A Survey Of Lossless And Reversible Data Hiding In Encrypted Images

Lokhande Mayuri Bhausaheb, Prof.N.G.Pardeshi.

[1] PG Student, Computer Department, SRES COE, Maharashtra, India.
[2] Assistant Professor, Computer Department, SRES COE, Maharashtra, India.

ABSTRACT

A system for lossless and reversible data hiding in encrypted images proposes a lossless, a reversible, and a combined data hiding schemes. To add one more level of security the scheme is applied for cipher text images. The cipher text is then encrypted by public key cryptosystems. The first scheme is lossless scheme. In this scheme, the cipher text pixels are replaced with new values. The replacement of pixel is done to embed the additional data into several LSB-planes of cipher text pixels by multi-layer wet paper coding. Then, the embedded data can be directly extracted from the encrypted domain, and the data embedding operation does not affect the decryption of original plaintext image. The second scheme is reversible scheme. In this scheme, a preprocessing is employed to shrink the image histogram before image encryption, so that the modification on encrypted images for data embedding will not cause any pixel oversaturation in plaintext domain. From the decrypted image we can then find the embedded data and the original image in spite of slight distortion. The third and final scheme is the combined scheme i.e. combination of lossless and reversible scheme. With the combined technique, there are two possible outcomes. A receiver may extract a part of embedded data before decryption, and extract another part of embedded data and recover the original plaintext image after decryption. In literature survey it was noticed that some of the previous system do not differenticiate between the two system I.e. reversible and lossless system. It is also noticed that if data embedding capacity increases then the image quality decreases. The existing system tries to overcome all these flaws.

Keyword: *- reversible data hiding, lossless data hiding, image encryption*

1. INTRODUCTION

There are various techniques available for data protection. Out of which encryption and data hiding are two effective means of data protection. The encryption techniques convert plaintext content into unreadable cipher text. The data hiding techniques embed additional data into cover media. The data can be embedded by introducing slight modifications. Data hiding may be performed with a lossless or reversible manner. In the proposed system the terms " lossless" and " reversible" will be distinguished. In the previous references these two terms have the same meaning.

If the display of cover signals containing embedded data is same as that of original cover even though the cover data have been modified for data embedding, in this case we can say that the data hiding method is lossless. If the original cover content can be perfectly recovered from the cover version containing embedded data even though a slight distortion has been introduced in data embedding procedure, in this case we can say that the data hiding scheme is reversible.

2. Literature Review

Author Xinpeng Zhang, in his paper" Reversible Data Hiding with Optimal Value Transfer" has tried to improve the performance of reversible data hiding. In order to achieve a good payload-distortion performance of reversible data hiding, his work first finds the optimal value transfer matrix by maximizing a target function of pure payload with an iterative procedure, and then proposes a practical reversible data hiding scheme. The differences between the original pixel-values and the corresponding values estimated from the neighbors are used to carry the payload that is made up of the actual secret data to be embedded and the auxiliary information for original content recovery [5].

Kede Ma, Weiming Zhang, Xianfeng Zhao, Nenghai Yu, and Fenghua Li have developed the system by reserving room before encryption. To make the data hiding process effortless, extra space is made empty in the previous stage. .The method can take advantage of all traditional RDH techniques for plain images and achieve excellent performance without loss of perfect secrecy. Furthermore, this novel method can achieve real reversibility, separate data extraction and greatly improvement on the quality of marked decrypted images. Reversible data hiding (RDH) in images is a technique, by which the original cover can be losslessly recovered after the embedded message is extracted [3].

Jessica Fridrich, Miroslav Goljan, Petr Lisonek, and David Soukal have shown that by using the wet paper coding, one can represent on average Nd bits by only flipping a part of dry elements where Nd is the number of dry elements. In this scenario, the data-hider may flip the dry elements by replacing [6].

W. Puech, M. Chaumont, and O. Strauss showed that data embedding is performed in encrypted domain & authorized receiver can recover the original plaintext image & extract the embedded data, in their paper A Reversible Data Hiding Method for Encrypted Images. AES is used for data encryption. Quality of decrypted image degrades [7].

X. Zhang in his paper Separable Reversible Data Hiding in Encrypted Image showed that data hider compresses the LSB of encrypted image to generate a sparse space for carrying additional data [8].

Xinpeng Zhang in his paper Reversible Data Hiding with Optimal Value Transfer improves the performance of reversible data hiding. In order to achieve a good payload-distortion performance of reversible data hiding, his work first finds the optimal value transfer matrix by maximizing a target function of pure payload with an iterative procedure, and then proposes a practical reversible data hiding scheme[9].

3. OVERVIEW OF THE YSTEM

3.1 Lossless Data Hiding Scheme

This scheme involves three parties:

1. An image provider.
2. A data hider.
3. A receiver.

The role of image provider is to encrypt each pixel of the original plaintext image using the public key of the receiver. The data hider is unaware with the original image. Data hider can modify the cipher text pixel values to embed some additional data into the encrypted image by multi-layer wet paper coding .There lies one condition that the decrypted values of new and original cipher-text pixel values must be same. The receiver have the encrypted image containing the additional data, a receiver knowing the data hiding key may extract the embedded data, while a receiver with the private key of the cryptosystem may perform decryption to retrieve the original plaintext image. The embedded data can be extracted in the encrypted domain, and cannot be extracted after decryption. That means the data embedding does not affect the decryption of the plaintext image [1].

3.2 Reversible Data Hiding Scheme

To shrink the image histogram some preprocessing is employed in reversible scheme. Then each pixel is encrypted with additive homomorphic cryptosystem by the image provider. When data hider have the encrypted image, he modifies the cipher text pixel values to embed a bit-sequence generated from the additional data and error-correction codes. . Due to the homomorphic property, the modification in encrypted domain will result in slight increase/decrease on plaintext pixel values. The advantage of histogram shrink before encryption is that the data embedding operation does not cause any overflow/underflow in the directly decrypted image[1].

3.3 Combined Data Hiding Scheme

In the lossless scheme and the reversible scheme, the data embedding operation is performed in the encrypted domain. The data extraction for above two schemes is very different. With the lossless scheme, data embedding does not affect the plaintext content and data extraction is also performed in encrypted domain. With the reversible scheme, there is slight distortion in directly decrypted image caused by data embedding, and data extraction and image recovery must be performed in plaintext domain. In the combined scheme, the image provider performs histogram shrink and image encryption. When having the encrypted image, the data-hider may embed the first part of additional data. On receiver side, the receiver firstly extracts the second part of additional data from the LSB-planes of encrypted domain [1].

4. CONCLUSION

In the lossless scheme, the embedded data can be directly extracted from the encrypted domain, and the data embedding operation does not affect the decryption of original plaintext image. In the reversible scheme, the additional data can be extracted from the plaintext domain, and, although a slight distortion is introduced in decrypted image, the original plaintext image can be recovered without any error. Due to the compatibility of the two schemes, the data embedding operations of the lossless and the reversible schemes can be simultaneously performed in an encrypted image. So, the receiver may extract a part of embedded data in the encrypted domain, and extract another part of embedded data and recover the original plaintext image in the plaintext domain.

5. ACKNOWLEDGEMENT

" A System for Lossless and reversible data hiding in encrypted images" had been a wonderful subject to research upon, which leads ones mind to explore new heights in the field of secure communication over a network. I dedicate all my seminar works to my esteemed guide, Prof. N. G. Pardeshi, whose interest and guidance helped me to complete the work successfully. This experience will always steer me to do my work perfectly and professionally. I also extend my gratitude to Prof. D.B. Kshirsagar (H.O.D. Computer Engineering Department) and Prof. P. N. Kalvadekar (P. G.Cordinator) who has provided facilities to explore the subject with more enthusiasm. I express my immense pleasure and thankfulness to all the teachers and staff of the Department of Comp. Engg., S.R.E.S COE, and Kopargaon for their co-operation and support. Last but not the least, I thank all others, and especially my friends who in one way or another helped me.

6. REFERENCES

[1]. Xinpeng Zhang, 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.

[2]. N. A. Saleh, H. N. Boghdad, S. I. Shaheen, A. M. Darwish, " High Capacity Lossless Data Embedding Technique for Palette Images Based on Histogram Analysis," *Digital Signal Processing*, 20, pp. 1629–1636, 2010.

[3]. K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption," *IEEE Trans. Information Forensics & Security*, 8(3), pp. 553-562, 2013.

[4]. X. Zhang, "Commutative Reversible Data Hiding and Encryption," *Security and Communication Networks*, 6, pp. 1396–1403, 2013.

[5]X. Zhang, "Reversible Data Hiding with Optimal Value Transfer, IEEE Trans. On Multimedia, 15(2), 316?325, 2013.

[6] J. Fridrich, M. Goljan, P. Lisonek, and D. Soukal, " Writing on Wet Paper," IEEE Trans. Signal Processing, 53(10), pp. 3923-3935, 2005.

[7].W. Puech, M. Chaumont, and O. Strauss, " A Reversible Data Hiding Method for Encrypted Images," *Security, Forensics, Steganography, and Watermarking of Multimedia Contents X*, *Proc. SPIE*, 6819, 2008.

[8].X. Zhang, " Separable Reversible Data Hiding in Encrypted Image," *IEEE Trans. Information Forensics & Security*, 7(2), pp. 526–532, 2012.

[9].X. Zhang, "Reversible Data Hiding with Optimal Value Transfer," *IEEE Trans. on Multimedia*, 15(2), 316–325, 2013