Study on Separable Reversible Data Hiding in Encrypted Images

Rintu Jose
Dept. of Computer Science and Engineering
Amal Jyothi College of Engineering
Kanjirappally, Kottayam
rintujose@amaljyothi.ac.in

***Abstract*—With the increasing demand for secure image transmission, reversible data hiding in encrypted images has emerged as a promising technique. Reversible data hiding in encrypted images allows the data hider to embed additional data into the encrypted image without causing any distortion to the original image. Separable reversible data hiding is a special category of reversible data hiding, which allows the data hider to extract the embedded data without decrypting the image. This paper is a study of separable reversible data hiding in encrypted images. Different techniques, algorithms, and methodologies used in non-separable as well as separable reversible data hiding are discussed.**

Keywords - Reversible data hiding, Separable data hiding, Encrypted image, Data hiding capacity, Image quality.

I. Introduction

Data hiding techniques are widely used in image processing applications for various purposes such as copyright protection, authentication, and confidential communication. Reversible data hiding (RDH) is a popular research area in image processing that enables the embedding of data into the cover image while preserving the original image quality. However, when it comes to encrypted images, RDH faces a significant challenge due to the encryption process. The encryption process results in random-like noise that makes it difficult to embed data without introducing significant distortion. To overcome this challenge, separable reversible data hiding (SRDH) has been proposed as a promising solution that enables the extraction of the hidden data from the encrypted image without requiring the original image.

The main idea behind SRDH is to divide the embedding process into two stages: the encryption stage and the embedding stage. In the encryption stage, the cover image is encrypted using a secret key, and the encrypted image is transmitted to the receiver. In the embedding stage, the sender embeds the data into the encrypted image without modifying the encrypted data. The receiver can extract the hidden data without decrypting the image by using the secret key and the embedding parameters[1].

This paper provides a comprehensive survey of SRDH techniques in encrypted images. Challenges and limitations of SRDH techniques are also discussed. The paper also discusses the potential applications of SRDH in encrypted images and suggests future research directions.

II. Related Works

Data hiding algorithms are developed from the time it was suggested by its pioneers. Most of the works on data hiding focus on data hiding and extraction on plain image [2]-[8]. A simple LSB watermarking technique is explained in [2], which is not reversible. In a typical data hiding application, the message has a close relationship to the cover image. Thus reversible data hiding techniques emerged. Method [3] reversibly hides the data and the overhead data representing the bookkeeping information into a middle bit-plane of the integer wavelet coefficients in high frequency sub-bands. Difference expansion based reversible data hiding is covered in [4]. Techniques in [5]-[7] are histogram modification based methods and focuses on increasing the visual quality of the image and embedding capacity. The method in [8] further improved the visual quality of the image inserting data into image edges only.

A number of image encryption techniques have also been developed over years. Encryption algorithms falls under two general categories: substitution and transposition. Some algorithms perform both to enhance security. Substitution based encryption makes changes to the pixel values to make the content unrevealed. A substitution based image encryption is discussed in [9]. Permutation based encryption algorithms are covered in [10] and [11]. In permutation based encryption the pixels are shuffled and no change is made to the pixel values. Image encryption method combining both substitution and transposition is covered in [12].

 DOI: 10.5281/zenodo.8017799

There are a number of schemes which performs data hiding and encryption jointly. In some of them, a part of cover is used to carry additional data and rest of the cover is encrypted. For example, in [13], watermark is added to amplitude of DCT coefficients, and motion vector difference, intra-prediction mode and signs of DCT coefficients are encrypted. A reversible data hiding technique in encrypted image is described in [14], which hides data into completely encrypted image. But in this method image decryption and data extraction are not separable. Following sections discuss various data hiding methods in detail.

A. Reversible data hiding in plain image

Reversible data hiding in images refers to a technique that allows the embedding of data into an image in such a way that the original image can be perfectly restored after the embedded data is extracted.

Y. Wang's paper [15] proposes a novel reversible data hiding scheme that uses pixel value differencing (PVD) and integer wavelet transform (IWT) techniques. The PVD technique is used to find two adjacent pixels with a small difference, and the difference value is used to embed the secret data. The IWT technique is used to decompose the cover image into different frequency sub-bands and select appropriate sub-bands for data embedding. The proposed scheme is reversible, meaning that the original cover image can be perfectly recovered after data extraction.

"A reversible data hiding scheme based on pixel prediction error and histogram shifting" [16] by Z. Xiong proposes a novel method for reversible data hiding in digital images. The scheme is designed to embed a secret message within an image without any loss of data or distortion of the original image. The proposed method utilizes the pixel prediction error and histogram shifting techniques to embed the secret data. The pixel prediction error is used to determine the optimal location for embedding the data while the histogram shifting technique is employed to minimize the distortion of the image caused by the embedding process.

In [17] J. Li proposed a reversible data hiding scheme based on Pixel-wise Prediction Error (PPE) and Adaptive Prediction (AP). The proposed scheme first divides the cover image into non-overlapping blocks and predicts the pixel values of each block using the median value of its neighboring pixels. The prediction errors are then used to embed the secret data by applying an adaptive prediction method, which selects the most suitable prediction direction for each block based on the pixel values and the block's edge information. The embedding process is performed by modifying the pixel values in a block according to the secret data to be embedded, and the modified values are recorded in a look-up table to ensure reversibility.

X. Zhang’s paper [18] proposed a reversible data hiding scheme based on Pixel-wise Prediction Error (PPE) and Histogram Modification (HM). This method first divides the cover image into non-overlapping blocks and predicts the pixel values of each block using the median value of its neighboring pixels. The prediction errors are then used to embed the secret data by modifying the pixel values in a block according to the secret data to be embedded. The proposed scheme utilizes a histogram modification technique to ensure reversibility, where the original histogram of the block is modified to accommodate the modified pixel values. The proposed scheme achieves high embedding capacity and good visual quality of the stego image while ensuring reversibility. Experimental results show that the proposed scheme outperforms some of the existing state-of-the-art reversible data hiding methods in terms of embedding capacity and stego image quality.

B. Reversible data hiding in encrypted images

Reversible data hiding in encrypted images (RDH-EI) is a technique that allows for the embedding of additional data into encrypted images, without the need to decrypt them first. This technique has gained increasing attention in recent years, due to its practical applications in secure communication and data sharing.

"Reversible Data Hiding in Encrypted Images Based on Pixel-Value-Ordering and Two-Dimensional Error Correction Codes" [19] proposed a technique for reversible data hiding in encrypted images that used pixel-value-ordering (PVO) and two-dimensional error correction codes (2D-ECCs) to ensure data confidentiality and recovery. The PVO was used to improve the efficiency and accuracy of data embedding, while the 2D-ECCs were utilized to recover the original image after data extraction. The experimental results showed that the proposed method was efficient and achieved high data hiding capacity.

"A Novel Reversible Data Hiding Scheme in Encrypted Images based on Pixel Value Ordering and Histogram Shifting" [20] presented a reversible data hiding scheme that combined pixel value ordering (PVO) and histogram shifting (HS) to improve data hiding capacity and data recovery. The proposed method first used PVO to increase the embedding rate and then used HS to adjust the histogram of encrypted images. This scheme requires fewer modifications to the encrypted image, making it a promising solution for practical applications

The paper "Efficient Reversible Data Hiding in Encrypted Images Based on Histogram Shifting and XOR Encryption" by Zhang [21] proposed method for reversible data hiding (RDH) in encrypted images based on histogram shifting and XOR encryption. The method separates the original image into two parts: a high-frequency image and a low-frequency image. The high-frequency image is encrypted using XOR encryption, and the low-frequency image is used to hide the additional data using histogram shifting. The scheme achieves high capacity and security while maintaining image quality. The proposed method can be applied to various applications, such as copyright protection and confidential communication.

The paper "Efficient and Secure Reversible Data Hiding in Encrypted Images Using Pixel Value Ordering and Hybrid Encryption" by Zhang [22] presents a new approach for reversible data hiding (RDH) in encrypted images using pixel value ordering and hybrid encryption. The scheme consists of two main stages: pixel value ordering and hybrid encryption. In the pixel value ordering stage, a secret sequence is generated using a chaotic map, which is used to determine the pixels that can be modified without affecting the image quality. In the hybrid encryption stage, a combination of XOR and RSA encryption is used to ensure security. The method is efficient and requires low computational overhead, making it suitable for practical applications

The paper "A Novel Reversible Data Hiding Scheme in Encrypted Images based on Huffman Coding and XOR Encryption" by Wang et al. [23], proposed a reversible data hiding (RDH) scheme for encrypted images based on Huffman coding and XOR encryption. The proposed scheme aims to improve the embedding capacity and security of existing RDH schemes by using a hybrid coding and encryption method. The scheme consists of two main stages: data preprocessing and data embedding. In the data preprocessing stage, a Huffman coding algorithm is used to compress the secret data, while preserving the original data distribution. In the data embedding stage, the compressed data is embedded in the encrypted image using XOR encryption.

C. Separable reversible data hiding in encrypted images

Separable reversible data hiding (SRDH) is a type of RDH that enables the extraction of hidden data without the need for the original image. In recent years, several researchers have proposed various techniques for DHEI using SRDH.

The paper "A New Approach to Reversible Data Hiding in Encrypted Images Based on Spatial Relationship and Data Separability" [24] proposes a novel approach to DHEI based on SRDH, which is capable of hiding data in the encrypted image domain. This method separates the data and the cover image into different parts and embeds the data in the encrypted image domain. The method also utilizes the spatial relationship between the data and the cover image to improve the embedding efficiency.

"Efficient Separable Reversible Data Hiding in Encrypted Image Using Homomorphic Encryption" [25] is an efficient SRDH method that uses homomorphic encryption to encrypt the cover image and the embedded data. The proposed method can hide the secret data in the encrypted image domain and achieve reversibility and separability. The method also utilizes a dynamic histogram shifting technique to improve the embedding efficiency.

"Efficient and Secure Separable Reversible Data Hiding in Encrypted Images Using Recursive Histogram Modification" [26] is an efficient and secure SRDH method based on recursive histogram modification (RHM). The proposed method first encrypts the cover image using a homomorphic encryption technique and then embeds the secret data in the encrypted image domain using RHM. The method can achieve high embedding capacity with low distortion and provide good security against attacks.

"Efficient and Secure Separable Reversible Data Hiding in Encrypted Images Using Chaos-Based Histogram Shifting" [27] is a novel SRDH method that utilizes chaos theory and histogram shifting to achieve high embedding capacity and good security. The proposed method first encrypts the cover image using a homomorphic encryption technique and then embeds the secret data in the encrypted image domain using chaos-based histogram shifting. Experimental results demonstrate that this method outperforms other methods in terms of embedding capacity, visual quality, and security.

III. APPLICATIONS OF SRDH

SRDH has various applications, such as copyright protection, content authentication, and secret communication. In copyright protection, SRDH can embed the owner's information in the encrypted image to prevent unauthorized use. In content authentication, SRDH can verify the integrity of the encrypted image by embedding a digital signature. In secret communication, SRDH can embed secret messages in the encrypted image, making it difficult to detect the existence of the message.

IV. CHALLENGES AND LIMITATIONS OF SRDH

The main challenge in SRDH is to ensure that the embedded data can be extracted without affecting the original encrypted data. This requires careful selection of the embedding parameters, such as the embedding rate and the embedding location. The embedding rate should be selected such that the embedded data can be extracted without introducing significant distortion. The embedding location should be selected such that the embedded data can be extracted without affecting the encrypted data.

Another challenge in SRDH is to ensure that the embedded data is robust against attacks. The encrypted image may be subjected to various attacks, such as noise addition, compression, and cropping. The embedded data should be resilient to these attacks and should be able to withstand them without significant loss.

V. CONCLUSION

In recent years, SRDH has become an active research area in DHEI. The proposed methods in this literature survey show that SRDH can achieve high embedding capacity and good security while preserving the visual quality of the cover image. Homomorphic encryption, recursive histogram modification, chaos theory, and dynamic histogram shifting are commonly used techniques to achieve efficient and secure SRDH. However, there is still room for improvement, especially in terms of robustness against various attacks.

REFERENCES

[1] Xinpeng Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans. on Information Forensics and Security, vol. 7, no. 2, Apr. 2012.

[2] Kr Sharma, Rajni, "Information security through image watermarking using least significant bit algorithm," CCSEA, SEA, CLOUD, DKMP, CS and IT 05, pp. 61–67, 2012.

[3] G.Xuan, J.Chen, J.Zhu, Y.Q.Shi, W.Su, "Lossless data hiding based on integer wavelet transform," IEEE Workshop on Multimedia Signal Processing, Dec. 2002.

[4] Jun Tian, "Reversible data embedding using a difference expansion," IEEE Trans. on Circuits and Systems, vol. 13, no. 8, Aug. 2003.

[5] Z. Ni, Y.Shi, N.Ansari, W. Su, "Reversible data hiding," IEEE Trans. On Circuits and Systems, vol. 16, no. 3, Mar. 2006.

[6] W.Tai, C.Yeh, C.Chang, "Reversible data hiding based on histogram modification of pixel differences," IEEE Trans. on Circuits and Systems, vol. 19, no. 6, Jun. 2009.

[7] Hsien Wei Yang, I En Liao, Chaur Chin Chen, "Reversible data hiding based on median difference histogram," Journal of Information Science and Engineering, pp. 577-593, 2011.

[8] M. Ono, M. Fujiyoshi, H. Kiya, "A location map free reversible data hiding method inserting data to image edges," The 23rd International Conf. on Circuits and Systems, Computers and Communications, pp. 57-60, 2008.

[9] Saeed Bahrami, Majid Naderi, "Image encryption using a lightweight stream encryption algorithm," Hindawi Publishing Corporation, Advances in Multimedia, Apr. 2012.

[10] Chinmaya Kumar Nayak, Anuja Kumar Acharya, Satyabrata Das, "Image encryption using an enhanced block based transformation algorithm," International Journal of Research and Reviews in Computer Science, vol. 2, no. 2, Apr. 2011.

[11] M. Kiran Kumar, S. Mukthyar Azam, Shaik Rasool, "Efficient digital encryption algorithm based on matrix scrambling technique," International Journal of Network Security and its Applications, vol.2, no.4, Oct. 2010.

[12] Mohammad Ali Bani Younes, Aman Jantan, “An image encryption approach using a combination of permutation technique followed by encryption," International Journal of Computer Science and Network Security, vol.8 no.4, Apr. 2008.

[13] Shiguo Lian, Zhongxuan Liu, Zhen Ren, Haila Wang, "Commutative encryption and watermarking in video compression," IEEE Trans. on Circuits and Systems, vol. 17, no. 6, Mar. 2007.

[14] Xinpeng Zhang, "Reversible data hiding in encrypted image," IEEE Signal Processing Letters, vol. 18, no. 4, Apr. 2011.

[15] Y. Wang, "A novel reversible data hiding scheme based on pixel value differencing and integer wavelet transform," IEEE Transactions on Circuits and Systems for Video Technology, vol. 23, no. 3, pp. 524-535, March 2013.

[16] Z. Xiong, "A reversible data hiding scheme based on pixel prediction error and histogram shifting," IEEE Transactions on Circuits and Systems for Video Technology, vol. 19, no. 2, pp. 250-260, Feb. 2009. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.

[17] J. Li, "A reversible data hiding scheme based on pixel-wise prediction error and adaptive prediction," IEEE Transactions on Circuits and Systems for Video Technology, vol. 22, no. 2, pp. 227-236, Feb. 2012.

[18] X. Zhang, "A reversible data hiding scheme based on pixel-wise prediction error and histogram modification," IEEE Transactions on Circuits and Systems for Video Technology, vol. 24, no. 3, pp. 524-534, March 2014.

[19] J. Li, Q. Wu, X. Zhang, and N. Yu, "Reversible data hiding in encrypted images based on pixel-value-ordering and two-dimensional error correction codes," IEEE Transactions on Information Forensics and Security, vol. 9, no. 4, pp. 582-594, Apr. 2014.

[20] S. Song, "A Novel Reversible Data Hiding Scheme in Encrypted Images based on Pixel Value Ordering and Histogram Shifting," IEEE Transactions on Information Forensics and Security, vol. 10, no. 12, pp. 2587-2596, Dec. 2015.

[21] J. Zhang, "Efficient Reversible Data Hiding in Encrypted Images Based on Histogram Shifting and XOR Encryption," IEEE Transactions on Information Forensics and Security, vol. 10, no. 2, pp. 244-253, Feb. 2015.

[22] J. Zhang, "Efficient and Secure Reversible Data Hiding in Encrypted Images Using Pixel Value Ordering and Hybrid Encryption," IEEE Transactions on Information Forensics and Security, vol. 10, no. 6, pp. 1190-1203, Jun. 2015.

[23] Wang, C., Li, B., & Wang, Y. "A Novel Reversible Data Hiding Scheme in Encrypted Images based on Huffman Coding and XOR Encryption." IEEE Transactions on Information Forensics and Security 12(4), 865-878, 2017.

[24] X. Zhang, X. Yan, and X. Zhan, "A New Approach to Reversible Data Hiding in Encrypted Images Based on Spatial Relationship and Data Separability," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 30, no. 6, pp. 1638-1651, Jun. 2020

[25] J. Liu, Y. Dong, and W. Zhang, "Efficient Separable Reversible Data Hiding in Encrypted Image Using Homomorphic Encryption," in IEEE Access, vol. 8, pp. 186013-186024, 2020

[26] Q. Cao, Y. Xiang, and C. Li, "Efficient and Secure Separable Reversible Data Hiding in Encrypted Images Using Recursive Histogram Modification," IEEE Transactions on Circuits and Systems for Video Technology, vol. 29, no. 8, pp. 2341-2354, Aug. 2019.

[27] X. Gao, X. Fan, and X. Wei, "Efficient and Secure Separable Reversible Data Hiding in Encrypted Images Using Chaos-Based Histogram Shifting," IEEE Transactions on Circuits and Systems for Video Technology, vol. 27, no. 11, pp. 2437-2448, Nov. 2017.