A Novel method by using reserving room before Encryption with a traditional RDH algorithm

L.Suresh, T. Sahana Edwin

Department of CSE, CMR College of Engineering and Technology, Telangana- India

Abstract- **Recently, more and more attention is paid to reversible data hiding (RDH) in encrypted images, since it maintains the excellent property that the original image cover can be losslessly recovered after which is embedded is extracted while protecting the image content's as confidential. All methods used previously embed data by reversibly vacating room from the images which are been encrypted, which may cause some errors on data extraction and/or image restoration. In this paper, we propose a novel method by reserving room before encryption with a traditional RDH algorithm, and thus it becomes easy for the data hider to reversibly embed data in the encrypted image. The proposed method can achieve real reversibility, that is, data extraction and image recovery are free of any error. Experiments show that this novel method can embed larger payloads for the same image quality as the previously used met*hods, such as for PSNR in dB.***

Index Terms- **Reversible data hiding, privacy protection, histogram shift, image encryption**

I. INTRODUCTION

Reversible data hiding (RDH) in images is a technique, by which the original cover can be Losslessly recovered after the embedded message is extracted. This important technique is widely used in medical imagery, military imagery and law forensics, where no distortion of the original cover is allowed. Since first introduced, RDH has attracted considerable research interest [1]. Kalker and Willems [2] established a rate-distortion model for RDH, through which they proved the rate-distortion bounds of RDH for memory less covers and proposed a recursive code construction which, however, does not approach the bound. Some attempts on RDH in encrypted images have been made.As when data is embedded into the image then there is occurrence of distortion in an image. So it is expected that after the data extraction the image quality should be maintained like the original image. But that image contains some distortions. With regard of distortion in image, Kalker and Willems[1] established a rate-distortion copy for RDH ,through which they showed the rate-distortion bounds of RDH for without memory covers and proposed a recursive code development which, however, does not move towards the bound [3]. Zhang et al. recovered the recursive code development for binary covers and proved that this development can gain the rate-distortion bound as long as the compacting algorithm reaches entropy, which launches the correspondence between data compression and RDH for binary covers [5].

A more popular method is based on difference expansion (DE), in which the difference of each pixel group is expanded, e.g., multiplied by 2, and thus the least significant bits (LSBs) of the difference are all zero and can be used for embedding messages. So in this way the additional data can be embedded into the covering media which is an improvement to the existing methods [6].

In 2007, Thodi and Rodriguez proposed a very different method by expanding the prediction errors. Because the prediction error is usually smaller than the difference between two consecutive pixel values, the stego image quality obtained by their method is better than that of Tian's method. However, Thodi and Rodriguez's method is also based on expansion-embedding technique, a larger distortion may occur; therefore, their method is not suitable for applications requiring high quality images.

II. REVERSIBLE DATA HIDING (RDH)

Reversible data hiding in images is a technique that hides data in digital images for secret communication. It is a technique to hide additional message into cover media with a reversible manner so that the original cover content can be perfectly restored after extraction of the hidden message. Traditionally, data hiding is used for secret communication. In some applications, the embedded carriers are further encrypted to prevent the carrier from being analyzed to reveal the presence of the embedment. Other applications could be for when the owner of the carrier might not want the other person, including data hider, to know the content of the carrier before data hiding is actually performed, such as military images or confidential medical images. In this case, the content owner has to encrypt the content before passing to the data hider for data embedment. The receiver side can extract the embedded message and recover the original image. Many reversible data hiding methods have been proposed recently .As is well known, encryption is an effective and popular means of privacy protection. In order to securely share a secret image with other person, a content owner may encrypt the image before transmission. In some application scenarios, an inferior assistant or a channel administrator hopes to append some additional message, such as the origin information, image notation or authentication data, within the encrypted image though he does not know the original image content. For example, when medical images have been encrypted for protecting the patient privacy, a database administrator may aim to embed the personal information into the corresponding encrypted images.

It may be also hopeful that the original content can be recovered without any error after decryption and retrieve of additional message at receiver side. Traditionally, data hiding is used for secret communication. In some applications, the embedded carriers are further encrypted to prevent the carrier from being analyzed to reveal the presence of the embedment. Other applications could be for when the owner of the carrier might not want the other person, including data hider, to know the content of the carrier before data hiding is actually performed, such as military images or confidential medical images.

In this case, the content owner has to encrypt the content before passing to the data hider for data embedment. The receiver side can extract the embedded message and recover the original image. A major recent trend is to minimize the computational requirements for secure multimedia distribution by selective encryption where only parts of the data are encrypted. There are two levels of security for digital image encryption: low level and high-level security encryption. In low-level security encryption, the encrypted image has degraded visual quality compared to that of the original one, but the content of the image is still visible and understandable to the viewers. In the high-level security case, the content is completely scrambled and the image just looks like random noise. In this case, the image is not understandable to the viewers at all. Selective encryption aims at avoiding the encryption of all bits of a digital image and yet ensuring a secure encryption.

Reversible data hiding is a technique to embed additional message into some distortion-unacceptable cover media, such as military or medical images, with a reversible manner so that the original cover content can be perfectly restored after extraction of the hidden message. As an effective and popular means for privacy protection, encryption converts the ordinary signal into incomprehensible data, so that the general signal processing typically takes place before encryption or after decryption. However, in some circumstances that a content owner does not trust the service provider, the ability to manipulate the encrypted data when keeping the plain content secret is desired. When the secret data to be transmitted are encrypted, a channel provider without any knowledge of the cryptographic key may compress the encrypted data due to the limited channel resource. Encryption is an effective means of privacy protection. To share a secret image with other person, a content owner may encrypt the image before transmission. In some cases, a channel administrator needs to add some additional message, such as the origin information, image notation or authentication data, within the encrypted image however he does not know the original image content. It may be also expected that the original content can be recovered without any error after decryption and retrieve of additional message at receiver side. That means a reversible data hiding scheme for encrypted image is desirable. Data hiding is referred to as a process to hide data (representing some information) into cover media. That is, the data hiding process links two sets of data, a set of the embedded data and another set of the cover media data.

In most cases of data hiding, the cover media becomes distorted due to data hiding and cannot be inverted back to the original media. That is, cover media has permanent distortion even after the hidden data have been removed. In some applications, such as medical diagnosis and law enforcement it is desired that the original cover media can be recovered efficiently with no loss. The marking techniques satisfying this requirement are referred to as reversible, lossless, distortion-free or invertible data hiding techniques. Performance of a reversible data-embedding algorithm Reversible data embedding, which is also called lossless data embedding, embeds invisible data (which is called a payload) into a digital image in a reversible fashion. As a basic requirement, the quality degradation on the image after data embedding should be low. An exciting feature of reversible data embedding is the reversibility, that is, one can remove the embedded data to restore the original image. Reversible data embedding hides some information in a digital image in such a way that an authorized party could decode the hidden information and also restore the image to its original state. The performance of a reversible data-embedding algorithm can be measured by the following

Payload capacity limit

Visual quality

Complexity

The distortion- free data embedding is the motivation of reversible data embedding. Data will certainly change the original content by embedding some data into it. Even a very slight change in pixel values may not be desirable, especially in sensitive imagery, such as military data and medical data. In such a scenario, every bit of information is important. From the application point of view, since the difference between the embedded image and original image is almost unnoticeable from human eyes, reversible data embedding could be thought as a secret communication channel since reversible data embedding can be used as an information carrier.

III. DATA HIDING IN IMAGES BY RESERVING ROOM BEFORE ENCRYPTION

Here we are investigating the data hiding technique which is reversible in nature. Thus it is termed as Reversible data hiding technique. Using the encrypted image as a cover data in which the data is embedded. In separable reversible data hiding technique firstly a content owner encrypts the original uncompressed image then a data hider compress the image to create space to accommodate some additional data. At the receiver side there are three possibilities to retrieve the embedded data and get covering data; this is the basic theme of this concept.

Reversible data hiding is a technique to embed additional message into some distortion-unacceptable cover media, such as military or medical images, with a reversible manner so that the original cover content can be perfectly restored after extraction of the hidden message. As an effective and popular means for privacy protection, encryption converts the ordinary signal into incomprehensible data, so that the general signal processing typically takes place before encryption or after decryption.

However, in some circumstances that a content owner does not trust the service provider, the ability to manipulate the encrypted data when keeping the plain content secret is desired. When the secret data to be transmitted are encrypted, a channel provider without any knowledge of the cryptographic key may compress the encrypted data due to the limited channel resource.

Data hiding is referred to as a process to hide data (representing some information) into cover media. That is, the data hiding process links two sets of data, a set of the embedded data and another set of the cover media data. In most cases of data hiding, the cover media becomes distorted due to data hiding and cannot be inverted back to the original media. That is, cover media has permanent distortion even after the hidden data have been removed. In some applications, such as medical diagnosis and law enforcement it is desired that the original cover media can be recovered efficiently with no loss. The marking techniques satisfying this requirement are referred to as reversible, lossless, distortion free or invertible data hiding techniques.

As name itself indicates that it is the reversible data technique but which is separable. The separable means which is able to separate .In other words, we can separate the some things, activities using suitable criteria. Here in separable reversible data hiding concept. The separation of activities i.e. extraction of original cover image and extraction of payload (data which was embedded).This separation requires some basic cause to occur. In separable data hiding key the separation exists according to keys.

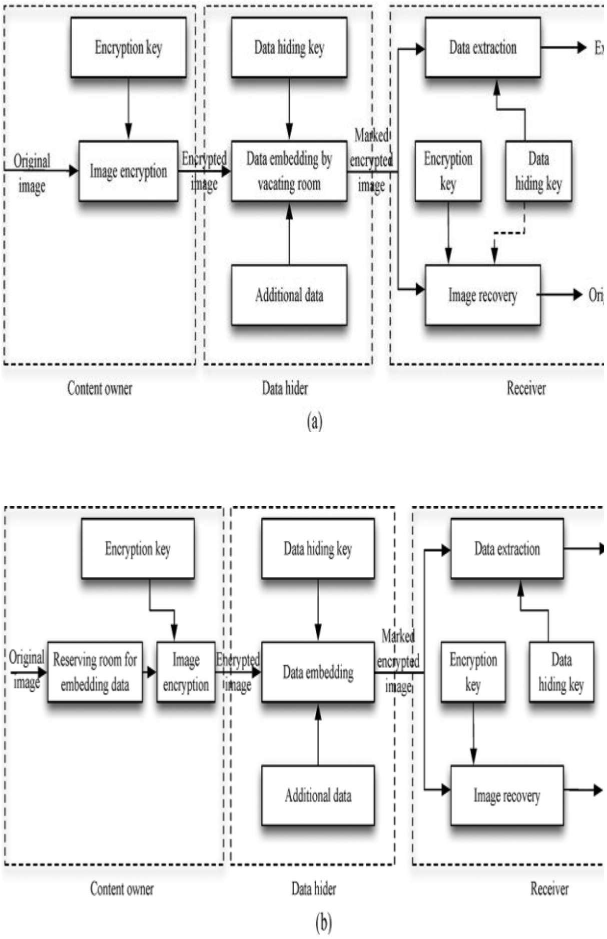

Fig. 1.Framework: "vacating room after encryption (VRAE)" versus framework: "reserving room before encryption (RRBE)." (Dashed line in (a) states that the need of data hiding key in image recovery varies in different practical methods). (a) Framework VRAE. Thus here gives same importance for both image and data. (b) Framework RRBE.

Here at the receiver side, there are three different cases are encountered. The separation of extracting the data and getting the cover media come to be exists.

That's why it is called as Separable Reversible Data hiding. Here I am investigating a hardware implementation of data hiding technique, which is reversible in nature.

There are several methods for data hiding in images available now. But most of them are not reversible in nature. Here in this paper we propose a method to achieve pure recovery of image and data.

In the Existing System, Vacating Room after Encryption technique is following. Since lossless vacating room from the encrypted images is relatively difficult and sometimes inefficient, why are we still so obsessed to find novel RDH techniques working directly for Encrypted Images.

In proposed method can achieve real reversibility, that is, data extraction and image recovery are free of any error. If we reverse the order of encryption and vacating room, i.e., reserving room prior to image encryption at content owner side, the RDH tasks in encrypted images would be more natural and much easier which leads us to the novel framework, "reserving room before encryption (RRBE)". Not only does the proposed method separate data extraction from image decryption but also achieves excellent performance in two different prospects.

Real reversibility is realized, that is, data extraction and image recovery are free of any error

For given embedding rates, the PSNRs of decrypted image containing the embedded data are significantly improved; and for the acceptable PSNR, the range of embedding rates is greatly enlarged.

A. Encrypted Image Generation

In this module, to construct the encrypted image, the first stage can be divided into two steps. Image Partition and Self Reversible Embedding followed by image encryption. At the beginning, image partition step divides original image into two parts and then, the LSBs of are reversibly embedded into with a standard RDH algorithm so that LSBs of 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 module, a content owner 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 lossless 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.

C. Data extraction and image recovery

In this module, 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. When the database manager gets the data hiding key, he can decrypt 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 up dated 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.

D. Data extraction and image restoration

Data extraction and Image recovery takes place at receiver side. using data hiding key receiver can extract the data where using encryption key he can extract the original image.

In this module, after generating the marked decrypted image, the content owner can further extract the data and recover original image. Reversible hiding allows extraction of the original host signal and also the embedded message. There are two important requirements for reversible data hiding techniques: the embedding capacity should be large; and distortion should be low. These two requirements conflict with each other. In general, a higher embedding capacity results in a higher degree of distortion. An improved technique embeds the same capacity with lower distortion or vice versa.

IV. SEPARABLE REVERSIBLE DATA HIDING

As name itself indicates that it is the reversible data technique but which is separable. The separable means which is able to separate .In other words, we can separate the some things, activities using suitable criteria. Here in separable reversible data hiding concept. The separation of activities i.e. extraction of original cover image and extraction of payload (data which was embedded).This separation requires some basic cause to occur. In separable data hiding key explained by Xin Peng Zhang the separation exists according to keys. Here at the receiver side, there are three different cases are encountered. The separation of extracting the data and getting the cover media come to be exists. That's why it is called as Separable Reversible Data hiding.

A. Compression

Compression of encrypted data has become considerable research interest in recent years. The traditional way of securely and efficiently transmitting redundant data is to first compress the data to reduce the redundancy, and then to encrypt the compressed data to mask its meaning. At the receiver side, the decryption and decompression operations are orderly performed to recover the original data. However, in some application scenarios, a sender needs to transmit some data to a receiver and hopes to keep the information confidential to a network operator who provides the channel resource for the transmission. That means the sender should encrypt the original data and the network provider tend to compress the encrypted data without any knowledge of the cryptographic key and the original data. There are several techniques for compressing/decompressing encrypted data have been developed. This paper a presented lossy compression method in which an encrypted grey image can be efficiently compressed by discarding the excessively rough and _ne information of coefficients generated from orthogonal transform. When having the compressed data, a receiver may reconstruct the principal content of original image by retrieving the values of coefficients.

A pseudorandom permutation is used to encrypt an original image, and the encrypted data are efficiently compressed by discarding the excessively rough and fine information of coefficients generated from orthogonal transform. After receiving the compressed data, with the aid of spatial correlation in natural image, a receiver can reconstruct the principal content of the original image by iteratively updating the values of coefficients. This way, the higher the compression ratio and the smoother the original image, the better the quality of the reconstructed image. The compression ratio and the quality of reconstructed image vary with different values of compression parameters. In the encryption phase of the Zhangs system, only the pixel positions are shuffled and the pixel values are not masked. With the values of elastic pixels, the coefficients can be generated to produce the compressed data.

V. RESULTS

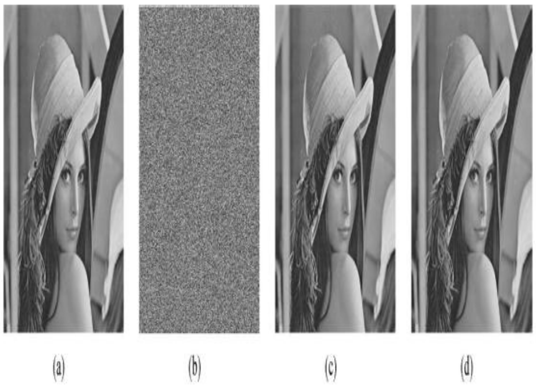

Fig.2. (a) Original image, (b) encrypted image, (c) decrypted image containing messages (embedding rate 0.1 bpp), (d) recovery version.

VI. CONCLUSION

Reversible data hiding in encrypted images is a new topic drawing attention because of the privacy-preserving requirements from cloud data management. In previous methods RDH process was implemented in encrypted images by vacating room after encrypting the image, as opposed to which we proposed by reserving room before encrypting the image. Hence, the data hider can have advantage of the extra space emptied out in previous stage will make the data hiding process much effortless. This 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 gain separate data extraction, real reversibility and greatly improvement on the quality of marked decrypted images.

VII. REFERENCES

[1] Meenal V.Jagdale, Dr. Shubhalaxmi P. Hingway, Sheeja S. Suresh, "Reversible Encryption and Data Hiding", Volume 2, Issue 1, January 2014.

[2]. Kede Ma,Weiming Zhang, Xeianfeng Zhao, ”Reversible data hiding in encrypted images by reserving room before encryption” IEEE Trans. On information forensic and security, VOL. 8 NO.3 March 2013.

[3]. W. Zhang, B. Chen, and N. Yu, “Improving various reversible data hiding schemes via optimal codes for binary covers,” IEEE Trans. Image Process., vol. 21, no. 6, pp. 2991–3003,Jun. 2012.

[4]. W. Zhang, B. Chen, and N. Yu, “Capacity-approaching codes for reversible data hiding,” in Proc 13th Information Hiding (IH’2011) LNCS 6958, 2011, pp. 255–269, Springer Verlag.

[5]. T. Kalker and F.M. Willems, “Capacity bounds and code constructions for reversible data hiding,” in Proc. 14th Int. Conf. Digital Signal Processing (DSP2002), 2002, pp. 71–76.

[6]. X. L. Li, B. Yang, and T. Y. Zeng, “Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection, IEEE Trans. Image Process., vol. 20, no. 12, pp. 3524–3533, Dec. 2011.

[7]. L. Luo et al., “Reversible image watermarking using interpolation technique,” IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 187–193,Mar. 2010.

[8]. P. Tsai, Y. C. Hu, and H. L. Yeh, “Reversible image hiding scheme using predictive coding and histogram shifting,” Signal Process., vol.89, pp. 1129–1143, 2009.

BIO DATA

Author 1

L.Suresh currently pursuing his M.Tech, in CMR College of Engineering and Technology, Telangana- India.

Author 2

T. Sahana Edwin working as Asst.Prof Department of CSE, CMR College of Engineering and Technology, Telangana- India