International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-2, Issue-1, January 2016
ISSN: 2395-3470
www.ijseas.com

A Survey on Data Hiding Techniques in Encrypted Images

Krishna Priya S[1], [2] Minu Lalitha Madhavu
[1] Sree Buddha College of Engineering, Alappuzha, India
[2] Sree Buddha College of Engineering, Alappuzha, India

Abstract
The transmission of confidential data over the network requires more security. So, for improving security in data transmission, we can hide the data inside an encrypted image. Hence the confidentiality of the image and the data embedded in the image is maintained. The data embedded can be extracted without any error, and also the cover image can be restored with error free. This type of techniques is termed as Reversible Data Hiding. We are conducting a survey in this paper based on different Reversible data hiding techniques. In this technique the original image can be recovered losslessly. If we use a combined lossless and reversible data hiding techniques, one part of data can be extracted before image encryption and another confidential part can be extracted after encryption.
Keywords: — *Data hiding, Reversible data hiding, Image encryption, Image decryption.*

1. Introduction

Nowadays the data is transmitted by embedding it in images. This way improves the security of the data. This type of data hiding in which the reversibility can be achieved is called as Reversible Data Hiding. This technique is mainly used in case of encrypted images. Hence the security of the cover image can be ensured. We can use this technique where situation in which both the transmitted data and the cover image is confidential.

Encryption provides security to confidential data. The major two areas stegenography and cryptography provides secure data transmission over internet. Stegenography provides much more security than the security provided by cryptography alone. Cryptography can protect the data during transmission but when it is decrypted, there is no more protection left.

The technique Reversible Data Hiding is established based on the steganography & security. That is the data is embedded in an encrypted image. In the very first step, the image is encrypted using any encryption algorithm. Then the data to be secured is embedded in the encrypted image. With an encrypted image with additional data, if the receiver has the data-hiding key, then he can extract the additional data even though he does not know the image content. If the receiver has the encryption key, then he can decrypt the received data to recover an image similar to the original image, but no able to extract the additional data. If the receiver has both the keys, then he can extract the additional data and also he can recover the original content which is errorless.

The data hiding techniques can be done in a lossless or reversible manner. The terms lossless and reversible can be distinguished in different manner. We can say that a data hiding method is lossless if the display of cover image containing embedded data is same as that of original cover even though the cover data have been modified for data embedding.

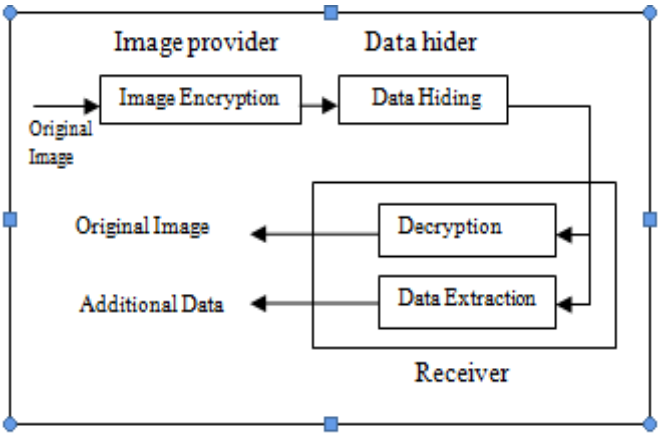

Fig.1 Sketch of lossless data hiding scheme

On the other hand, we can say that a data hiding method is reversible if the original image content can be perfectly recovered from the image version containing embedded data even though a slight

distortion has been introduced in data embedding procedure.

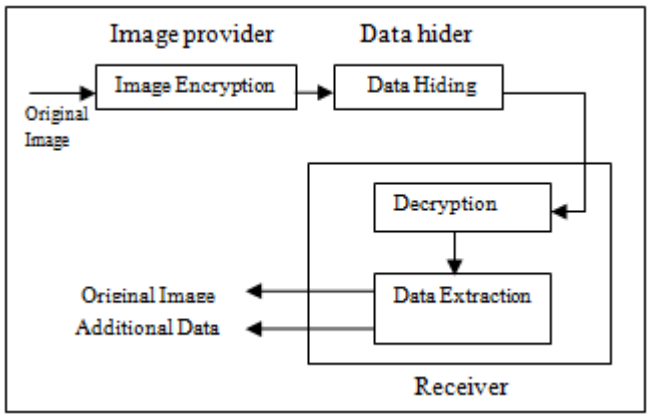

Fig.2 Sketch of reversible data hiding scheme

Both these lossless and reversible data hiding schemes can be combined together to get a more secure and error free data hiding technique .The data embedding process can be done in encrypted domain in both schemes. But the data extraction processes in two schemes are different. Hence by combining these two schemes we can embed two parts of data into a single image. That means the additional data for various purposes may be embedded into an encrypted image, and a part of the additional data can be extracted before decryption and another part can be extracted after decryption.

2. LITERATURE SURVEY

Reversible data hiding emphasis 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 [1] 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.

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 measured through various factors such as the payload capacity limit, visual quality and complexity. This system uses the differences between two neighbouring 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.

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. They 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.

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].

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] proposed 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 neighbouring 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.

Mark Johnson and et.al [10] 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.

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. 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 that uses the reserving concept before encryption. The advantages of this proposed system is to maintain the extra space for embedding data in data hider module.

Jiantao zhou , Weiwei Sun, et,al [12] proposed another reversible data hiding scheme over encrypted images. The data embedding is achieved through a public key modulation mechanism and so there is no need of a secret key. There is a powerful two class SVM classifier at the receiver side to distinguish between encrypted and non-encrypted image patches and it also allows to jointly decoding the embedded message and the original image. The data embedding is done by simple XOR operations, without the need of accessing the secret key.

3. CONCLUSION

Reversible data hiding in encrypted image is a powerful technique for the security of data. Data hiding in encrypted images provides double security for the data such as image encryption as well as data hiding. The existing systems contains some problems so we need to remove the problems by combining lossless and reversible technique means, data extraction and recovery of image are error free. The PSNR will be improved to get original cover image back. By combining lossless and reversible data hiding techniques, more advanced and efficient data embedding can be done in encrypted images.

.

Acknowledgments

We are grateful to our project guide and PG Coordinator Prof. Minu Lalitha Madhavu 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 Computer Science & Engineering of Sree Buddha College of Engineering, Alappuzha.

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.

[12] Jiantao Zhou, Weiwei Sun, Li Dong,Xianming Liu, Oscar C. Au,and Yuan Yan Tang, "Secure Reversible Image Data Hiding over Encrypted Domain via Key Modulation", IEEE transactions on circuits and systems for video technology,2015

Krishna Priya S received B.Tech. degree in Computer Science and Engineering from Kerala University, India. Pursuing M.Tech. degree in Computer Science and Engineering from Kerala University, India.

Minu Lalitha Madhavu received B.Tech. degree in Computer Science and Engineering from Rajiv Gandhi Institute of Technology , MG University, India, received M.Tech. degree in Technology Management from Kerala University, India. Currently, She is Assistant Professor at Sree Buddha College of Engineering, Kerala University, India