RESEARCH ARTICLE OPEN ACCESS

A Survey Paper on Lossless and Reversible data hiding in Encrypted Images

Veena S. Nair [1], Dhanya K. Sudhish [2]
Department of Computer Science and Engineering
Alappuzha, Kerala

ABSTRACT
There are various techniques to transfer secret data from a source to destination. Data hiding is one of the effective means of communication. Data hiding is a technique of hide data into some media such as image, video, audio etc. This method is steganography. By this technique, the security of secret data increases and the authorized receiver can perfectly extract the data. Encryption is another way for secure transmission. Encryption is a technique of convert data into unreadable cipher text format. There exists many methods that combines encryption and data hiding. Some techniques causes distortion to image while embedding and some other technique can embed small amount of data. The different methods for data hiding are described in this paper.

Keywords:- XOR, Cryptography

I. INTRODUCTION

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.

II. RELATED WORKS

The various methods used for data security are described here.

Zhaoxia Yin et .al in [1] "reversible data hiding in encrypted images based on block histogram shifting" proposed a new reversible data hiding in encrypted image framework. In this method, additional data can be embedded into an encrypted image which is previously encrypted using Josephus traversal. By using block histogram shifting approach, hidden peak pixels is adopted to perform reversible data hiding. An authorized receiver can extract the data by using both keys. This technique has higher embedding capacity. But limitation is it reduces the image quality.

Xinperg Zhang et .al in [2] "reversible data hiding in encrypted images based on progressive recovery" proposed a new method for data hiding. Three persons are involved in this process. Content owner encrypts the original image and upload cipher text into server. The data hider resides on the server divides the encrypted image into three channels and embeds different amount of data into each one and make it marked encrypted image. The receiver can extract the additional data from marked encrypted image and plaintext image can recovered. It can embed a large amount of data. But main disadvantage of this method is higher distortion rate.

Wien Hong et .al in [3] "An improved reversible data hiding in encrypted images using side match" proposes a system where image is encrypted by using XOR operator to each bit with a key. The encrypted image is grouped as chunks and each chunk embed one bit. The data extraction and image regaining in done by using this chunks. And another factor is a side matching technique is used to check the smoothness. The smoothness is evaluated by concatenating the edges of chunks. The advantage of this system is that the side matching technique reduces error rate. But limitation is error occurs when chunk size increases.

Xinpeng Zhang et .al in [4] "Separable reversible data hiding in encrypted image", a novel scheme for separable reversible data hiding is proposed. This scheme is made up of image encryption, data embedding and data extraction/image recovery phase. In the first phase, content owner encrypts the original plain text image using an encryption key to create an encrypted image. Then data hider compress the least significant bit of encrypted image using a data hiding key to

create a sparse space to accommodate additional data. If a receiver has data hiding key, he may extract the additional data, though he does not know image content. If he has the encryption key, he can decrypt the image, but cannot extract the additional data. The receiver can extract additional data and decrypt original image only by using both the keys. The advantage of this method is using lossless compression. Because of lossless compression, data can be perfectly separated from the image. Drawback of this method is that only small amount of data can hide.

Kede Ma et .al in [5] "Reversible data hiding in encrypted images by reserving room before encryption", proposes a new method. In this method, the content owner reserves a room for additional data before encryption. By using traditional RDH method, embedding LSB of some pixel into other pixel and empty out the room and after that encrypt the image. Then the additional data is embedded on these rooms. On the receiver side, receiver can extract and decrypt correctly. Limitation of this method is amount of the additional data is less.

X. Zhang et .al in [6] "An improved reversible data hiding in encrypted images", a more improved method for data hiding is proposed. In this method, randomly selects pixels from image for secret data hiding. Because of this, no one knows which pixel is used to hide. A key is used to select the pixels randomly. Here estimate half of the pixels in the plain text image to obtain estimation error to hide secret data. Advantage is maximum embedding rate.

Jessica Fridrich et .al in [7] "Lossless data embedding for all image formats", suggested a system for lossless data embedding. It provides three methods for data embedding based on the capacity and alternation. The first technique is compression of LSB of the coefficient of signal. The succeeding techniques pre-processing the image. It can remove the error which occurred during embedding. But limitation of this method is the image get distorted when data is embed, and these distortions cannot remove.

X. Zhang et .al in [8] "Reversible data hiding in encrypted images," proposed a reversible data hiding procedure. The owner encrypts the uncompressed image by using the encryption key. Then data is embed into image by using data hiding key. Before data hiding, the data hider compress the image to provide space for additional data. On the receiver side, the receiver can decrypt the image by using encryption key. But he cannot extract data without knowing data hiding key. The authorized receiver should possess both keys. So only an authorized user can access the secret data.

Gyan Singh Yadav et .al in [9] "A Novel Visual Cryptography Scheme Based on Substitution Cipher", proposed a system for secured communication. It uses a twofold of encryption. In the first fold, the image is encrypted row wise and then column wise by using Caesar cipher and a key. A random matrix is generated. Then the secret image or data can be XOR ed with this matrix. This scheme is more secure and it is lossless. So the data can perfectly retrieved without any loss. The size of the key used is equal to the greatest common divisor of the number of the rows and columns of secret images. So the size of the key is large. It is difficult to handle large keys. This is the drawback of this scheme.

Shruti M. Rakhunde et .al in [10] "New Approach for Reversible Data Hiding Using Visual Cryptography" proposed a scheme of reversible data hiding with lossless recovery. Here the additional data is embed before image encryption. A modified algorithm for reversible data hiding is used in this scheme. After hiding data, a visual cryptography method is used to encrypt the image. This scheme increases the amount of data that can be hide into an image.

Patel Roshni et .al in [11] "Lossless Method for Data Hiding in Encrypted Image", proposes a scheme of data embedding into encrypted image using lossless method. Here content owner encrypts the image using a key. After that data hider compress the least significant bit of the image to produce a sparse space for secret data. The data hiding is lossless. So the receiver can correctly decrypts the data from the image. Limitation is it will cause distortion to the image.

Masaaki fujiyoshi et .al in [12] "A separable lossless data embedding scheme in encrypted images considering hierarchical privilege", presents an idea of separable lossless data embedding. The content owner first encrypts the image and simultaneously prepare a room for additional data. The room reservation is performed on the basis of the histogram shifting. Then the encrypted image carry secret data sent to receiver. The receiver can extract the data by using the key sets and seven different actions. The data is more securely transferred by using this scheme.

Xinperg Zhang et .at in [13] "lossless and reversible data hiding in encrypted images with public key cryptography", proposes a combined data hiding scheme in encrypted images. In this paper, lossless data hiding and reversible data hiding schemes are combined together. In lossless scheme, the cipher text pixels are replaced to embed the additional data into image. For this multilayer wet paper coding is used. The embed data can directly decrypt from encrypted image. In reversible data hiding, histogram of the image is shrink before encryption. Then secret data is embed into one to one manner. The reversible data is extracted only from plain text image. On the receiver side, receiver may extract first part of data before decryption and extract second part after decryption. The advantage of this method is more amount of data can hide. But limitation of this method is multilayer wet paper coding technique is not efficient. It cause more distortion to the image.

III. COMPARISON BETWEEN RELATED WORKS

Methods	PSNR(dB)	distortion
Reversible data hiding in encrypted images based on block histogram shifting	58.6	low
Reversible data hiding in encrypted images based on progressive recovery	38.1	Not mentioned
An Improved Reversible data hiding in encrypted images using side match	Not mentioned	low
Separable reversible data hiding in encrypted image	39.0	No
Reversible data hiding in encrypted images by reserving room before encryption	36.0	Not mentioned
An improved reversible data hiding in encrypted images	59.1	high
Lossless data embedding for all image formats	Not mentioned	No
Reversible data hiding in encrypted images	37.9	Low
A novel visual cryptography scheme based on substitution cipher	Not mentioned	high
A new approach for reversible data hiding using visual cryptography	43.08	high
Lossless method for data hiding in encrypted images	51.1	Not mentioned
A Separable lossless data embedding scheme in encrypted images considering hierarchical privilege	50.82	low
Lossless and Reversible data hiding in encrypted images with public key cryptosystems	49.7	Very low

IV CONCLUSION AND FUTURE WORKS

This paper compares different techniques used to hide data into encrypted images. Some techniques may hide large amount of data while some other hide small amount of data. Some techniques cause distortion to the image. Some techniques can perfectly retrieve data. Some methods badly affect both image and data. Every methods has its own advantages and limitations. All methods does not provide complete data security. Since communication through network requires high data security, an efficient and secured method is required. The combination of lossless and reversible method is so efficient. It hides two type of secret data. But multilayer wet paper coding technique cause more distortion to the image. If combine lossless and reversible data hiding in encrypted images with random pixel selection method, it will increase data security. It randomly selects some pixel to hide data by using a key. Because of this randomness, it is not easy to extract data for an unauthorized user. By using the key, receiver can find out the pixels and extract data. As a future work, hide lossless and reversible data in encrypted image using random pixel selection method has to be proposed. It will improves data security and payload capacity.

ACKNOWLEDGMENT

We thank members of Computer Science and Information Technology department of College of Engineering and Management, Punnapra, for their valuable support and feedbacks.

REFERENCES

[1] Zhaoxia Yin, Andrew Abel, Xinpeng Zhang and Bin Lio, “Reversible Data Hiding In Encrypted Image Based On Block Histogram Shifting ,”

[2] Zhenxing Qian, Xinpeng Zhang and Guorui Feng “Reversible Data Hiding in Encrypted Images Based on Progressive Recovery”

[3] W. Hong , T. Chen ,and H. Wu, “An improved reversible data hiding in encrypted images using side match,” IEEE Signal Process. Letter, vol. 19, no. 4, pp. 199–202, Apr. 2012., 1892, pp.68-73.

[4] X. Zhang, “Separable reversible data hiding in encrypted image,” IEEE Trans.Inf.ForensicsSecurity, vol.7, no.2, pp. 826–832, Apr.2012.

[5] Kede Ma, Weiming Zhang, Xianfeng Zhao, Nenghai Yu, and Fenghua Li, “Reversible Data Hiding in Encrypted Images by Reserving Room before Encryption”, IEEE transactions on information forensics and security,vol.8,no.3,march2013

[6] Shuang Yi and Yicong Zhou, “An improved reversible data hiding in encrypted images ,” Department of Computer and Information Science University of Macau, Macau 999078, China

[7] J.Fridrichand M.Goljan,“Lossless data embedding for all image formats, ”in Proc. SPIE Proc. Photonics West ,Electronic Imaging, Security and Watermarking of

Multimedia Contents, San Jose, CA, USA, Jan. 2002, vol. 4675, pp. 572–583

[8] X. Zhang, "Reversible data hiding in encrypted images,"IEEE Signal Process. Lett. vol. 18, no. 4, pp. 255–258, Apr. 2011.

[9] Gyan Singh Yadav and Aparajita Ojha, "A Novel Visual Cryptography Scheme Based on Substitution Cipher" IEEE transaction on image information processing 2013

[10] Shruti M. Rakhunde and Archana A. nikose, "New Approach for Reversible Data Hiding Using Visual Cryptography", 2014 Sixth International Conference on Computational Intelligence and CommunicationNetworks.

[11] Patel Roshni, prof. Aslam Durvesh and Patel urvisha, "Lossless Method for Data Hiding In Encrypted Image", IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems ICIIECS'15.

[12] Masaaki FUJIYOSHI, "A Separable Lossless Data Embedding Scheme In Encrypted Images Considering Hierarchical Privileg", Department of Information and Communication Systems, Tokyo Metropolitan University 6–6 Asahigaoka, Hino-shi, Tokyo 191–0065, Japan.

[13] Xinpeng Zhang, Jing Long, Zichi Wang, and Hang Cheng, "Lossless and Reversible Data Hiding in Encrypted Images with Public Key Cryptography", IEEE Transactions on circuit and video technology, 2015