International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 12
August 2016

A Study of Reversible and Lossless Data Hiding Techniques in Encrypted

B. Lakshmana Rao
PG Scholar
Department of CSE,
DIET, ANAKAPALLE, Visakhapatnam

A.A.Narasimham
Associate Professor,
Department of CSE,
DIET, ANAKAPALLE, Visakhapatnam

Abstract: *Reversible data hiding a novel technique which is used to embed additional information in the encrypted images, applies in military and medical images, which can be recoverable with original media and the hided data without loss. The distribution 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 lossless scheme, the cipher text pixels are replaced with new values 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. In the reversible scheme, a preprocessing is employed to shrink the image histogram before image encryption. 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. The cipher text pixels are replaced with the additional data into new values to embed several cipher text pixels by wet paper coding at multiple layer. From original image the embedded data can be extracted and the original image can be recovered from the decrypted image directly. The embedded data can directly be extracted from the encrypted domain. The decryption of original plaintext image doesn't affects data embedding operation. With the combined technique, before decryption a receiver may extract a part of embedded data, and recover the original plaintext image after decryption. A slight distortion is introduced due to the compatibility between the lossless and reversible schemes. The data embedding operations can be performed in the two manners simultaneously performed in an encrypted image and decrypted image.*

Keywords: Data hiding, Reversible data hiding, Image encryption, Image decryption, Histogram-Shrink, Difference- Expansion (DE), Plain-Text (PE), Cipher-Text (CT)

1. INTRODUCTION

Reversible data hiding was mainly proposed for authentication. At starting phase reversible algorithms have small embedding capacity and poor image quality. While the encryption techniques convert plaintext content into ciphertext, The data hiding techniques embed additional data into cover media by introducing small changes. In some distortion unacceptable cases, data hiding may be performed with a lossless or reversible manner. In number of cases of data hiding, the cover media will results some loss of original content due to data hiding and cannot be extracted back to the original cover media, because some permanent loss has occurred to the cover media even after the hidden data have been retrieved out. In some applications area, such as military, medical diagnosis, it is difficult to recover original content as well as original quality of image. There are different methodology are there of data embedding in reversible or lossless manner as, here pixels with the most used color in a palette image are assigned to some unused color indices for carrying the additional data, and these indices are redirected to the most used color. This way, although the indices of these pixels are altered, the actual colors of the pixels are kept unchanged. On the other hand, In cryptography, encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption denies the message content to the interceptor. Usually encryption is used when one needs to keep his/her data private. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, generating cipher text that can only be read if decrypted.

For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. Such an algorithm is necessary for the decryption of the message because without it, any party will be able to crack the code and access the data. Although for a well-designed encryption scheme, large computational resources and skill are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients, but not to unauthorized interceptors. The rapid development of data transfer through internet made it easier to send the data accurate and faster to the destination. There are many transmission media to transfer the data to destination like e-mails; at the same time it is may be easier to modify and misuse the valuable information through hacking. So, in order to transfer the data securely to the destination

Without any modifications, there are certain approaches like cryptography and steganography. Various instruments, for example, distinction extension, histogram shift and lossless pressure, have been utilized to build up the reversible information concealing systems for computerized pictures. As of late, a few decent forecast methodologies and ideal move likelihood under payload-mutilation measure have been acquainted with enhance the execution of reversible information covering up. 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].

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. 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. OVERVIEW OF THE PROJECT

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

.

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 homomorphism 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 homomorphism 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.

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.

4. PROBLEM DEFINITION

There are existing systems having the key tool for information hiding which is Vacating the room after encryption. It consists of problems such as, the extracted data may contain errors. If there is no availability of sufficient space then some data may be lost & that is why the data is missing at the receiver side which can be termed as data with error. Again the un-availability of memory space is a big problem. Some space is created at the time

of data embedding which is a time consuming process. After data extraction the image recovered does not contain the qualities of the original cover. Some distortions are introduced into the image. But it is possible in future that the quality may be improved as compared to existing system.

Data encryption using steganograph

Steganography was getting used in earlier days to send the data to the receiver. The symmetric key is used by both sender and receiver to encrypt and decrypt the data.

Disadvantage:

As same key is used by both sender and receiver there was highly chances to decrypt the data by the unauthorized person.

5. PROPOSED SYSTEM

The proposed scheme is made up of image encryption, data embedding and data-extraction/image-recovery phases. The content owner encrypts the original uncompressed image using an encryption key to produce an encrypted image. Then, the data-hider compresses the least significant bits (LSB) of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data. At the receiver side, the data embedded in the created space can be easily retrieved from the encrypted image containing additional data according to the data-hiding key. Since the data embedding only affects the LSB, a decryption with the encryption key can result in an image similar to the original version. When using both of the encryption and data-hiding keys, the embedded additional data can be successfully extracted and the original image can be perfectly recovered by exploiting the spatial correlation in natural image. Fig. 2 shows the three cases at the receiver side.

Here propose a new reversible data embedding technique, which can embed a large amount of data (5–80 kb for a 512 x 512 x 8 grayscale image) while keeping a very high visual quality for all natural images, specifically, the PSNR of the marked image versus the original image is guaranteed to be higher.

Image Encryption

Assume the original image is in uncompressed format and each pixel with gray value falling into [0, 255] is represented by 8 bits.

In encryption phase, the exclusive-or results of the original bits and pseudo-random bits are calculated

where ri,j,k are determined by an encryption key using a standard stream cipher. Then, B,i,j,k are concatenated orderly as the encrypted data. A number of secure stream cipher methods can be used here to ensure that anyone without the encryption key, such as a potential attacker or the data hider, cannot obtain any information about original content from the encrypted data.

Data Embedding

In the data embedding phase, some parameters are embedded into a small number of encrypted pixels, and the LSB of the other encrypted pixels are compressed to create a space for accommodating the additional data and the original data at the positions occupied by the parameters. The detailed procedure is as follows According to a data-hiding key, the data-hider pseudo-randomly selects Np encrypted pixels that will be used to carry the parameters for data hiding. In encryption phase, the exclusive-or results of the original bits and pseudo-random bits are calculated Here, Np is a small positive integer, for example, Np=20. The other (N-Np) encrypted pixels are pseudo-randomly permuted and divided into a number of groups, each of which contains L pixels. The permutation way is also determined by the data-hiding key.

Image Decryption

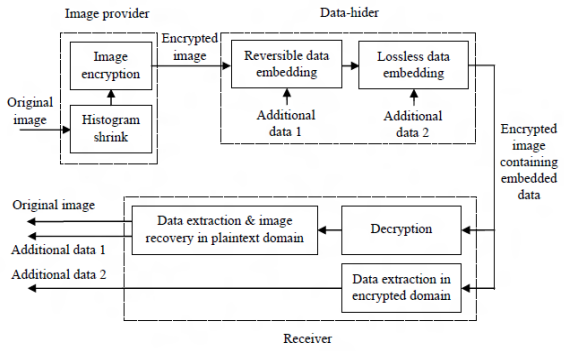
When having an encrypted image containing embedded data, a receiver firstly generates ri,j,k according to the encryption key, and calculates the exclusive-or of the received data and ri,j,k to decrypt the image. We denote the decrypted bits as b1i,j,k . Clearly, the original five most significant bits (MSB) are retrieved correctly. For a certain pixel, if the embedded bit in the block including the pixel is zero and the pixel belongs to S1, or the embedded bit is 1 and the pixel belongs to S0 , the data-hiding does not affect any encrypted bits of the pixel. So, the three decrypted LSB must be same as the original LSB, implying that the decrypted gray value of the pixel is correct. On the other hand, if the embedded bit in the pixel's block is 0 and the pixel belongs to S0, or the embedded bit is 1 and the pixel belongs to S1 , the decrypted LSB

Data Extraction

If the receiver has both the data-hiding, he may aim to extract the embedded data According to the data-hiding key, the values of M,L and S, the original LSB of the Np

selected encrypted pixels, and the (N-Np) * S/L - Np additional bits can be extracted from the encrypted image containing embedded data. By putting the Np LSB into their original positions, the encrypted data of the Np selected pixels are retrieved, and their original gray values can be correctly decrypted using the encryption keys. In the following, we will recover the original gray values of the other (N-Np) pixels This paper proposes a novel scheme for separable reversible data hiding in encrypted image. In the proposed scheme, the original image is encrypted using an encryption key and the additional data are embedded into the encrypted image using a data-hiding key. With an encrypted image containing additional data, if the receiver has only the data-hiding key, he can extract the additional data though he does not know the image content. If he has only the encryption key, he can decrypt the received data to obtain an image similar to the original one, but cannot extract the embedded additional data. If the receiver has both the data-hiding key and the encryption key, he can extract the additional data and recover the original image without any error when the amount of additional data is not too large.

6. EXPERIMENTAL RESULTS



Sketch of combined scheme

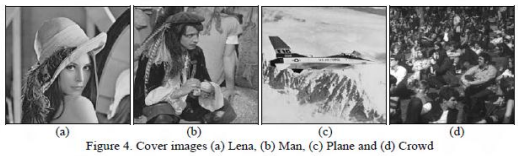


Figure 4. Cover images (a) Lena, (b) Man, (c) Plane and (d) Crowd

Table 1. Average payload of lossless scheme with respect to different K

K	1	2	3	4	5
Average embedding rate (bits per pixel) with Paillier cryptosystem	0.499	0.749	0.875	0.937	0.968

Figure 5. Directly decrypted Lena of reversible scheme (a) $\delta = 4$, a total of 4.6×10^4 bits embedded and PSNR = 40.3 dB, (b) $\delta = 7$, a total of 7.7×10^4 bits embedded and PSNR = 36.3 dB

7. 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. Original content recovery plays vital role in the secure communication and gives best result in field like medical, army..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. Data hiding irreversible manner in encrypted images is providing double security for confidential data by using techniques such as image encryption. 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. encrypted domain, and the data embedding operation does not affect the decryption of original plaintext image. In the reversible scheme, a preprocessing of histogram shrink is made before encryption, and a half of ciphertext pixel values are modified for data embedding. On receiver side, 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.

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

AUTHORS

B. Lakshmana Rao
PG Scholar
Department of CSE,
DIET, ANAKAPALLE,
Visakhapatnam

A.A.Narasimham
Associate Professor,
Department of CSE,
DIET, ANAKAPALLE,
Visakhapatnam