Data Hiding Techniques and Key Modulations in Encrypted Images

DUVVI NALINI TEJA[1], **DR. M. SAMPATH KUMAR**[2]

[1]PG Scholar, Dept of CS & SE, Andhra University, Visakhapatnam, AP, India.

[2]Associate Professor, Dept of CS & SE, Andhra University, Visakhapatnam, AP, 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.

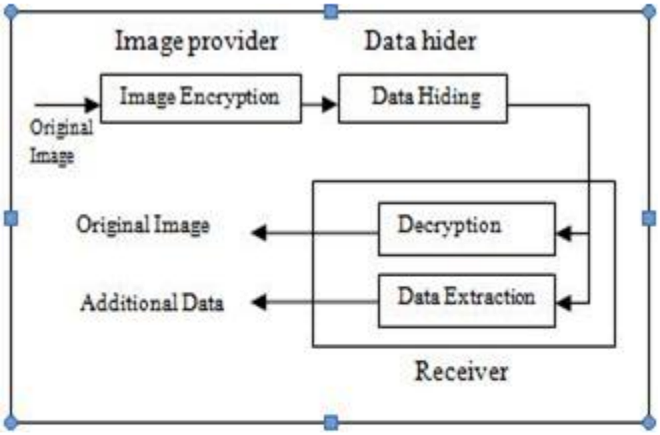


Fig.1 Sketch of lossless data hiding scheme

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.

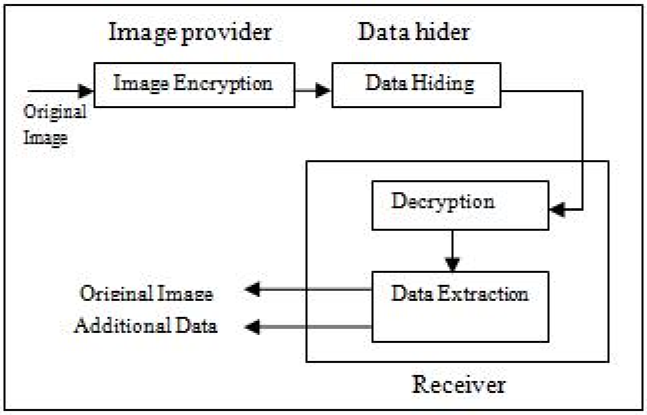


Fig.2 Sketch of reversible data hiding scheme

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.

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.

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

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..

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.

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

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.

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.

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.

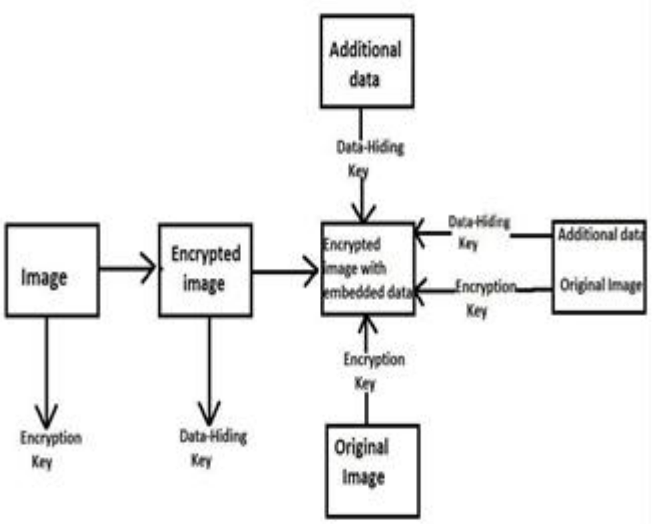
Wei Zhang and Xianfeng Zhao [11] have proposed the system that maintains the reversibility. This paper defines the reversible data-hiding in encrypted image by using spare space as reserving room before encryption. Here more attention on RDH technique which maintains the reversibility that means original cover recovered after embedding additional data. It provides the security and confidentiality to user.

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.

3. EXISTING TECHNIQUES

2.1 Reversible Data Hiding

Data hiding is the way of hiding information into a cover media. It requires two set of data that are embedded data and set of cover media data. In some case cover media distorted due to perform hiding operation but this type of changes are not acceptable by some applications such as medical imagery, military imagery and law-forensic etc. so that a novel method become more popular among the researches i.e. known as Reversible data hiding (RDH).It is the technique that perform lossless embedding operation and recover the origin after the extraction. If cover medium distorted permanently when hidden message have been removed. Original Image encrypted into image encryption by using the encryption-key algorithm at the side of image owner. After that in the data hider module we can embed some additional data with the use of data-hiding key, finally gets the encrypted image that containing additional data and that image require to decryption at the receiver side. This concept describe by following figure.



Reversible data hiding techniques can be generally classified into two frameworks

1. Vacate room after encryption
2. Reserve room before encryption

In the first framework, vacate room after encryption (VRAE), a content owner first encrypts the original image using a standard cipher with an encryption key. After producing the encrypted image, the content owner hands over it to a data hider (e.g., a database manager) and the data hider can embed some auxiliary data into the encrypted image by losslessly vacating some room according to a data hiding key. Then a receiver, maybe the content owner himself or an authorized third party can extract the embedded data with the data hiding key and further recover the original image from the encrypted version according to the encryption key.

In the second framework, reserve room before encryption (RRBE), the content owner first reserve enough space on original image and then converts the image into its encrypted version with the encryption key. Now, the data

embed ding process in encrypted images is inherently reversible for the data hider only needs to accommodate data into the spare space previous emptied out. The data extraction and image recovery are identical to that of Framework VRAE. Obviously, standard RDH algorithms are the ideal operator for reserving room before encryption and can be easily applied to Framework RRBE to achieve better performance customary idea is followed in which the redundant image content is losslessly compressed and then encrypts it with respect to protecting privacy.

4. OVERVIEW OF PROPOSED METHOD

Problem and some space created at the time of embedding. So this is also time consuming process. After extracting the data we cannot achieve the originality. Some distortion exists in the system. So our aim is to remove this type of distortion form the system. There are lots of problems in the existing system. So objective is to recover the problems in future, which are described below:

- The extracted data may contain error.
- Time-consuming process.
- Availability of memory space.
- The key contents are not store of original image.

These entire problem recovered by using the concept of “Reserving Room Before encryption (RRBE)”. With the use of VRAE concept with cannot achieve original data after encryption. So that new concept used for achieve this property i.e. RRBE. The proposed system extracted data losslessly after encryption.

5. REVERSIBLE DATA HIDING IN ENCRYPTED IMAGES BY RESERVING ROOM BEFORE ENCRYPTION

In this framework, a customary idea is followed in which the redundant image content is losslessly compressed and then encrypts it with respect to protecting privacy. RRBE primarily consists of four stages:

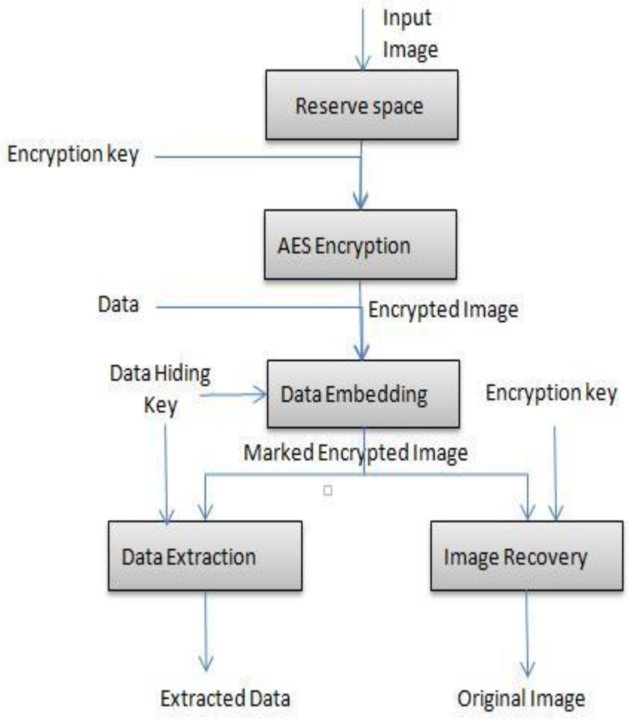
- Generation of encrypted image.
- Data hiding in encrypted image.
- Data extraction.
- Image recovery

5.1 GENERATION OF ENCRYPTED IMAGES

Actually, to construct the encrypted image, the first stage can be divided into three steps:

- Image partition
- Self-reversible embedding
- 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.



5.2 DATA HIDING IN ENCRYPTED IMAGE

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 locating the encrypted version of A, denoted by . Since has been rearranged to the top of E, it is effortless for the data hider to read 10 bits information in LSBs of first 10 encrypted pixels. After knowing how many bit-planes and rows of pixels he can modify, the data hider simply adopts 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 and further encrypts according to the data hiding key to formulate marked encrypted image denoted by E'. Anyone who does not possess the data hiding key could not extract the additional data.

5.3 DATA EXTRACTION AND IMAGE RECOVERY

1) Case 1: Extracting Data from Encrypted Images: To manage and update personal information of images which are encrypted for protecting clients' privacy, an inferior database manager may only get access to the data hiding key and have to manipulate data in encrypted domain. The order of data extraction before image decryption guarantees the feasibility of this work in this case. When the database manager gets the data hiding key, he can decrypt the LSB-planes of and extract the additional data by directly reading the decrypted version. When requesting for updating information of encrypted images, the database manager, then, updates information through LSB replacement and encrypts updated information according to the data hiding key all over again. As the whole process is entirely operated on encrypted domain, it avoids the leakage of original content.

2) Case 2: Extracting Data from Decrypted Images: In Case 1, both embedding and extraction of the data are manipulated in encrypted domain. On the other hand, there is a different situation that the user wants to decrypt the image first and extracts the data from the decrypted image when it is needed. The following example is an application for such scenario. Assume Alice outsourced her images to a cloud server, and the images are encrypted to protect their contents. Into the encrypted images, the cloud server marks the images by embedding some notation, including the identity of the images' owner, the identity of the cloud server and time stamps, to manage the encrypted images. Note that the cloud server has no right to do any permanent damage to the images. Now an authorized user, Bob who has been shared the encryption key and the data hiding key, downloaded and decrypted the images. Bob hoped to get marked decrypted images, i.e., decrypted images still including the notation, which can be used to trace the source and history of the data. The order of image decryption before/without data extraction is perfectly suitable for this case.

6. EXPERIMENTAL STUDY

Data Hiding For JPEG Images

This paper proposes a lossless data hiding technique for JPEG images based on histogram pairs. It embeds data into the JPEG quantized 8x8 block DCT coefficients and can achieve good performance in terms of PSNR versus payload through manipulating histogram pairs with optimum threshold and optimum region of the JPEG DCT coefficients. It can obtain higher payload than the prior arts. In addition, the increase of JPEG file size after data embedding remains unnoticeable. These have been verified by our extensive experiments.

Digital Image Water Marking

Watermarking, which belong to the information hiding field, has seen a lot of research interest recently. There is a lot of work begin conducted in different branches in this field. Steganography is used for secret communication, whereas watermarking is used for content protection, copyright management, content authentication and tamper Detection. In this paper we present a detailed survey of existing and newly proposed stenographic and

Watermarking techniques. We classify the techniques based on different domains in which data is embedded.

Digital Image steganography In simple words, Steganography can be defined as the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. Though the concept of steganography and cryptography are the same, but still steganography differs from cryptography. Cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret. Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected purpose of steganography is partly defeated The strength of steganography can thus be amplified by combining it with cryptography. Reversible Data hiding In Encrypted Image This work proposes a novel reversible data hiding scheme for encrypted image. After encrypting the entire data of an uncompressed image by a stream cipher, the additional data can be embedded into the image by modifying a small proportion of encrypted data. With an encrypted image containing additional data, one may firstly decrypt it using the encryption key, and the decrypted version is similar to the original image. According to the data-hiding key, with the aid of spatial correlation in natural image, the embedded data can be successfully extracted and the original image can be perfectly recovered.

Lossless Compression

The feasibility of lossless compression of encrypted images has been recently demonstrated by relying on the analogy with source coding with side information at the decoder. However previous works only addressed the compression of bi-level images, namely sparse black and white images, with asymmetric probabilities of black and white pixels. In this paper we investigate the possibility of compressing encrypted grey level and color images, by decomposing them into bit-planes. A few approaches to exploit the spatial and cross-plane correlation among pixels are discussed, as well as the possibility of exploiting the correlation between color bands. Some experimental results are shown to evaluate the gap between the proposed solutions and the theoretically achievable performance.

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. 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.

Future enhancement

The lossless compression method is used for the encrypted image containing embedded data, the additional data can be still extracted and the original content can be also recovered since the lossless compression does not change the content of the encrypted image containing embedded data. this method cab be applied for videos and can be embed message in to video with out loss of video content. Can be applied in networking and the keys are sent and received securely.

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

Author's Profile:

D.Nalini Teja,

pursuing her M.Tech in the department of Computer Science and Engineering, Andhra University College of Engineering, Visakhapatnam, A.P., India.

Dr.M.Sampath Kumar, B.E.(EEE), M.E. (Comp.Engg.), Ph.D.

Working as associate professor in the department of Computer Science and Systems Engineering, Andhra University, Visakhapatnam, AP India.

His research fields are in Cryptography, Algorithms, Data Security, Microcomputers