A Comparative Study on Reversible Data Hiding in Encrypted Images using Various Frameworks

Sayeesh[#], Manjunath Kotari[&], Harish Kunder[$], Chanchal Antony[%]

*#PG Scholar, Dept. of CSE, Alva's Institute of Engineering & Technology, Mijar, Moodbidri (D.K), Karnataka,India *Professor & Head, Dept. of CSE, Alva's Institute of Engineering & Technology, Mijar, Moodbidri (D.K), Karnataka,India*

$Associate Professor, Dept. of CSE, Alva's Institute of Engineering & Technology, Mijar, Moodbidri (D.K), Karnataka,India

%Senior Asst. Professor, Dept. of CSE, Alva's Institute of Engineering & Technology, Mijar, Moodbidri (D.K), Karnataka, India

Abstract

We need more security for data transmission in computer networks. Nowadays most popularly we store and manage variety of data in cloud server. We need to protect the privacy of the data that is stored in cloud server. Many robust message encryption methods have been developed to such methods. Reversible data hiding in encrypted images is form of steganography in which we hide data within images. In this paper, we compare vacating room after encryption (VRAE), reserving room before encryption (RRBE) and reversible image transformation (RIT) frameworks for reversible data hiding in encrypted images. In the framework VRAE, the cloud server embeds data by losslessly vacating room from the encrypted images by using the idea of compressing encrypted images. In the framework RRBE, the image owner first empties out room by using reversible data hiding method in the plain images. After that, the image is encrypted and outsourced to the cloud and the cloud server can freely embed data into the reserved room of the encrypted image. RIT-based framework allows the user to transform the content of original image into the content of another target image with the same size. The transformed image, which looks like the target image, is used as the encrypted image and is outsourced to the cloud.

Keywords: *Reversible data hiding (RDH), vacating room after encryption (VRAE), reserving room before encryption (RRBE), reversible image transformation (RIT), image encryption, privacy protection*

I. INTRODUCTION

Communication is one of the most important needs of human beings. For communication purpose, most of the people are using different devices like mobile phones, phones, laptops etc. Most of these devices use certain network to make the communication easier. Device level security can be ensured by using facilities like setting passwords, biometric authentication schemes etc. But while coming to the network level security the most important challenge that world faces today is to ensure data security. Data security basically means protection of data from unauthorized users or hackers and providing high-level security to prevent data modification. The area of data security has gained more attention over the recent period of time due to the massive increase in data transfer rate over the internet. In order to improve the security features of data transfers over the internet, many techniques have been developed like steganography, digital watermarking and image cryptography.

The protection of these types of multimedia data can be done with the help of cryptographic techniques such as encryption and data hiding algorithms. While the encryption techniques convert plaintext content into unreadable ciphertext, the data-hiding techniques embed additional data into cover media by introducing slight modifications. In recent years, more attention is paid to reversible data hiding in images, since it maintains the excellent property that the recovered original cover image is lossless after embedded secret data is extracted. This important technique is widely used in military images, medical images and law forensics, where no distortion of original cover is allowed.

Data hiding techniques are required these days due to rapid development of internet. A large amount of data is transferred using internet. Data hiding is technique in which secret data is hidden in some cover media like image, audio, video files etc. Generally images are preferred cover media due to large transmission of images over internet. Two main types of data hiding techniques exist: Irreversible data hiding and Reversible data hiding. In case of irreversible data hiding at the extraction side only secret message is

recovered but in reversible data hiding both secret message and cover media is recovered without any distortion as shown in Fig 1. Thus data hiding is necessary for protection and authentication of data. When only protection of data is required, it is called steganography but when authentication of data is required, it is called watermarking. In some domains such as medical and military, even a slightest distortion is not acceptable so reversible data hiding (RDH) is required.

For RDH certain requirements need to be specified these are given as follows:

- Marked image quality: The marked image quality should be good. It means after embedding data in
- cover image the modification in cover image should be less. So that only intended recipient can detect the communication.
- Payload: Payload is number of bits that are hidden in the cover image. For effective RDH the payload should be high.
- Auxiliary information: It is the amount of information that is required to be sent at the extraction stage for perfect recovery of cover image and secret message. It should be as less as possible.
- Overflow/Underflow problem: This problem is observed in images while performing any mathematical computations when the pixel value increases than 255 or reduces than 0.Thus the pixel values should strictly lie in range (0,255).

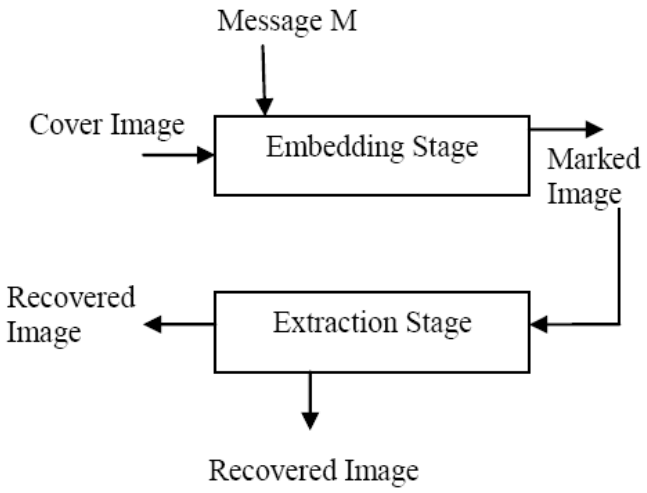

Fig. 1 Basic Reversible Data Hiding

Idea of reversible data hiding in encrypted images (RDH-EI) originates from reversible data hiding (RDH) in plaintext images [1], [2]. It is feasible in the applications, such as cloud storage and medical systems. In cloud storage, a content owner can encrypt an image to preserve his/her privacy, and upload the encrypted data onto cloud [3],[4]. On the cloud side, when managing huge amount of encrypted images, an administrator can embed additional messages (e.g., labels, time stamps, category information etc.) into the ciphertext. This embedding not only saves the storage overhead, but also provides a convenient way of searching encrypted images. On the recipient side, when a user downloads the encrypted data containing additional messages from the server, he/she can losslessly recover the original images after decryption.

Nowadays outsourced storage by cloud becomes a more and more popular service, especially for multimedia files, such as images or videos, which need large storage space. To manage the outsourced image, the cloud server may embed some additional data into the images, such as image category and notation information and use such data to identify the ownership [5] or verify the integrity of images. Obviously, the cloud service provider has no right to introduce permanent distortion during data embedding into the outsourced images. Therefore, reversible data hiding (RDH) technology is needed, by which the original image can be losslessly recovered after the embedded message is extracted.

II. RELATED WORK

In practical aspect, many RDH techniques have emerged in recent years. Fridrich et al. [6] constructed a general framework for RDH. By first extracting compressible features of original cover and then compressing them losslessly, spare space can be saved for embedding auxiliary data. A more popular method is based on difference expansion (DE) [7], 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. Another promising strategy for RDH is histogram shift (HS) [8], in which space is saved for data embedding by shifting the bits of histogram of gray values.

In [9], Hwang et al advocated a reputation-based trust-management scheme enhanced with data coloring (a way of embedding data into covers) and software watermarking, in which data encryption and coloring offer possibilities for upholding the content owner's privacy and data integrity. Obviously, the cloud service provider has no right to introduce permanent distortion during data coloring into encrypted data. Thus, a reversible data coloring technique based on encrypted data is preferred. Suppose a medical image database is stored in a data centre, and a server in the data centre can embed notations into an encrypted version of a medical image through a RDH technique. With the notations, the server can manage or

verify its integrity without having the knowledge of the original content, and thus the patient's privacy is protected. On the other hand, a doctor, having the cryptographic key, can decrypt and restore the image in a reversible manner for the purpose of further diagnosing.

Recently, Zhang *et al* proposed the optimal histogram modification algorithm [10], [16] for RDH by estimating the optimal modification probability [17],[18]. On the other hand, cloud service for outsourced storage makes it challenging to protect the privacy of image contents. For instance, recently many private photos of Hollywood actress leaked from iCloud. Although RDH is helpful for managing the outsourced images, it cannot protect the image content. Encryption is the most popular technique for protecting privacy. So it is interesting to implement RDH in encrypted images (RDH-EI), by which the cloud server can reversibly embed data into the image but cannot get any knowledge about the image contents. Inspired by the needs of privacy protection, many methods have been presented to extend RDH methods to encryption domain. From the viewpoint of compression, these methods on RDH-EI belong to three frameworks: Framework I "vacating room after encryption (VRAE)", Framework II "reserving room before encryption (RRBE)" and Framework III "reversible image transformation (RIT)".

III. THREE DIFFERENT FRAMEWORKS

The framework of vacating room after encryption (VRAE) is illustrated in Fig. 2. In this framework, 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 losslessly vacating some room according to a data hiding key. Then a receiver, may be 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 the encryption key. In VRAE, the original image is encrypted directly by the sender, and the data-hider embeds the additional bits by modifying some bits of the encrypted data. The idea was first proposed in [19], in which the owner encrypts the original image by Advanced Encryption Standard, and the data-hider embeds 1 bit in each block containing n pixels, meaning that the embedding rate is $1/n$ bpp. On the receiver side, data extraction and image recovery are realized by analyzing the local standard deviation during decryption of the marked encrypted image. This method requires that image decryption and data extraction operations must be done jointly. In other words, extraction and decryption are inseparable.

As shown in Fig. 3, in the framework of reserving 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 embedding 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 recovery are identical to that of framework VRAE. In this framework, the space for hiding data is reserved before the encryption of the image. Then the image is encrypted using an encryption key. The data-hider can hide data into the locations reserved for it using a data-hiding key. Since locations for additional data is identified before encryption, this framework can exploit the image characteristics to identify the suitable locations for additional data. Apart from that, this framework offers complete separability i.e., reserving room followed by image encryption can be done by one person and hiding additional data by a different person (similar as in the case of radiologist and database manager). This separability is possible in data extraction and image restoration also.

In the reversible image transformation (RIT) based framework as shown in Fig.4, the content owner encrypts the original image into another plaintext image using encryption key. The data hider embed/extract data into/from plaintext image using any classical RDH methods. The receiver extracts the embedded data from plaintext image using key to get the data. In reversible image transformation (RIT) framework, RIT transfers the semantic (content) of the original image I into the semantic of another image J. The word reversibility means that I can be losslessly restored from the transformed image; therefore RIT can be viewed as a special encryption scheme called "Semantic Transfer Encryption. In other words, the resultant transformed image which is also the encrypted image E(I) will look similar with J. The image J is selected to be irrelevant with I but has the same size of I and thus the content of the image I is protected. Because the "encrypted image" is in a form of plaintext, it will avoid the notation of the cloud server, and the cloud server can easily embed data into the "encrypted image" with traditional RDH methods for plaintext images.

IV. COMPARISON BETWEEN THREE FRAME WORKS

Fig. 5 depicts the comparison between three frameworks. In VRAE and RRBE frameworks, the user's images are stored in the form of ciphertext in the cloud account, while in the RIT-based framework the image is stored in a form of plaintext.

In the framework VRAE shown in Fig 5 (a), such as schemes in [20] and [21], the image owner (sender) encrypts the image I into E(I) with a key K. The cloud server embeds data by compressing the encrypted image E(I) and generates Ew(I) that is stored in the cloud. When getting a retrieval request, the cloud server returns E'w (I) to the receiver, may be an authorized third party, who generates I through a process of joint decompression and decryption with the key K. Herein, E'w(I) may be just Ew(I) or a modified version obtained by removing the embedded data. Note that the cloud server cannot restore E(I) from Ew(I), since decompression should be joined with decryption with the help of K. In this framework, the complexity is taken on by the receiver who must join the process of decompression and decryption to get the original image. In other words, the compression-based RDH method used by the cloud server should be specified together with the receiver, i.e. the RDH method is receiver-based.

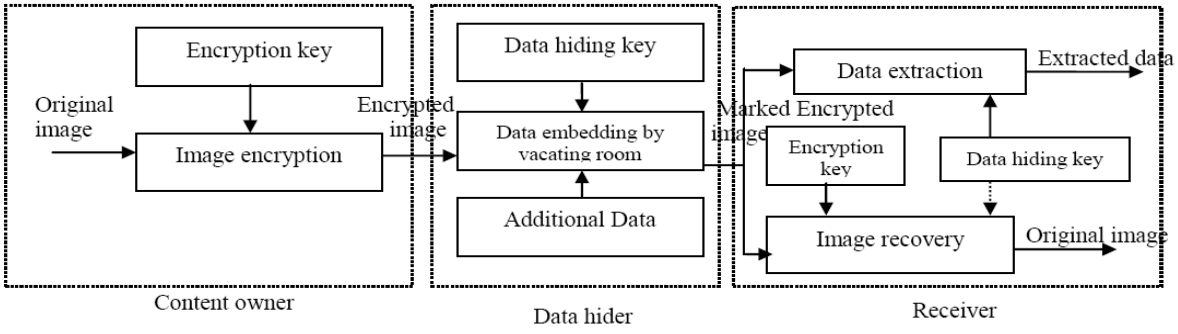

Fig.2 Framework VRAE

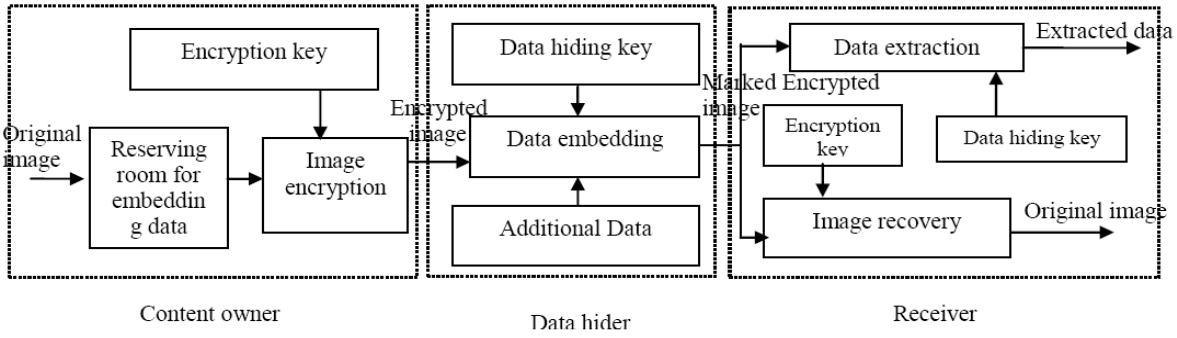

Fig. 3 Framework RRBE

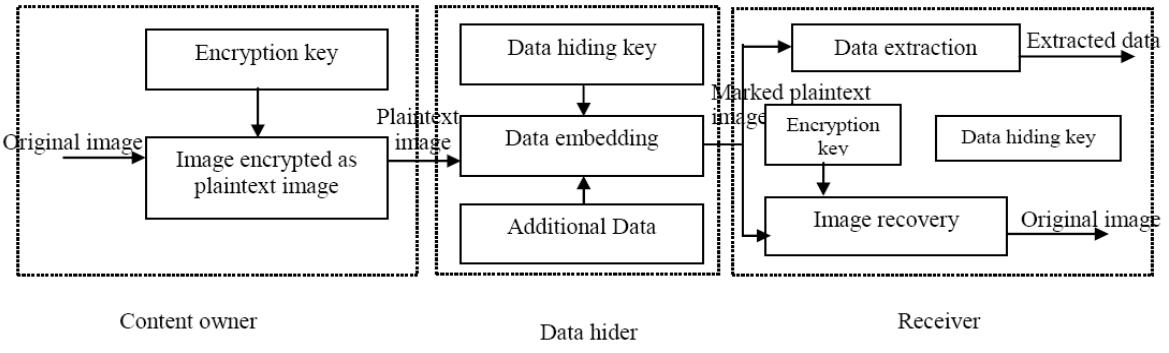

Fig. 4 Framework RIT

In the framework RRBE shown in Fig 5(b), such as schemes in [22],[23], the image owner (the sender) reserves room from image I and encrypts it into E(I) with a key K, and then sends it to the cloud server who embeds data into the reserved room and generates Ew(I). Ew(I) is stored in the cloud, from which the cloud server can extract the data that is used for management. When an authorized user (the receiver) wants to retrieve image, the cloud server can restore E(I) from Ew(I) and send E(I) to the user who can decrypt E(I) and get I with the key K. In the framework RRBE, the complexity is borne by the sender who

should reserve room for RDH by exploiting the redundancy within the image and thus the RDH method used by the cloud should be specified with the sender, that is, the RDH method used by cloud by cloud is sender-related.

In the RIT based framework depicted in Fig 5(c), the image I is "encrypted" into another plaintext image E(I) with a key K, so all images of the users, encrypted or not, will be stored in the cloud in the form of plaintexts. The cloud server can embed/extract data into/from E(I) with any classical RDH method for plaintext images. And E(I) can be recovered from

Extracted data

Marked Encrypted image

Original image

Receiver

Extracted data

Marked plaintext image

Original image

Receiver

the watermarked image Ew(I) by the cloud and sent back to the authorized user who anti-transforms it to get the original image I with the key K. The main advantages of RIT based framework is, the user can outsource the encrypted image to the cloud in a form of plaintext and thus it will avoid the attention of curious cloud and the cloud server can easily embed data into the encrypted image by selecting any one of the RDH methods for plaintext images. In other words, the RDH used by the cloud is irrelevant with both the sender and receiver, which is called a client-free RDH-EI scheme. "Client free" is important for the scenario of public clouds, in which it is hard for the cloud server to ask the clients how to encrypt or decrypt their data, because the cloud is thought to be only semi-honest.

V. CONCLUSION

In this paper we compared three different frameworks for RDH-EI. Reversible data hiding in encrypted images is a new topic drawing attention because of the privacy-preserving requirements from cloud data management.

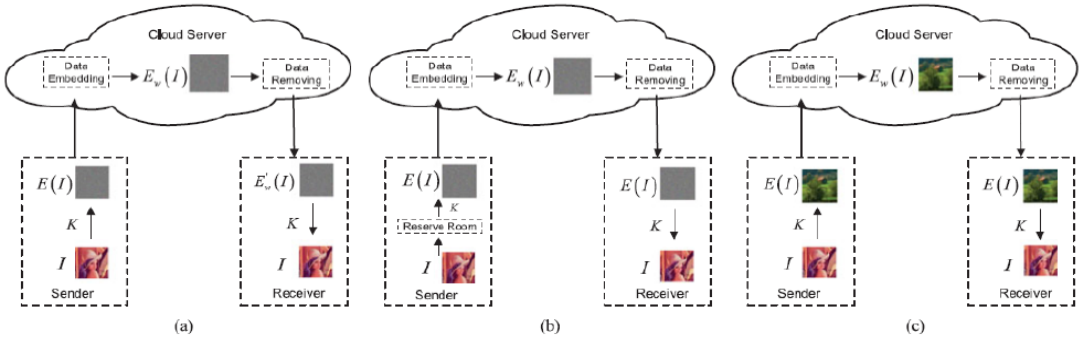

Fig.5 Comparison between three frameworks of RDH-EI. (a) Framework VRAE (b) Framework RRBE (c) RIT-based framework

For the VRAE framework, the data extraction and image recovering procedures are mainly accomplished by measuring the smoothness of the recovered image, thus they may suffer from incorrectly extraction of secret data and/or original image, and the embedding rate is relatively low. An RRBE framework suggests reserving spare space from the original image before encryption, and embedding the secret data into the reserved spare space. This framework can achieve real reversibility, separate data extraction and greatly improvement on the quality of marked decrypted images. In RIT-based framework, the semantic of original image to the semantic of another image and thus protect the privacy of the original image.

REFERENCES

[1] X. Hu, W. Zhang, X. Li, and N. Yu, "Minimum rate prediction and optimized histograms modification for reversible data hiding," IEEE Trans. Inf. Forensics Security, vol. 10, no. 3, pp. 653–664, Mar. 2015.

[2] X. Li, W. Zhang, B. Ou, and B. Yang, "A brief review on reversible data hiding: Current techniques and future prospects," in Proc. IEEE ChinaSummit Int. Conf. Signal Inf. Process., 2014, pp. 426–430.

[3] H. Wang, W. Zhang, and N. Yu, "Protecting patient confidential information based on ECG reversible data hiding," Multimedia Tools Appl.,vol. 75, no. 21, pp. 13733–13747, 2015, doi:10.1007/s11042- 015-2706-2

[4] Z. Fu et al., "Achieving efficient cloud search services: Multi-keyword ranked search over encrypted cloud data supporting parallel computing," IEICE Trans. Commun., vol. 98, no. 1, pp. 190–200, 2015.

[5] K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring," IEEE Internet Comput., vol. 14, no. 5, pp. 14–22, Sep./Oct.2010

[6] J. Fridrich and M. Goljan, "Lossless data embedding for all image formats," in Proc. SPIE Proc. Photonics West, Electronic Imaging, Securityand Watermarking of Multimedia Contents, San Jose, CA, USA,Jan. 2002, vol. 4675, pp. 572–583.

[7] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896,Aug. 2003.

[8] 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.