International Journal of Advanced Computer Technology
ISSN: 2319-7900 www.ijact.org Volume 12, Issue 3, May June 2023

A Survey on Reversible Image Data Hiding Using the Hierarchical Block Embedding Technique

Aman Khare, Naveen Khare
Department of Electronic Communication
Babulal Tarabai Institute of Research and Technology, Sagar (MP), India
amankhare15@gmail.com, naveenkhare90@gmail.com

Abstract: --The use of graphics for data concealment has significantly advanced the fields of secure communication and identity verification. Reversible data hiding (RDH) involves hiding data within host media, such as images, while allowing for the recovery of the original cover. Various RDH approaches have been developed, including difference expansion, interpolation techniques, prediction, and histogram modification. However, these methods were primarily applied to plain photos. This study introduces a novel reversible image transformation technique called Block Hierarchical Substitution (BHS). BHS enhances the quality of encrypted images and enables lossless restoration of the secret image with a low Peak Signal-to-Noise Ratio (PSNR). The cover image is divided into non-overlapping blocks, and the pixel values within each block are encrypted using the modulo function. This ensures that the linear prediction difference in the block remains consistent before and after encryption, enabling independent data extraction without picture decryption. In order to address the challenges associated with secure multimedia data processing, such as data encryption during transmission and storage, this survey investigates the specific issues related to reversible data hiding in encrypted images (RDHEI). Our proposed solution aims to enhance security (low Mean Squared Error) and improve the PSNR value by applying the method to encrypted images.

Keywords: Reversible Data Hiding (RDH), Block Histogram Shifting (BHS), Histogram Modification, Image Encryption, Image Decryption, Image Recovery, PSNR, MSE.

I. INTRODUCTION

Data hiding is a method that holds promise for achieving data security in the context of Responsible AI. It involves concealing information within a different form of media. This can be done by encoding confidential data into existing text or embedding audio files into digital images. With the increasing diversity and ubiquity of digital assets, the importance and applications of data hiding are expanding [1]. In today's digital age, where digital communication and multimedia data are prevalent, data hiding has become crucial. Secure communication across all mediums, such as machine learning services, is essential for responsible AI.

Additionally, protecting digital intellectual property from theft and misuse is essential for accountability in responsible AI. The traditional forms of data hiding can be categorized into watermarking, steganography, and cryptography [2]. Data hiding is both an art and a science that involves communicating secret data within multimedia carriers such as images, audio, and video files. There are two main types of data hiding: digital steganography and watermarking. Reversible data hiding refers to an approach where data is hidden within a host media, which can be a cover image. The algorithm used in reversible data hiding allows for lossless recovery of the original image after data extraction. Reversible data embedding, also known as lossless data embedding, involves embedding invisible data (payload) into a digital image in a reversible manner. A crucial requirement for reversible data embedding is to minimize quality degradation on the image after data embedding. An intriguing feature of reversible data embedding is its

reversibility, meaning that the embedded data can be removed to restore the original image. Data hiding techniques are used to embed information into covers such as audio, image, and video files. These techniques find applications in copyright protection, media notation, integrity authentication, and covert communication. Most data-hiding methods modify only the least significant part of the cover media, such as an image or video, to generate marked media, ensuring perceptual transparency. However, this embedding process typically introduces permanent distortion to the cover, making it impossible to reconstruct the original cover fully.

In certain applications like medical imagery, military, and law forensics, no degradation of the original cover is allowed. For such cases, reversible data hiding (RDH) or lossless data hiding methods are used, enabling lossless restoration of the original cover after extracting the embedded message. Fig 1.1 shows the block diagram of RDH, emphasizing the low-quality degradation as a basic requirement [3]. Reversible steganography or watermarking can restore the original carrier without any or with negligible distortion after extracting the hidden data, making reversible data hiding increasingly popular.

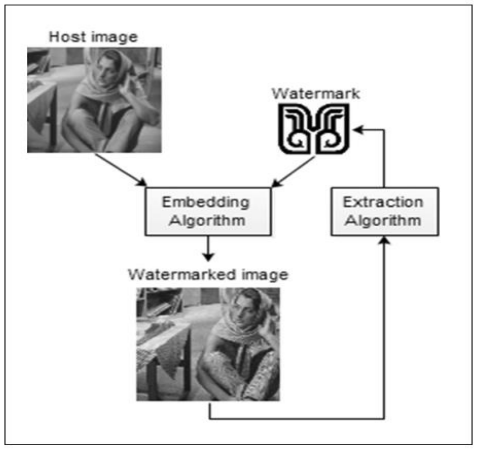

Figure 1: Reversible data hiding in the process

The key feature of reversible data embedding is its reversibility, allowing for the removal of embedded data to restore the original image. From the perspective of information hiding, reversible data embedding hide information in a digital image so that authorized parties can decode the hidden information and restore the image to its original, pristine state. An information-hiding system is characterized by four aspects: capacity, security, perceptibility, and robustness [3].

1.1 Reversible Data-Hiding Techniques

Reversible data hiding techniques have been developed over the years, offering various methods for hiding data reversibly. Several different techniques have been proposed, as outlined below.

A. Circular Visual Cryptography: Introduced in 2005, circular visual cryptography involves hiding multiple confidential data sets into circular images. The scheme displays these images in the circular images' inner and outer regions. However, the central part of the circular shadow image can cause low resolution on the images in the inner portion [4]. It enables data encryption into two-ringed shadow images, allowing the simultaneous hiding of two confidential data sets.

B. LSB Modification-Based Technique: One of the earliest methods for reversible data hiding is LSB (Least Significant Bit) modification. This well-known technique involves replacing the LSB of each signal sample with a secret data bit. These bits are read in the same scanning order during extraction to reconstruct the secret data [4].

C. Difference Expansion (DE) Based Technique: Tian proposed the Difference Expansion (DE) based technique for Reversible Data Hiding [2]. This technique explores redundancy in the image content to discover extra storage space. DE is used to embed a payload into digital images reversibly. The DE method offers high payload capacity, visual quality, and low computational complexity [5].

D. Histogram Shift-Based Technique: Histogram-shifting-based reversible data hiding schemes involve embedding data by shifting the histogram in a fixed direction. The peak and the zero points in these schemes are two crucial

points. The peak point corresponds to the grayscale value with the maximum number of pixels in the image histogram, while the zero point represents the point where the histogram value is zero. Selecting the minimum number of pixels as the zero point helps increase the embedded capacity. In histogram-shifting-based algorithms, the pixels between the peak and zero pairs are modified during the embedding process. The pixel in the peak point carries a bit of the secret message, while the other pixels are modified without embedding any secret data. The hiding capacity of histogram shifting-based data hiding is determined by the number of pixels in the peak points, with a higher number of peak pixels resulting in a higher hiding capacity. More peak and zero-point pairs can increase the hiding capacity. However, finding additional pairs can be challenging if the zero points are not easily identified [6].

These techniques demonstrate the advancements in reversible data hiding, offering different approaches for embedding and extracting hidden data while maintaining the original data integrity.

II. RELATED WORK

Reversible data hiding has been an active area of research in recent years, and several important techniques have been proposed. This section overviews existing reversible data hiding in encrypted images (RDH-EI) techniques, categorized based on the underlying image processing mechanisms involved. In K. Ma et al. [7], the authors introduce an RRBE (Reversible Rich Bit Embedding) method, which takes a different approach than other state-of-the-art methods. The original image is divided into blocks, and a fluctuation function is used to evaluate the correlation between pixels within each block. The blocks are further categorized into two groups: group A, consisting of textured blocks, and Group B, consisting of relatively homogeneous blocks. Group A's LSB (Least Significant Bit) plane is embedded into group B's pixels using histogram shifting to create space for secret message embedding. 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. The secret message can be embedded by substituting the LSBs of the remaining pixels in group A. It is worth noting that the first three LSBs of each pixel can be utilized. In F. Huang et al. [8], the authors identify that existing algorithms for embedding secret data in the clear domain cannot be directly applied in the encrypted domain due to security concerns. To address this, they propose a new encryption strategy that enables conventional data-hiding algorithms designed for the clear domain to be applied directly to encrypted images. The original image is divided into non-overlapping blocks, and all pixels within each block are encrypted using the XOR operation with a pseudo-randomly generated byte. The encrypted blocks are then permuted in a pseudo-random manner. Notably, the pixels within the same block are not scrambled; only the order of the blocks is changed. This encryption method preserves the statistical properties of the original image, including the histogram of pixel differences or prediction errors.

Consequently, conventional data-hiding algorithms designed for the clear domain can be applied to encrypted images, although the embedding capacity is limited by the handling of under/overflow problems. In Ge et al. [9], a novel method of reversible data hiding in encrypted images (RDH-EI) is proposed. The authors present a single-level embedding approach involving an image owner, a data hider, and a recipient. The image owner encrypts the original image into a ciphertext image, dividing it into blocks and applying a permutation key to permute all blocks pseudo-randomly. Using an encryption key, the owner further encrypts the contents of all blocks using a stream cypher algorithm, ensuring that pixels inside each block share the same stream bytes. Once the encrypted image is uploaded onto the server, the data hider embeds additional messages into the ciphertext. The data hider divides the encrypted image into blocks, selects peak pixels from each block using an embedding key, and performs histogram shifting to

embed the additional message within each block. On the recipient side, the hidden message is extracted using the embedding key, and the original image is losslessly recovered using the permutation key and the encryption key.

A multi-level approach is proposed, where the embedding process is iteratively used to generate marked encrypted images. The proposed method achieves better embedding efficiency and error-free recovery than existing works. Xiao et al. [10] proposed a separable reversible data hiding scheme in encrypted images based on pixel value ordering (PVO). The original image is encrypted using homomorphism encryption by the content owner, and the data hider embeds the secret data in the encrypted domain. The PVO strategy enables data hiding in each block, and additive homomorphism ensures that the performance of PVO in the encrypted domain is comparable to that in the plain domain. The homomorphism encryption does not cause data expansion, allowing for improved payload. The watermarked encrypted image allows for the extraction of additional data if the receiver has the data hiding key. A decrypted image similar to the original can be obtained if the receiver has the encryption key. If the data hiding and encryption keys are available, the additional data can be extracted without errors, and the original image can be recovered losslessly. Xu et al. [11] proposed a novel separable and error-free reversible data hiding scheme in encrypted images for applications such as cloud storage and computing. The scheme utilizes interpolation technology and employs a stream cypher to encrypt sample pixels and a specific encryption mode to encrypt the interpolation error of non-sample pixels. Without knowledge of the original image content, the data hider can reversibly embed secret data into the interpolation error using a modified version of histogram shifting and difference expansion techniques. Data extraction can be performed in either the encrypted or decrypted domain, and real reversibility is achieved without any errors.

Experimental results demonstrate the feasibility and efficiency of the proposed scheme. In Lin et al. [12], a bit-plane block embedding (BPBE) algorithm is designed for hiding secret messages in binary images, which is further applied for reversible data hiding in encrypted images. The algorithm embeds the least-significant-bit (LSB) planes into higher most-significant-bit (MSB) planes using BPBE before encryption, allowing additional data to be embedded into the LSB planes of encrypted images. Depending on the available keys, the receiver can extract additional data, reconstruct the original image, or perform both data extraction and image recovery. The proposed scheme achieves a higher embedding rate than some state-of-the-art methods while maintaining acceptable image quality. In I. J. Lai et al. [13], an image transformation technique is proposed where a target image similar to the secret image is selected, and each block of the target image is replaced by a similar block of the secret image while embedding the map between secret blocks and target blocks. Although reversible, this method is only suitable for target images similar to the secret image and may compromise the encrypted image's visual quality. In Y. L. Lee et al. [14], an improvement to Lai et al.'s method is introduced by transforming the secret image to a randomly selected target image without using a database. The secret image's blocks are transformed into blocks of the target image using reversible colour transformation, and the necessary information for restoring the secret image, such as parameters and block indexes, is added to the transformed blocks, creating the encrypted image. This method enhances the quality of the encrypted image, but the transformation itself is not reversible, preventing lossless reconstruction of the secret image. Yu et al. [15] proposed a new reversible data hiding in encrypted images (RDHEI) method with hierarchical embedding. A hierarchical label map generation technique is introduced for the bit-planes of the plaintext image using prediction techniques. The hierarchical label map is compressed and embedded into the encrypted image. The hierarchical embedding technique divides prediction errors into small-magnitude, medium-magnitude, and large-magnitude categories, marked by different labels. Unlike conventional techniques, pixels with

both small-magnitude and large-magnitude prediction errors are used to accommodate secret bits, resulting in a higher embedding payload. Experimental results on standard datasets validate the proposed RDHEI method.

III. EXPECTED OUTCOME

In the field of reversible data concealment, the expected outcome is to advance the research and development in terms of theory, frameworks, techniques, and applications. The goal is to achieve the optimal trade-off between payload capacity, reconstructed image quality, and security levels. This requires thorough exploration and innovation in various areas. Specifically, there is a need for developing specialized approaches for new formats and containers, with a focus on extensions for JPEG family images that exhibit low peak signal-to-noise ratio (PSNR) and high error rates based on block-based hiding schemes (BHS). Overcoming the challenges associated with low PSNR and high error rates is crucial in achieving satisfactory performance. The proposed strategies aim to enhance the overall performance of reversible data concealment techniques by reducing errors, increasing PSNR, and improving the quality of the reconstructed images. The expected outcome is to contribute to developing more efficient and effective methods for reversible data concealment, addressing the limitations and challenges faced in the field.

CONCLUSION

This survey has provided an overview of the development and advancements in reversible data hiding in encrypted images (RDHEI) techniques. The motivation and applications of RDHEI approaches were discussed, highlighting the growing importance of reversible techniques in maintaining data privacy and security. Traditional methods of reversible data hiding in encrypted images had several limitations, including the inability to protect image content, low hiding capacity, complex computations, poor image clarity, inefficient data compression, and decoding issues. In order to address these limitations, a novel framework called Data Hiding in Encrypted Image by Reversible Image Transformation (RIT) was proposed. This framework transforms a secret image into a randomly selected target image, resulting in an encrypted image with good visual quality. The secret image can be accurately restored without any loss, ensuring the security of the image content. The field of RDHEI, particularly in the context of encrypted images (RDH-EI), holds great potential and can significantly impact digital security. However, several challenges must be addressed, such as determining the optimal trade-off between data hiding capacity and the reconstructed image's quality, ensuring the hidden data's robustness, and considering factors like separability and commutability. The proposed methods in this survey aim to enhance security by achieving low mean square error (MSE) and improving the peak signal-to-noise ratio (PSNR) value in encrypted images. By incorporating these techniques, the overall security and quality of the reconstructed images can be improved. In conclusion, RDHEI techniques, especially in encrypted images, offer promising data privacy and security solutions. Ongoing research and development in this field will continue to shape the future of digital security and contribute to advancements in reversible data-hiding techniques.

References

[1]. Li, X., Li, B., Yang, B., and Zeng, T. (2013). A general framework for histogram-shifting-based reversible data hiding. IEEE Transactions on Image Processing, 22(6), 2181-2191.

[2]. Li, X., Zhang, W., Gui, X., and Yang, B. (2015). Efficient reversible data hiding based on multiple histograms modification. IEEE Transactions on Information Forensics and Security, 10(9), 2016-2027.

[3]. Huang, F., Huang, J., and Shi, Y. Q. (2016). The new framework for reversible data hiding in the encrypted domain. IEEE Transactions on Information Forensics and Security, 11(12), 2777-2789.

[4]. Chandramouli, R., and Memon, N. (2001). Analysis of LSB-based image steganography techniques. In Proceedings 2001 International Conference on Image Processing (Cat. No. 01CH37205) (Vol. 3, pp. 1019-1022). IEEE.

[5]. Hu, Y., Lee, H. K., Chen, K., and Li, J. (2008). Difference expansion-based reversible data hiding using two embedding directions. IEEE Transactions on Multimedia, 10(8), 1500-1512.

[6]. Tai, W. L., Yeh, C. M., and Chang, C. C. (2009). Reversible data hiding based on histogram modification of pixel differences. IEEE Transactions on Circuits and Systems for Video Technology, 19(6), 906-910.

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

[8]. Huang, F., Huang, J., and Shi, Y. Q. (2016). A new framework for reversible data hiding in the encrypted domain. IEEE Transactions on Information Forensics and Security, 11, 2777-2789.

[9]. Ge, H., Chen, Y., Qian, Z., and Wang, J. (2018). A high-capacity multi-level approach for reversible data hiding in encrypted images. IEEE Transactions on Circuits and Systems for Video Technology, 29(8), 2285-2295.

[10]. Xiao, D., Xiang, Y., Zheng, H., and Wang, Y. (2017). Separable reversible data hiding in encrypted images based on pixel value ordering and additive homomorphism. Journal of Visual Communication and Image Representation, 45, 1-10.

[11]. Xu, D., and Wang, R. (2016). Separable and error-free reversible data hiding in encrypted images. Signal Processing, 123, 9-21.

[12]. Lin, J. Y., Chen, Y., Chang, C. C., and Hu, Y. C. (2019). Reversible Data Hiding in Encrypted Images Based on Bit-plane Block Embedding. J. Inf. Hiding Multim. Signal Process., 10(2), 408-421.

[13]. Lai, I. J., and Tsai, W. H. (2011). Secret-fragment-visible mosaic image–a new computer art and application for information hiding. IEEE Transactions on Information Forensics and Security, 6(3), 936-945.

[14]. Lee, Y. L., and Tsai, W. H. (2014). A new secure image transmission technique via secret-fragment-visible mosaic images by nearly reversible colour transformations. IEEE Transactions on Circuits Systems and Video Technol., 24(4), 695-703.

[15]. Yu, C., Zhang, X., Zhang, X., Li, G., and Tang, Z. (2021). Reversible data hiding with hierarchical embedding for encrypted images. IEEE Transactions on Circuits and Systems for Video Technology, 32(2), 451-466.