Reversible data hiding in encrypted images: A survey

Ms.Mili Els Jose
Assistant Professor, Department of Computer science and Engineering
Viswajyothi College of Engineering and Technology. Vazhakulam, Kerala, India

Abstract: *This paper presents a survey of various methods for reversible data hiding in Encrypted Images. Reversible data hiding is a technique to embed additional message into a cover media with a reversible manner so that the original cover image can be perfectly restored after extraction of the hidden message. It will give security to the embedded data. But in the areas like cloud storage, medical systems etc. it is important to give protection to the image also .To solve this problem Reversible data hiding in encrypted images are used.*

Keywords - *Reversible Data Hiding, Image Encryption, Image Recovery.*

I. Introduction

Now a days outsourcing data to the cloud became more popular service .This cloud storage is mainly used to store videos or images which needs large storage area. The cloud storage may embed some additional data to the images such as owner name or image category etc. to manage the outsourced data. But the cloud storage has no authority to damage the user data. So reversible or lossless data hiding can be used for data hiding. Also It is vital to protect the privacy of data. Under such demands, reversible data hiding in encrypted images (RDH-EI) got more attraction..

II. REVERSIBLE DATA HIDING IN ENCRYPTED IMAGES (RDH-EI)

In RDH-EI, reversible data hiding is performed in an encrypted domain. The content owner encrypts the original image using any image encryption methods and sends it to the data hider. Data hider embeds additional information into the encrypted image using any reversible data hiding method. The receiver can extract the hidden data and decrypt the image. Common methods in Reversible Data Hiding are LSB Substitution, Difference Expansion[9], Histogram Modification method[1], [10] etc. There are two main types of Encryption: Symmetric encryption(Private key cryptography) Asymmetric encryption(Public key cryptography)

III.IMPORTANT METHODS OF RDH-EI

A. *REVERSIBLE DATA HIDING IN ENCRYPTED IMAGES[2]*

In [2] there are three parties: the content owner, data hider and the receiver. A content owner encrypts the original image using an encryption key to get the encrypted image. The data hider embeds data inside the encrypted image using data hiding key. The receiver extracts the embedded data from the encrypted image and then performs image recovery

Image Encryption [2]

This is done by performing an Exclusive Or operation between original bits and pseudo random bits. These pseudo random bits are calculated using Encryption key. Then the XOR results of various pixels are concatenated orderly.

Data Embedding [2]

This image is handed over to data hider and he can embed some extra data into the encrypted image by flipping a small part of the of encrypted image. The data hider first segments the encrypted image in a number of non-overlapping blocks of size s*s. For each block of size s2 divide pixels into two groups' s0 and s1according to a data hiding key. Then to be embedded data was checked .If the data to be embedded is 0, flip the 3 LSB bit of the encrypted pixel in s0. And if it is 1, then flip 3 LSB of pixel in s1.The other encrypted data will not change

.

Data Extraction and image Recovery [2]

The receiver got the encrypted image with the embedded data. The decryption operation is performed by the receiver. This is done by performing XOR operation with bits of the encrypted image and pseudorandom bits .This pseudo random bits are generated using encryption key. Then the 5 MSB bits of each pixels are received correctly.

For data extraction the decrypted image is divided into different blocks .Then the pixels of each block is divided into two parts i.e. s0 and s1.For each blocks three LSB's of s0 and s1 are flipped so as to form new blocks h1 and h2 .Then h0 or h1 contains the original LSB and this can be identified by using a fluctuation function. The result of this function is stored in f0 and f1 and by comparing f0 and f1the receiver can perform data extraction. If f0<f1 treat h0 as the original content and extract bit 0 otherwise h1 is the original content and extract bit 1.

Advantage [2]

1. This is an excellent scheme with low computational complexity.

Disadvantage [2]

1. There is a risk for the bit extraction and image recovery when divided block is relatively small.
2. The encrypted images got attention of the intruders when this method is used with cloud storage.

B. *SEPARABLE REVERSIBLE DATA HIDING IN ENCRYPTED IMAGE[4]*

The data-hider compresses the least significant bits (LSB) of the encrypted image using a data-hiding key to create a extra space to accommodate the additional data. The method proposed in [4] is made up of three phase's image encryption, data embedding and data embedding/image recovery phases. The content owner encrypt the original image using an encryption key.

Image Encryption [4]

This is done by performing an Exclusive or operation between original bits and pseudo random bits. These pseudo random bits are calculated using Encryption key. Then the XOR results of various pixels are concatenated orderly.

Data embedding [4]

Using a data hiding key, the data hider compresses the LSB of the encrypted image to create space to accommodate the additional data and original data at the positions are then occupied by parameters.

Data extraction/Image recovery phases [4]

In this phase, there are three cases to consider the receiver has only the data hiding key, only the encryption key and both data hiding and encryption key. With the data hiding key the receiver can only extract the embedded data. With the encryption key the user can only decrypt the image.in the third case user can bot extract the embedded data and decrypt the image.

Advantage [4]

1. This is an excellent scheme with low computational complexity.

Disadvantage [4]

1. The quality of the directly decrypted image is satisfactory
2. The encrypted images got attention of the intruders when this method is used with cloud storage.

C. *REVERSIBLE DATA HIDING IN ENCRYPTED IMAGES BY RESERVING ROOM BEFORE ENCRYPTION[7]*

In [7], the content owner reserves enough space on original image and then the image is encrypted using encryption key. The data hider only needs to accommodate data in the vacated space. The receiver then performs the data extraction and image recovery.

This method contains 4 different stages [7]

Generation of the encrypted image:

First step of this stage is the pixel division, here the image is divided into two parts A and B. Next step is self-reversible embedding .In this stage, LSB's of A are reversely embedded into LSB's of B with any standard RDH algorithms so that LSB's of A can accommodate messages. In the next step, the encrypted version of the image is created using stream cipher.

Data hiding in encrypted Image:

The encrypted image is send to the data hiderThe data hider perform data hiding using LSB substitution method.

Data Extraction and Image Recovery:

Data can extract from both the encrypted image and decrypted image. With the data hiding key receiver can decrypt LSB planes of the encrypted image and extract the additional information by reading the decrypted part. On the other hand, with the encryption key and data hiding key a user can decrypt the image and extract additional information from the LSB bits.

Advantages [7]:

1. Data extraction and image recovery are free of any error.
2. The PSNRs of the decrypted image containing embedded data are significantly improved for the given embedding rate.

Disadvantage [7]:

1. The encrypted images got attention of the intruders when this method is used with cloud storage.

D. LOSSLESS AND REVERSIBLE DATA HIDING IN ENCRYPTED IMAGES WITH PUBLIC-KEY CRYPTOGRAPHY [5]

In [5] a lossless, a reversible, and a combined data hiding scheme for public -key encrypted images.

Lossless Data Hiding Scheme [5]

The image provider encrypts each pixel of the plain text image using a public key. For encryption a generalization of pallier crypto system [6] is used. The encrypted image is send to the data hider. The data hider, without having any knowledge about the original image, will modified the cipher text pixel and embed data into it using by multilayer wet paper coding. The receiver can extract the embedded data from the encrypted domain .A direct decryption can result in the original image.

Reversible Data Hiding Scheme [5]

A pre-processing is employed to shrink the image histogram and then the image is encrypted. For encryption a generalization of pallier crypto system [6] is used. The encrypted image is send to the data hider. When having the encrypted image, the data hider, modifies the cipher text pixel values to embed the secret data and error correction codes. The receiver performs image decryption using private key. Then the embedded data was extracted from the decrypted image using the data hiding key.

Combined scheme [5]

The image provider performs histogram shrink and image encryption. . For encryption a generalization of pallier crypto system [6] is used. When having the encrypted image, the data hider may embed the first part of additional data using reversible scheme. Then the data hider embeds the second part of additional data using lossless scheme. On the receiver side, the receiver first extracts the second part of embedded data from the LSB-planes of encrypted image. After decryption with his private key, receiver extracts the first part of additional data and recovers the original plaintext image.

Advantages [5]:

1. With this system, pixel division or reorganization is avoided so the computational complexity is less.
2. The encryption or decryption performed on the cover pixels so the amount of encrypted data can be lowered.

Disadvantage [5]

1. Although the error correction mechanism is used large payload will cause failures for data extraction and image recovery.

IV. CONCLUSION

Now a Days Reversible data hiding in Encrypted images gets more popularity in the area of data communication.. In this paper different methods for reversible data hiding in encrypted images are presented with advantages and disadvantages. All these methods aim to reproducing image and secret data with maximum accuracy

REFERENCES

[1] J. Tian, “Reversible data embedding using a difference expansion,” IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, 2003.

[2] X. Zhang, “Reversible Data Hiding In Encrypted Image”S,‖ IEEE Signal Processing Letters, vol. 18, no. 4, pp. 255–258, 2011

[3] W. Puech, M. Chaumont, and O. Strauss, “A Reversible Data Hiding Method For Encrypted Images,” Proc. SPIE, vol. 6819, p. 68191E, Feb. 2008.

[4] X. Zhang, “Separable Reversible Data Hiding In Encrypted Image,”IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832,Apr. 2012.

[5] Xinpeng Zhang, Member, IEEE, Jing Long, Zichi Wang, and Hang Cheng, “Lossless And Reversible Data Hiding In Encrypted Images With Public-Key Cryptography”, IEEE Transactions On Circuits And Systems For Video Technology, Vol. 26, No. 9, September 2016

[6] P. Paillier, “Public-key cryptosystems based on composite degree residuosity classes,” in Advances in Cryptology (Lecture Notes in Computer Science), vol. 1592. Berlin, Germany: Springer-Verlag, 1999, pp. 223–238.

[7] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, “Reversible data hiding in encrypted images by reserving room before encryption,” IEEE Trans. Inf. Forensics Security, vol. 8, no. 3, pp. 553–562,Mar. 2013.

[8] Ahmet Murat Tekal, Eli Saber, Mehmet Utku Celik , Gaurav Sharma,”Lossless Generalized-LSB Data Embedding”, IEEE Transactions On Image Processing, Vol. 14, No. 2, February 2005

[9] J. Tian, “Reversible watermarking by difference expansion,” in Proc.Workshop on Multimedia and Security, J. Dittmann, J. Fridrich, and P.Wohlmacher, Eds., Dec. 2002, pp. 19–22.