Reversible Data Hiding in Encrypted Images: A Critical Review

Akanksha Bansal[1] Prof. Dr. Manoj Ramaiya[2]
[1,2]Shri Ram College of Engineering and Management, Banmore, India

Abstract— The global digital revolution has made this earth more comfortable and smart. This has inspired many engineers to design smart applications in every sphere of modern life. The dark side of the coin is the security of the data. This has motivated technical research in the direction of efficient and hi fi tempered proof data hiding. The most popular technique is reversible data hiding (RDH). The other common name for this method is lossless data hiding. The world technical community is busy publishing the research papers on RDH. There is an ample of scope for developing software tools, which can support image steganography, combined with text encryption. The data is hidden behind some digital cover media. This media can be an image, video, audio or text. The hidden data is transmitted over some channel and it may contain some secret key. This key ensures the authenticated delivery of the payload. The receiver gets the original data after the separation of the same from the actual media. The RDH method helps to recover the original hidden message from the digital data. This method is lossless and this quality is suitable for real life applications like medical science, defence, big data storage etc. The cloud storage can be useful for secured data storage like drop box and google drive. The RDH is used in encrypted images in these applications. The variations in the method can be with and without pre-processing the encrypted images (RDHEI). In this paper, the most common methods of hiding the encrypted images have been reviewed. There are few methods, which allow large data embedding and very efficient while other are not so efficient. The few algorithms discussed are able to provide the lossless data hiding while few have partial distortions. The methods covered are having their own merits and demerits. The better combination is reversible data hiding and lossless recovery of the original carrier and data in encrypted image. The embedding pixels are randomly chosen. The secret key makes it more secure. The random selection of the embedding pixels makes it very difficult to intrude into the communication channel. The secret key at the receiving end opens the lock and the hidden data can easily be recovered without distorting the carrier data. On the basis of the analysis of the entire research papers the unique reversible data hiding method using histogram shifting –imitated approach. The image is broken into finite number of segments and one segment is chosen to hide the data. Each segment is represented in the form of histogram. The peak points are chosen on the basis of intensity of the pixel value. The secret data is hidden into the cover image by modifying the peak point pixel value in the same segment. This embedding method yields high embedding capacity and robust data security.

Key words: Reversible Data Hiding, Lossless Data Hiding, Payload, Histogram, Image Encryption, PSNR, Robust, Embedding Data Hiding Capacity

I. INTRODUCTION

Reversible Data hiding is the method of hiding data inside a cover file so that both the data and the cover file could be recovered lossless at the receiver. The transmitter side of such systems involves a cover image, additional data, encryption key and data hiding key. The original image will be encrypted, data will be hidden and then image will be transmitted. The receiver thus needs to decrypt the image and extract the data.

For maintaining the security of images, two different approaches can be employed that is one encrypting the image using the encryption keys and second approach can be without using the keys, where the image is divided into different shares to maintain the image secrecy. This allows the visual information to be encrypted in such a way that their decryption can be performed by human visual system. Unfortunately heavy computation cost and key management limit the employment of the first approach and the poor quality of the recovered image from the random shares limit the application of the second approach. More and more attention is paid to reversible data hiding in encrypted images. Data hiding plays an important role in information security. It aims at embedding imperceptible confidential information data in cover media such as static images, audio, videos, 3D meshes and so on. As long as images are concerned data hiding which cannot perceive between stegno image and cover image by human, the cover image still can get harmed in processing. Many different techniques have been proposed to get back the cover image lossless. The reversibility means not only embedding data but also original image can be precisely recovered in the extracting stage. Most hiding techniques perform data embedding by altering the contents of a host media. As a result the host image cannot be completely recovered after the bit extraction. These types of data hiding techniques are thus irreversible. However in a number of domains such as military, legal and medical imaging although some embedding distortion is admissible, permanent loss of signal fidelity is undesirable. This highlights the need for Reversible (Lossless) data embedding techniques. Thus the proposed approach gives a novel technique for reversible data hiding using visual cryptography. With the scheme involving use of secret keys have limitations as regards key management. In addition in some cases the available keys for encryption are limited (restricted key space), also high computation involved in encryption. All these factors comprise the problem domain for using traditional encryption techniques in reversible data hiding. In opposite to this approach the method using visual cryptography techniques involve no use of keys for encryption keeping computational cost for encryption /decryption low.

Today's a large demand of internet application requires data to be transmitted in a secure manner. Data transmission through public networks are not secured because of interception and improper manipulation of eavesdropper. Security is an important aspect for data transmission. The data hiding and encryption are the two prominent methods of data security. There are mainly two types of data hiding. If the data hiding is said to be "lossless", then the display of the cover signal containing embedded data is same as that of

original cover. If the original plain text image can perfectly recovered from the image containing embed data, then such data hiding is said to be "reversible". Combination of data hiding and encryption methods are applicable in various fields. For example, the medical images have been protected with patient's information. With this method the information about the patient are embed into medical image. So these information are protected. There are many methods for data security. Some uses lossless data hiding scheme and some other methods uses reversible data hiding scheme. Some methods combines both data hiding and encryption methods. Sometimes distortions are causes to the original image.
Different RDH Techniques used are:

A. Reversible Data Hiding with Optimal Value Transfer

In reversible data hiding techniques, the values of host data are modified based on particular rules and the original host content is perfectly restored after extraction of the hidden data on receiver side. Here the optimal rule of value modification under a payload-distortion criterion is found by using an iterative procedure, and a practical reversible data hiding scheme is proposed. The secret data, as well as the auxiliary information used for content recovery, are carried by the differences between the original pixel-values and the corresponding values estimated from the neighbors. The estimation errors are modified according to the optimal value transfer rule. The host image is divided into a number of pixel subsets and the auxiliary information of a subset is embedded into the estimation errors in the next subset. A receiver can successfully extract the embedded secret data and recover the original content in the subsets with an inverse order. Using this method a good reversible data hiding performance is achieved.

Reversible data hiding in encrypted images by reserving room before encryption most reversible data hiding techniques embed data by vacating room from the encrypted images. But this cause errors on data extraction. In this method room is reserved before encryption using a traditional RDH algorithm. This method has four stages: generation of encrypted image, data hiding in encrypted image, data extraction and image recovery. Encrypted image generation includes image partition, self-reversible embedding followed by image encryption. In image partition original image is divided into two parts A and B. Least significant bits of a are embedded reversibly into B with a standard RDH algorithm so that least significant bits of A can be used for accommodating the data. Encrypted image is rearranged to generate its final version. After the encrypted image is obtained data hider can embed data into it. Data can be extracted from encrypted or decrypted images. In data extraction from encrypted image both embedding and extraction of data are done in encrypted domain. In extracting data from decrypted image the image is first decrypted and then data is extracted from it. This reversible data hiding technique achieves real reversibility. There is good improvement in the quality of marked decrypted images.

B. Reversible Data Hiding with Optimal Value Transfer

The optimal rule of value modification under a payload-distortion criterion is found by using an iterative procedure, and a practical reversible data hiding scheme is proposed. The secret data, as well as the auxiliary information used for content recovery, are carried by the differences between the original pixel-values and the corresponding values estimated from the neighbors. Here, the estimation errors are modified according to the optimal value transfer rule. Also, the host image is divided into a number of pixel subsets and the auxiliary information of a subset is always embedded into the estimation errors in the next subset. A receiver can successfully extract the embedded secret data and recover the original content in the subsets with an inverse order. This way, a good reversible data hiding performance is achieved.

C. Reversible Image Watermarking using Interpolation Technique

Watermarking embeds information into a digital signal like audio, image, or video. Reversible image watermarking can restore the original image without any distortion after the hidden data is extracted which can embed a large amount of covert data into images with imperceptible modification. In this scheme the interpolation-error, the difference between interpolation value and corresponding pixel value, to embed bit by expanding it additively or leaving it unchanged. Due to the slight modification of pixels, high image quality is preserved. Experimental results also demonstrate that the proposed scheme can provide greater payload capacity and higher image fidelity compared with other state-of-the-art schemes.

II. LITERATURE SURVEY

There are many techniques available regarding reversible data hiding in encrypted image such as follows:
A. Secret Fragment Visible Mosaic Images to Information Hiding Lai et al. [1] proposes an image transformation technique, which selects a target image similar to the secret image, then replaces each block of the target image by 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 with the secret image, and the visual quality of encrypted image is not so good.

Via Secret Fragment Visible Mosaic Images by Nearly Reversible Color Transformations Lee et al. [4] improve Lai et al.'s method by transforming the secret image to a randomly selected target image without any use of database. In Lee et al.'s method, each block of the secret image is transformed to a block of the target image with a reversible color transformation [5], and then the required information for restoring secret image, such as parameters, indexes of block, is added into the transformed blocks, it gives Encrypted image. Lee et al.'s method can transform a secret image to a randomly selected target image, and increase quality of the encrypted image. However, in Lee et al.'s method, the transformation is not reversible. So that secret image cannot be lossless reconstructed.

By Reserving Room before Encryption Authors [12] proposed a novel method for RDH in encrypted images, for that method they do not "vacate room after encryption" as done previously but "reserve room before encryption with a

traditional RDH algorithm, and thus it is easy for the data hider to reversibly embed data in the encrypted image. The proposed method can achieve real reversibility that is data extraction and image recoveries are error free. First up all they empty out room by embedding LSBs of some pixels into other pixels with a traditional RDH method and then encrypt the image, so the positions of these LSBs in the encrypted image can be used to embed data. Not only the proposed method separate data extraction from image decryption but also achieves excellent performance.

With Public Key Cryptography This correspondence [8] proposed a lossless, reversible and data hiding schemes for public-key-encrypted images probabilistic and homomorphic properties of cryptosystems. With these schemes, the pixel division/reorganization is avoided and the encryption/decryption is performed on the cover pixels directly so that the amount of encrypted data and the computational complexity are lowered. Due to data embedding on encrypted domain may result in a little bit distortion in plaintext domain due to the homomorphic property, the embedded data can be extracted and the original content can be recovered from the directly decrypted image. With the combined technique, a receiver may extract a part of embedded data before decryption, and extract another part of embedded data and recover the original plaintext image after decryption.

Via Key Modulation the data embedding is achieved through a public key modulation [9] mechanism, which allows us to embed the data via simple XOR operations, without accessing the secret encryption key. At the decoder side, a powerful two-class SVM classifier is designed to distinguish encrypted and no encrypted image patches, allowing us to jointly decode the embedded message and the original image signal. The proposed approach provides higher embedding capacity and is able to perfectly reconstruct the original image as well as the embedded message.

With Distributed Source Encoding This technique [10] aims to enhance scheme of reversible data hiding (RDH) in encrypted images using Slepian-Wolf source encoding which was inspired by DSC? After the original image is encrypted by the content owner using a stream cipher, the data-hider compresses a series of selected bits taken from the encrypted image to make spare room to accommodate for the secret data. With two different keys, the proposed method is separable. The hidden data can be completely extracted using the embedding key, and the original image can be approximately reconstructed with high quality using the encryption key. If the receiver has both the embedding and encryption keys, receiver can extract the secret data and perfectly recover the original image. The proposed method achieves a high embedding payload and good image reconstruction quality and avoids the operations of room-reserving by the sender.

By Patch-level Sparse Representation In [10] proposed a novel method called the HC_SRDHEI, which inherits the merits of RRBE, and the reparability property of RDH methods in encrypted images for a better relation between neighbor pixels, we propose consider the patch-level sparse representation when hiding the secret data. Compared to state-of-the-art alternatives, the room vacated for data hiding. The data hider simply adopts the pixel replacement to substitute the available room with additional secret data. The data extraction and cover image recovery are separable, and are free of any error. Experimental results on three datasets shows that the proposed method has average MER can reach 1.7 times as large as the previous best alternative method provides. The performance analysis implies that proposed method has a very good potential for practical applications.

Using Side Match W. Hong [11] proposed an improved version of Zhang's reversible data hiding method in encrypted images. Which divides the encrypted image into blocks, and each block carries one bit by flipping three LSBs of a set of pre-defined pixels. The data extraction and image recovery can be achieved by examining the block smoothness. Data recovery of block is performed in descending order of the absolute smoothness difference between two candidate blocks. The side match technique is employed to further reduce the error rate. I. Encrypted Image based on Chaotic Map A reversible data hiding technique in encrypted images based on chaotic maps [6] in which the secret data is embedded into the encrypted image and the original cover image can be loselessly recovered at the receiver end. Chaosis able to perfectly reconstruct the original image as well as the embedded message. F. with Distributed Source Encoding This technique [9] aims to enhance scheme of reversible data hiding (RDH) in encrypted images using Slepian-Wolf source encoding which was inspired by DSC? After the original image is encrypted by the content owner using a stream cipher, the data-hider compresses a series of selected bits taken from the encrypted image to make spare room to accommodate for the secret data. With two different keys, the proposed method is separable. The hidden data can be completely extracted using the embedding key, and the original image can be approximately reconstructed with high quality using the encryption key. If the receiver has both the embedding and encryption keys, receiver can extract the secret data and perfectly recover the original image. The proposed method achieves a high embedding payload and good image reconstruction quality and avoids the operations of room-reserving by the sender.

By Patch-level Sparse Representation In [10] proposed a novel method called the HC_SRDHEI, which inherits the merits of RRBE, and the separable property of RDH methods in encrypted images for a better relation between neighbor pixels, we propose consider the patch-level sparse representation when hiding the secret data. Compared to state-of-the-art alternatives, the room vacated for data hiding. The data hider simply adopts the pixel replacement to substitute the available room with additional secret data. The data extraction and cover image recovery are separable, and are free of any error. Experimental results on three datasets shows that the proposed method has average MER can reach 1.7 times as large as the previous best alternative method provides. The performance analysis implies that proposed method has a very good potential for practical applications. H. Using Side Match W. Hong [11] proposed an improved version of Zhang's reversible data hiding method in encrypted images. Which divides the encrypted image into blocks, and each block carries one bit by flipping three LSBs of a set of pre-defined pixels. The data extraction and image recovery can be achieved by examining the block

smoothness. Data recovery of block is performed in descending order of the absolute smoothness difference between two candidate blocks. The side match technique is employed to further reduce the error rate.

Encrypted Image based on Chaotic Map A reversible data hiding technique in encrypted images based on chaotic maps [12] in which the secret data is embedded into the encrypted image and the original cover image can be lossless recovered at the receiver end. Chaos based cryptosystems are being widely used for practical applications due to their properties like pseudo randomness, sensitivity on initial conditions and system parameters and the combination of reduced execution time, high security and high complexity to break the cryptosystem. This proposed system provides improved retrieved cover image quality, High data hiding capacity, Data extraction without error and a Lower bound PSNR of 50.91dB it gives better results than the existing system.

Research topic	Author , year	Method used	Advantages	Short comings
Reversible data hiding with optimal value transfer	Xinpeng Zhang, 2013	Rule of value modification under a payload distortion criterion is found by using an iterative procedure, and it propose practical reversible data hiding scheme	The mechanism gives a new rule of value modification and it can be used on various cover values	Computation complexity prediction will higher
Separable reversible data hiding in encrypted image	X. Zhang, 2012	Separable reversible data hiding, which consists of image encryption, data embed and extraction & Image recovery phases	Faster implementation	Inefficient data compression
Improve various reversible data hiding schemes via optimal codes for binary covers	W. Zhang, B. Chen, and N. Yu 2012	Decompression algorithm. is used as the coding scheme for embedding data	Code construction is proved to be optimal when the compression algo Reaches entropy	Difficulty in design codes for gray scale covers.
Reversible image watermarking using interpolation technique	Lixin Luo, Z. Chen, Xiao Zeng and Z Xiong 2010	It is used for minimize interpolation-error & the difference between interpolation value and Corresponding pixel value	Which can embed a large amount of data into images, and achieves better image quality	Errors in Calculation of interpolation will affect the secret information
Reversible Data Hiding in Encrypted Image	Xinpeng Zhang, 2011	With an encrypted image containing additional data, a receiver may firstly decrypt it using the encryption key, and the decrypted version is similar to the original image. According to the data-hiding key, he can further extract the embedded data and recover the original image from the decrypted version	the data-hiding key is not used, it is still impossibleto extract the additional data and recover the original image	Although someone with the knowledge of encryption key can obtain a decrypted image and detect the presence of hidden data using LSB-steganalytic methods
Difference Expansion Reversible Image Watermarking Schemes	Subhanya R.J (1), AnjaniDayanandh N (2)" 2014	Usesthe watermarking algorithm that embeds image/ text data invisibly into a video based on Integer Wavelet Transform and to minimize the mean square	can improve the quality of the watermarked image and give more robustness of the watermark and also increasing PSNR	Low hiding capacity and complex computations
An Effective Algorithm of Encryption and Decryption of Images Using Random Number Generation Technique and Huffman coding" .	Mr.T. Sri Harish Reddy, S. Kiran 2013	This algorithm is based on Ceaser Cipher algorithm, random generation technique, concept of shuffling the rows i.e. rows transposition and Huffman Encoding	provides high security to an image and occupies minimum memory space	Some problems in the decoding section such that , here Huffman coding is used

Table 1: Literature Review Summary

III. THE PROPOSED METHOD

This paper proposes a novel reversible data hiding scheme based on the histogram-shifting-imitated approach. Instead of utilizing the peak point of an image histogram, the proposed scheme manipulates the peak points of segments based on image intensity. The secret data can be embedded into the cover image by changing the peak point pixel value into other pixel value in the same segment. The proposed method uses a location map to guarantee the correct extraction of the secret data. Since the modification of the pixel value is limited with in each segment, the quality of the stego image i sonly related to the size of the segmentation, which means after embedding data into the cover image, it can be reused to do the multi-layerdataembeddingwhilemaintainingthehighqualityofthefinalstegoimage.

IV. CONCLUSION

A survey on various reversible data hiding techniques is executed. Reversible data hiding systems for encrypted image with a low computation complexity is analysed, which consists of image encryption, data hiding and data extraction. The original images are encrypted by an encryption strategy. So a revision about an encryption strategy is done. Although a data hider does not know the novel content, he can embed the top-secret data into the encrypted image by altering a part of encrypted data. So methods for data embedding are also noticed.

REFERENCES

[1] 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.
[2] 2014 Celebrity Photo Hack, [Online]: Available: Http:/En.Wikipedia.Org/Wiki/2014_Celebrity_PhotO_Hack.
[3] F. Bao, R. H. Deng, B. C. Ooi, et al., "Tailored reversible watermarking schemes for authentication of electronic clinical atlas," IEEE Trans. on Information Technology in Biomedicine, vol. 9, no. 4, pp. 554-563, Dec. 2005
[4] Y.-L. Lee and W.-H. Tsai, "A new secure image transmission technique via secret-fragment-visible mosaic images by nearly reversible color transformations," IEEE Trans. Circuits Syst. & Video Technol., vol. 24, no. 4, pp. 695–703, 2014.
[5] E. Reinhard, M. Ashikhmin, B. Gooch, and P. Shirley, "Color transfer between images," IEEE Computer Graphics and Applications, vol. 21, no. 5, pp. 34–41, 2001.
[6] AlkaDileep, K.Anusudha, Muhammed Asad P. T., "An Efficient Reversible Data Hiding Technique in Encrypted Images Based on Chaotic Map," IEEE International Conference on Control Instrumentation, Communication and Computational Technologies, 2015.
[7] K. Ma, W. Zhang, X. Zhao, N. Yu, F. Li, "Reversible data hiding in encrypted images by reserving room before encryption," IEEE Trans. on Information Forensics and Security, vol. 8, no. 3, pp. 553-562, Mar. 2013.
[8] Xinpeng Zhang, Jing Long, Zichi Wang, and Hang Cheng, "Lossless and Reversible Data Hiding in Encrypted Images with Public Key Cryptography," IEEE Trans. on Circuits and Systems for Video Technology, 2015.
[9] J. Zhou, W. Sun, L. Dong, et al., "Secure reversible image data hiding over encrypted domain via key modulation," IEEE Trans. on Circuits and Systems for Video Technology, vol. 26, no. 3, pp. 441-452, Mar. 2016.
[10] Z. Qian, and X. Zhang, "Reversible data hiding in encrypted image with distributed source encoding," IEEE Trans. on Circuits and Systems for Video Technology, vol. 26, no. 4, pp. 636-646, Apr. 2016.
[11] X. Cao, L. Du, X. Wei, et al., "High capacity reversible data hiding in encrypted images by patch-level sparserepresentation," IEEE Trans. On Cybernetics, vol. 46, no. 5, pp. 1132-1143, May. 2016
[12] W. Hong, T. Chen, H. Wu, "An improved reversible data hiding in encrypted images using side match," IEEE Signal Processing Letters, vol. 19, no. 4, pp. 199202, Apr. 2012.

