Scientific Journal Impact Factor (SJIF): 1.711

e-ISSN: 2349-9745
p-ISSN: 2393-8161

International Journal of Modern Trends in Engineering and Research
www.ijmter.com

Reversible Data Hiding in Encrypted Image: A Review

Ms. Nuzhat Ansari[1], Prof. Rahila Sheikh[2]
[1]*Dept. Of Computer Sci. & Engg., Rajiv Gandhi College of Engg. Research & Tech., Chandrapur,Maharashtra,India*
[2]*Dept. Of Computer Technology,Rajiv Gandhi College of Engg. Research &Tech., Chandrapur,Maharashtra,India*

Abstract-Recently, more and more attention is paid to reversible data hiding (RDH) in encrypted images, since it maintains the excellent property that the original cover can be losslessly recovered after embedded data is extracted while protecting the image content's confidentiality. All previous methods embed data by reversibly vacating room from the encrypted images, which may be subject to some errors on data extraction and/or image restoration. In this survey paper, we discuss about various methods and algorithms which were used for reversible data hiding (RDH) in encrypted image to make data hiding process effortless. We also use visual cryptographic approach for encryption which helps to protect the image during transmission. The scheme is suitable for authentication based application where collective acceptance and decision making plays an important role. The main goal is to retrieve the original image with lossless process and minimum computation during image encryption /decryption by using keyless approach.
Keywords - Reversible Data Hiding, image encryption, Visual Cryptography, encryption/decryption, authentication.

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.

Reversible Data Hiding: Reversible data hiding is an approach where data is hidden in an encrypted image. A reversible data hiding is an algorithm, which can recover the original image losslessly from the stego-image after the hidden data have been extracted. This important technique is widely used in medical imagery, military imagery and law forensics where no distortion of original image is allowed [2].

Visual Cryptography: Visual cryptography (VC) is a process where a secret image is encrypted into shares which refuse to divulge information about the original secret image. Its strength is a fact that the decryption of the secret image is through human visual system without computation [5].

II. RELATED WORK

Reversible data embedding has drawn lots of interest recently. Being reversible, the original digital content can be completely restored. As the amount of information needed to be embedded (payload and original values in the embedding area) is larger than that of the embedding area and the space saved from compression will be used for embedding the payload.

Siddharth Malik, Anjali Sardana, Jaya [3] proposed an approach without the use of encryption keys. Maintaining the secrecy and confidentiality of images is a vibrant area of research, with two different approaches being followed, the first being encrypting the images through encryption algorithms using keys; the other approach involves dividing the image into random shares to maintain the images secrecy. The proposed technique involves splitting an image into multiple shares. The shares so generated reveal no information about the original secret image and to retrieve the secret image all the shares are required. The proposed technique is implemented with the SDS algorithm and involves three steps – Sieving, Division and Shuffling. This technique involves computation during the encryption and decryption stages and the results are to be viewed on the computer monitors hence it is natural for us to use the additive color model. The scheme presented here is a (z, z) threshold scheme i.e. for retrieving a secret image that has been divided into z shares all z shares are required. No shares individually convey any information about the secret image, nor do a combination of subset of random shares.

Mehmet U. Celik, Gaurav Sharma, A. Murat Tekalp, Eli Saber [4] proposed a novel reversible data hiding technique, which enables the exact recovery of the original host signal upon extraction of the embedded information. A generalization of LSB (least significant bit) modification is proposed as the data embedding method, which introduces additional operating points on the capacity-distortion curve. Lossless recovery of the original is achieved by compressing portions of the signal that are susceptible to embedding distortion, and transmitting these compressed descriptions as a part of the embedded payload. It represents a high-capacity, low-distortion, lossless data embedding algorithms. In all algorithms, recovery of the original image is enabled by compressing, transmitting, and

recovering these features. This property of the proposed method provides excellent compression of relatively simple image features.

Moni Naor and Adi Shamir [5] proposed visual cryptography which is a method of protecting confidential information. It encrypts the content of information using some mathematical computation and then the decryption is done to revert back onto the original image and it requires the use of a secret key. With remarkable advances in computer technology, using a computer to decrypt secret image is infeasible in some situations. In these situations, the human visual system is one of the most convenient and reliable technique to do secret recovery. They come up with a visual secret sharing scheme, where an image is divided or broken up into n shares so that only someone with all n shares could decrypt the image, while someone with any n-1 shares can reveal no information about the original image. Each share is printed on a separate transparency (which serve the purpose of secret key) and decryption is performed by overlaying the shares when all n shares are overlaid, the original image gets appeared. Visual Cryptography provides one of the secure ways to transfer images on the Internet. The advantage of visual cryptography is that it exploits human eyes to decrypt secret images with no computation required.

Jun Tian [1] proposed reversible data embedding which has drawn lots of interest recently. Being reversible, the original digital content can be completely restored. He proposed reversible data embedding method for digital images. This paper explores the redundancy in digital images to achieve very high embedding capacity, and keep the distortion low. DE technique was introduced, which discovers extra storage space by exploring the redundancy in the image content. During data embedding, modify all changeable difference values, by either adding a new LSB (via the DE) or modifying its LSB. To guarantee an exact recovery of the original image, One should also embed the original values of those modified LSBs. In brief, the date-embedding DE algorithm consists of six steps: calculating the difference values, partitioning difference values into four sets, creating a location map, collecting original LSB values, data embedding by replacement, and finally an inverse integer transform.

Wen-Chung Kuo, Shao-Hung Kuo, Lih-ChyauWuu [9] proposed a reversible data hiding scheme based on EMD data hiding and JPEG image compression technology still keeping high embedding capacity, security and good compression ratio. Both data hiding and data compression are very important technologies in the field of image processing. It seems that there is no relationship between data hiding and data compression because most of the data hiding mechanisms focus on information security and the data compression mechanisms emphasize the compression ratio. . In fact, they are closely related. Until now, there are many literatures to discuss the secret data how to be embedded into the media image. Unfortunately, the stegno-image's size will be increased when the media image is hidden a lot of secret data. In order to overcome this disadvantage, a reversible data hiding scheme based on EMD data hiding and JPEG compression technology has been proposed in this paper. According to the experimental results, proposed scheme still keeps high embedding capacity, security and good compression ratio.

J. Fridrich, M. Goljan, and D. Rui [10] presented a review of reversible watermarking techniques and showdifferent methods that are used to get reversible data hiding technique with higher embedding capacity and invisible objects. Watermark need not be hidden. Watermarking can be applied to images, text, audio/video, software. In this review authors have described the different data hidingtechniques. The Image watermarking technique is used for protection and authentication of intellectual property. Invisible watermarking of images, the watermark image is embedded in a primary image such that watermark isintentionally perceptible to a human observer whereas in the case of invisible watermarking the embedded data isnot perceptible, but may be extracted/detected

by a computer program.The lossless watermarking technique is a process that is used for the exact recovery of the original image. Lossless watermarks found applications in fragile authentication, integrity protection, and metadata embedding. It is especially important for medical and military images. The lossless watermarking technique is also refer to as invertible, or distortion-free data hiding technique because it is capable of restoring the embedded image to its original state without accessing any side information. We can say that the embedding distortion can be erased or removed from the embedded image.

C. Anuradha, S. Lavanya [11] proposed secure and authenticated discrete reversible data hiding in cipher images deals with security and authentication. In the first phase, a content owner encrypts the original uncompressed image using an encryption key. Then, a data hider may compress the least significant bits of the encrypted image using a data hiding key to create a sparse space to accommodate some additional data. With an encrypted image containing additional data, if a receiver has the data hiding key, receiver can extract the additional data though receiver does not know the image content. If the receiver has the encryption key, can decrypt the received data to obtain an image similar to the original one, but cannot extract the additional data. If the receiver has both the data hiding key and the encryption key, can extract the additional data and recover the original content without any error by exploiting the spatial correlation in natural image when the amount of additional data is not too large. It is also a drawback because if the receiver has any one key as known, and then he can take any information from the encrypted data. In order to achieve authentication SHA-1 algorithm is being used. The proposed scheme is made up of image encryption, data embedding and data-extraction/image-recovery phases. This paper proposes a separable reversible data hiding in encrypted image. In the proposed scheme, the original image is encrypted using an encryption key and the additional data are embedded into the encrypted image using data-hiding key. With an encrypted image containing additional data, if the receiver has only the data-hiding key, he can extract the additional data though receiver does not know the image content. If receiver has only the encryption key, he can decrypt the received data to obtain an image similar to the original one, but cannot extract the embedded additional data.

III. PROPOSED WORK

The proposed method combines the benefits of two different approaches together that are reversible data hiding and visual cryptography. This gives an efficient solution to overcome the limitations of existing schemes in the area of reversible data hiding. Losslessly vacating the room from the encrypted image is relatively difficult and sometimes inefficient, so in the proposed system we have applied a method of vacating the room for embedding data prior to the image encryption, hence the vacated room can be used to hide the secret data. For image encryption instead of using any standard cipher, here a method of visual cryptography is used. In visual cryptography approach the image is divided into random shares and for retrieving the image all the shares will be required. Thus the image is protected in transmission and secret data is also transmitted securely. It does not involve the use of keys for encryption, has low storage and bandwidth requirements, while also keep the computation cost low during encryption and decryption. Thus key management is not an issue but the proposed method provides complete lossless image recovery and data extraction.

In general, we hide the data in the image only in the pixel value, the proposed system will divide an image into individual RGB components and stores each bit in the corresponding components. Since we are dividing the pixel value into three components, so the search space we get is three times more. This means we can add large amount of data in the image without degrading the quality of the image. The proposed method aims at achieving complete reversibility with minimum computation by employing keyless approach of visual cryptography.

It involves following steps:

1) Vacating room for embedding data
2) Data Embedding in reserved vacated room
3) Image Encryption using keyless SDS algorithm
4) Original image recovery
5) Data extraction

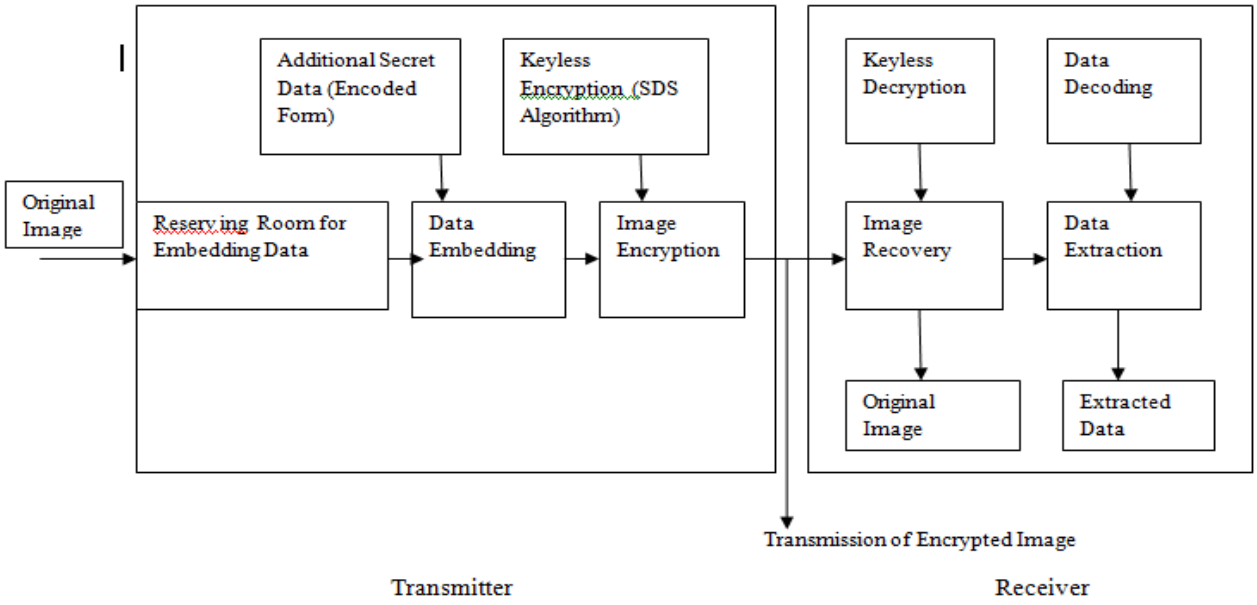

Fig.1: Framework for Proposed Scheme

IV. CONCLUSION

Reversible data hiding in encrypted image is drawing lots of attention because of privacy preserving requirements. Thus proposed scheme provides a completely new framework for reversible data hiding. Here in this approach we have used a new technique for reserving room before encryption of image. Thus the data hider can benefit from the extra space emptied out in previous stage before encryption to make data hiding process effortless. In the proposed approach we take advantage of visual cryptography approach for encrypting the image. Thus the image is protected in transmission and secret data is also transmitted securely. The employed technique involves the three main steps that are sieving, division and shuffling the images. Thus random shares are so generated from shuffled shares of image are transmitted. As this approach does not involve any use of keys is keyless approach for image encryption with the complete lossless image recovery and data extraction.

REFERENCES

[1] Jun Tian "Reversible Data Embedding Using a Difference Expansion" Transactions on circuits and systems for video technology, VOL. 13, NO. 8, AUGUST 2003.

[2] Kede Ma, Weiming Zhang, Xianfeng Zhao, Nenghai Yu, and Fenghua Li, " Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption" , IEEE Transaction on Information Forensics and Security, Vol.8, No.3, March 2013.

[3] Siddharth Malik, Anjali Sardana, Jaya, "A Keyless Approach to Image Encryption",2012 international conference on Communication systems and Network Technologies ©2012 IEEE.

[4] Mehmet U. Celik, Gaurav Sharma, A. Murat Tekalp, Eli Saber, "Reversible Data Hiding", IEEE ICIP 2002.

[5] Moni Naor and Adi Shamir, "Visual cryptography", in Proceedings of Advances in Cryptology EUROCRYPT 94, LNCS Vol. 950, pages 1-12. Springer-Verlag, 1994.

[6] Kuo-Ming Hung, Wen-Kai Su, Ting-Wen Chen, Li-Ming Chen, "Reversible Data Hiding Base on VQ and Halftoning Technique",8th International Conference on Information Science and Digital Content Technology(ICIDT),© IEEE 2012.

[7] Jose, R.; Abraham, G, "A separable reversible data hiding in encrypted image with improved performance", Emerging Research Areas and 2013 International Conference on Microelectronics, Communications and Renewable Energy(AICERA/ICMiCR), 2013 Annual International Conference ©IEEE 2013

[8] Jithi P V, Anitha T Nair, "Progressive Visual Cryptography with Watermarking for meaningful shares", International Multi-Conference on Automation , computing , Communication , control and Compressed Sensing (iMac4s), 2013.

[9] Wen-Chung Kuo, Shao-Hung Kuo, Lih-ChyauWuu, "High Embedding Reversible Data Hiding Scheme for JPEG", Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing,(IIH-MSP),Oct,2010.

[10] J. Fridrich, M. Goljan, and D. Rui, "Lossless Data Embedding - New Paradigm in Digital Watermarking", In Special Issue on Emerging Applications of Multimedia Data Hiding, Vol. 2, pp. 185-196, February 2002.

[11] C. Anuradha, S. Lavanya, "Secure and Authenticated Reversible Data Hiding in Encrypted Image", International Journal of Advanced Research in Computer Science and Software Engineering, volume 3,issue 4, April 2013

