ISSN:0975-9646

A Survey on Secure Data Hiding Techniques in Encrypted Images

[1]Anjaly Mohanachandran, [2]Mary Linda P.A.

[1,2]Department Of Computer Science and Engineering
KMCT College of Engineering and Technology
Calicut, Kerala, India

***Abstract—* The security plays an important role in transmission of confidential data over internet. So, as a part of improving security in data transmission, we will hide the data inside an encrypted image. Thereby, confidentiality of the image as well as the embedded data is maintained. The embedded data can be extracted without any error , and also the cover image restoration is also free from error. Such a method used here is termed as Reversible Data Hiding (RDH). So, here we are conducting a survey based on different Reversible data hiding techniques. Since it maintains the excellent property that the original image can be losslessly recovered after embedded data is extracted. The major application of this method is medical imagery, military where both data and cover image is confidential. The most improved technique of reversible data hiding is the one in which content owner creates space for data embedding before encryption of cover image. After that the data hider embeds the data inside it. Then at the receiver side host can extract the data and recover the original image separately. Thus the concept Reserve Room Before Encryption (RRBE) of the RDH improves the security.**

***Keywords* — Data Hiding, Reversible data hiding, Image encryption, Image decryption.**

I. INTRODUCTION

Nowadays transmission of data by embedding it in digital images has widely increased. The security can be improved by sending data in this way. Such a Data hiding scheme in which real reversibility can be achieved is termed as Reversible Data Hiding (RDH).This RDH technique can be used in case of encrypted images. Thereby security of the cover image can be ensured. The situation in which both the transmitted data and the cover image is confidential, then we can make use of reversible data hiding technique in encrypted images.

Encryption is also a major factor that provides security to confidential data. So, stegenography and cryptography are major two areas which provide secure data transmission over internet. The security provided by stegenography is more than the security provided by cryptography alone. Cryptography can protect the data while transmission but when it is decrypted, there is no more protection left.

The technique RDH is established based on the steganography & security. While transferring the data from the source to destination, there is a chance of occurring intruder attack and that steals the confidential information. So, this type of transmission is restricted by some applications such as military imagery, law forensic etc. The existing RDH techniques do not give real reversibility. All the previous methods embed data by reversibly vacating room from the encrypted images (VRAE) which may subject to some errors in data extraction and image recovery. And also the hackers can recover the embedded data from the original image easily because data is placed in particular bit position after image encryption. But the proposed RDH technique can take the advantage of all the traditional techniques. The new technique Reserve Room Before Encryption (RRBE) can achieve separation in data extraction and image recovery. Thus the security is maintained.

II. LITERATURE SURVEY

Reversible data hiding emphases on the data embedding or extraction. The main aim of this technique is the error free and separable data extraction and image recovery.

Xinpeng Zhang presented a scheme in which, a content owner encrypts the original image using an encryption key, and a data-hider embeds additional data into the encrypted image using a data-hiding key yet he does not know the original content. With an encrypted image containing additional data, a receiver may first decrypt it according to the encryption key, and then extract the embedded data and recover the original image according to the data-hiding key. In the scheme, the activity of data extraction is not separable from the activity of content decryption. In other words, the additional data must be extracted from the decrypted image, so that the principal content of original image is opened before data extraction, and, if someone has the data-hiding key but not the encryption key, he is not able to extract any information from the encrypted image containing additional data [1].

Z. Ni, Y. Shi, N. Ansari, and S. Wei ,[2] have proposed a system that perform the Reversible Data hiding by using the histogram shift operation for RDH. In this system used the spare space for embedding the data by shifting the bins of gray scale values. The embedding capacity measured by the use of number of pixels in peak point. This system has some benefits such as it is simple and has constant PSNR ratio, capacity is high and distortion is very low. This system has some disadvantages such as more time consuming while searching the image number of times.

J.Tian [3] has proposed a system which uses difference expansion method for embedding data in reversible manner for digital images. Reversible data embedding means lossless embedding. Here quality degradation was very low after embedding the data. This paper describes how to measure the performance of the system by using the concept of reversible data embedding. This can be measure through various factors such as the payload capacity limit, visual quality and complexity. This system uses the differences between two neighboring pixels. The LSB's of the differences are all zero and this embedded to the message. The benefits of the system are no loss of data while performing compression and decompression. This system is useful for audio and video data. The drawbacks of the system are achieving error because of division by 2 and due to bit replacement visual quality degrade.

Reversible watermarking enables the embedding of useful information in a host signal without any loss of host information. Tian's difference-expansion technique is a high-capacity, reversible method for data embedding. However, the method suffers from undesirable distortion at low embedding capacities and lack of capacity control due to the need for embedding a location map. Diljith M. Thodi et.al [4] proposes a histogram shifting technique as an alternative to embedding the location map. The proposed technique improves the distortion performance at low embedding capacities and mitigates the capacity control problem. We also propose a reversible data-embedding technique called prediction-error expansion. This new technique better exploits the correlation inherent in the neighborhood of a pixel than the difference-expansion scheme. Prediction-error expansion and histogram shifting combine to form an effective method for data embedding. The experimental results for many standard test images show that prediction-error expansion doubles the maximum embedding capacity when compared to difference expansion. There is also a significant improvement in the quality of the watermarked image, especially at moderate embedding capacities.

W. Zhang, B. Chen, and N. Yu [5] have proposed a system which uses a decompression algorithm for embedding the data .It approaching the codes for reversible data hiding and improve the recursive code construction for binary bounds and this type of construction achieve the result that is rate-distortion bound that uses the concept of compression algorithm. This system checks the equivalency between data compression and RDH for binary bounds. This system defines many benefits such as reduces the distortion, improve the RDH schemes for spatial. This system also has some drawback such as not consider grey scale for designing recursive codes.

Wei Liu et.al suggested a lossless compression method for encrypted gray image using progressive decomposition and rate-compatible punctured turbo codes. In this method they developed resolution progressive compression, which has been shown to have much better coding efficiency and less computational complexity than existing approaches [6].Wei Liu and et.al observed that lossless compression of encrypted sources can be achieved through Slepian-Wolf coding. For encrypted real-world sources such as images, they are trying to improve the compression efficiency. In this paper [6], he proposed a resolution progressive compression scheme which compresses an encrypted image progressively in resolution, such that the decoder can observe a low-resolution version of the image, study local statistics based on it, and use the statistics to decode the next resolution level. He focused on the design and analysis of a practical lossless image codec, where the image data undergoes stream-cipher based encryption before compression. Resolution progressive compression is used for this problem, which has much better coding efficiency and less computational complexity than existing approaches [6].

L. Luo et al. [7] have used an interpolation technique for reversible image watermarking. Reversible image watermarking restores the original image without any distortion after performing the extraction of hidden data. In this system we can embed large amount of covert data for imperceptible modification. Digital watermarking is the form of data hiding that are used to embed the covert information into digital signal. This paper based on adaptive interpolation-error expansion, which provides very low distortion rate and lager capacity. It also improves the image quality.

X. L. Li, B. Yang, and T. Y. Zeng [8] have used a hybrid algorithm. It is basically uses three algorithms adaptive embedding, Predictive –Error Expansion (PEE) and Pixel selection. Predictive Error expansion is important for embedding the data and used for reversible watermarking. It provides authentication and integrity to the user. It also improves the payload with low distortion. Where distortion free data required we use the concept of watermarking. PEE is an improvement of the Difference Expansion (DE). The proposed system described the threshold value for pixel of image and it divides the image pixels into two parts. Afterward select the pixel on the basis of capacity parameter and threshold. Adaptive embedding and pixel selection performed simultaneously. This system reduces the embedding impact with the use of decreasing the modification and improves the visual quality.

Wien Hong et.al [9] proposes an improved version of Zhang's reversible data hiding method in encrypted images. The original work partitions an 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. Zhang's work did not fully exploit the pixels in calculating the smoothness of each block and did not consider the pixel correlations in the border of neighboring blocks. These two issues could reduce the correctness of data extraction. This letter adopts a better scheme for measuring the smoothness of blocks, and uses the side-match scheme to further decrease the error rate of extracted-bits. The experimental results reveal that the proposed method offers better performance over Zhang's work. For example, when the block size is set to 8x8, the error rate of the Lena image of the proposed method is 0.34%, which is significantly lower than 1.21% of Zhang's work.

. Mark Johnson investigated the novelty of reversing the order of these steps, i.e., first encrypting and then compressing. He showed that in certain scenarios his scheme requires no more randomness in the encryption key than the conventional system where compression precedes encryption. Mark Johnson and et.al has examined the possibility of first encrypting a data and then compressing it, such that the compressor does not have knowledge of the encryption key. The encrypted data can be compressed using distributed source coding principles, because the key will be available at the decoder. They showed that under some conditions the encrypted data can be compressed to the same rate as the original, unencrypted data could have been compressed [10].

Wei Zhang and Xianfeng Zhao [11] have proposed the system that maintains the reversibility. This paper defines the reversible data-hiding in encrypted image by using spare space as reserving room before encryption. Here more attention on RDH technique which maintains the reversibility that means original cover recovered after embedding additional data. It provides the security and confidentiality to user. It is new topic for cloud data management because of privacy preserving requirements. The Existing System implemented by the use of the concept of RDH in encrypted images by vacant room before encryption, but proposed system was opposite of it in this we use the reserving concept before encryption. The advantages of this proposed system is to maintain the extra space for embedding data in data hider module. This system achieves excellent performance without any loss of data.

III. Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption

Losslessly vacating room from the encrypted images is relatively difficult and sometimes inefficient. A novel framework RRBE is used. RRBE primarily consists of four stages:

- Encrypted image generation.
- Data hiding in encrypted image.
- Data extraction.
- Image recovery

The content owner first reserves enough space on original image and then convert the image into its encrypted version with encryption key. Then the data hider embeds the data in the space created and encrypts it using data hiding key. At the receiver side, the data can be extracted by using data hiding key and image can be decrypted using the same encryption key. Both the data and image can be extracted if the receiver has both data hiding and encryption key. Thus the separation of data extraction and image recovery is implemented.

A. Generation of Encrypted Images

To construct the encrypted image, the first stage can be divided into three steps: Image partition, Self-reversible embedding, and Image encryption.

At the beginning, image partition step divides original image into two parts A and B ; then, the LSBs of A are reversibly embedded into B with a standard RDH algorithm so that LSBs of A can be used for accommodating messages; at last, encrypt the rearranged image to generate its final version.

B. Data hiding in encrypted image

In this step, the content owner encrypts the original image using standard cipher with an encryption key. Once the data hider acquires the encrypted image, he can embed some data into it, although he does not get access to the original image. The embedding process starts with LSB replacement to substitute the available bit-planes with additional data. Finally, the data hider sets a label following to point out the end position of embedding process.

C. Data extraction and image recovery

Data extraction is independent from image decryption. While extracting data from encrypted images to manage and update personal information of encrypted images, for protecting client's privacy, an inferior database manager may only get access to the data hiding key and using it data can be manipulated. Thus privacy of image is maintained. There exist two cases:

- Case 1: Extracting data from encrypted images.
- Case 2: Extracting data from decrypted images.

IV. Conclusion

Reversible data hiding techniques provide security to data transmission. Studies show that the previous methods of RDH have many drawbacks this can be solved using the new RDH technique Reserving room before encryption. The data hider can benefit from the extra space emptied out in previous stage to make data hiding process effort- less. Moreover, this new method can achieve real reversibility; separate data extraction and image recovery thereby greatly improve the quality of restored images.

Acknowledgment

We are grateful to our project guide and Head of the Department Prof. Mary Linda P.A for her remarks, suggestions and for providing all the vital facilities like providing the Internet access and important books, which were essential. We are also thankful to all the staff members of the Department of Information Technology and Computer Science & Engineering of KMCT College of Engineering and Technology, Calicut.

References

[1] X. Zhang, "Reversible data hiding in encrypted images," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255258, Apr. 2011.

[2] Z. Ni, Y. Shi, N. Ansari, and S. Wei, "Reversible data hiding," *IEEE Trans.Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354–362, Mar.2006.

[3] J. Tian, "Reversible data embedding using a difference expansion" Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890 2003.

[4] D.M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," IEEE Trans.Image Process., vol. 16,no. 3, pp. 721–730, Mar. 2007.

[5] W. Zhang, B. Chen, and N. Yu, "Improving various reversible data hiding schemes via optimal codes for binary covers" vol. 21, no. 6, pp. 2991–3003, June. 2012.

[6] Wei Liu, Wenjun Zeng, Lina Dong, and Qiuming Yao "Efficient Compression of Encrypted Grayscale Images", Image Processing, IEEE Transactions Vol: 19, April 2010, pp. 1097 –1102.

[7] L. Luo et al., "Reversible image watermarking using interpolation ," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 187–G. Xuan, J. Chen, J. Zhu, Y.Q. Shi, Z. Ni, and W. Su, "Lossless Data hiding.

[8] X. L. Li, B. Yang, and T. Y. Zeng, "on adaptive prediction-error expansion and pixel selection Image Process., vol. 20, no. 12, pp. 3524.

[9] W. Hong, T. Chen, and H.Wu, "An improved reversible data hiding in encrypted images using side match," IEEE Signal process. Lett.,vol. 19, no. 4, pp. 199–202, Apr. 2012.

[10] M. Johnson, P. Ishwar, V.M. Prabhakaran, D. Schonbergand K. Ramchandran, "On compressing encrypted data," IEEE Trans. Signal Process., vol. 52, no. 10, pp. 2992-3006, Oct. 2004.

[11] Kede Ma, Wei. Zhang, Xianfeng Zhao, "Reversible data Hiding in Encrypted Images by reserving Room before encryption", IEEE trans. On information forensics and security, vol,8 No.3 , march 2013.