and Systems for Video Technology 29, no. 8: 2285-2295, 2018.

[9]. Xiao, Di, Yanping Xiang, Hongying Zheng, and Yong Wang. “Separable reversible data hiding in encrypted image based on pixel value ordering and additive homomorphism.” Journal of Visual Communication and Image Representation 45: 1-10, 2017.

[10]. Xu, Dawen, and Rangding Wang. “Separable and error-free reversible data hiding in encrypted images.” Signal Processing 123: 9-21, 2016.

[11]. Lin, Jiang-Yi, Yu Chen, Chin-Chen Chang, and Yu-Chen Hu. “Reversible Data Hiding in Encrypted

Images Based on Bit-plane Block Embedding." J. Inf. Hiding Multim. Signal Process. 10, no. 2: 408-421, 2019.

[12]. I.-J. Lai and W.-H. Tsai, "Secret-fragment-visible mosaic image–a new computer art and its application to information hiding," IEEE Trans. Information Forensics and Security, vol. 6, no. 3, pp. 936–945, 2011.

[13]. Y. L. Lee and W.-H. Tsai, "A new secure image transmission technique via secret-fragment-visible mosaic images by nearly reversible colour transformations," IEEE Trans. Circuits Syst. & Video Technol., vol. 24, no. 4, pp. 695–703, 2014.

[14]. Yu, Chunqiang, Xianquan Zhang, Xinpeng Zhang, Guoxiang Li, and Zhenjun Tang. "Reversible data hiding with hierarchical embedding for encrypted images." IEEE Transactions on Circuits and Systems for Video Technology 32, no. 2: 451-466, 2021.

[15]. K. Ma, W. Zhang, X. Zhao, N. Yu, F. Li, Reversible data hiding in encrypted images by reserving room before encryption, IEEE Transactions on Information Forensics and Security 8, 553–562, 2013.

[16]. Wu, Xin. "Reversible Data Hiding for Encrypted Image Based on Block Mean Difference Histogram Shifting." In 2024 4th International Conference on Neural Networks, Information and Communication (NNICE), pp. 320-324. IEEE, 2024.