SURVEY ON REVERSIBLE DATA HIDING IN ENCRYPTED IMAGES

Ms.Fameela.K.A,Mrs. Najiya.A and Asst.prof.Mrs. Reshma.V.K
Department of Computer Science and Engineering
Nehru College of Engineering and Research Center, Pampady, Thrissur, Kerala.

Abstract: Reversible data hiding is a process to reverse the marked media back to the original cover media after the hidden data were extracted. In this technique information to be transferred is embedded into an encrypted image. Room reservation for data embedding can be done before or after image encryption. In this paper data hiding techniques were explained and compared based on room reservation.

Keywords: Reversible data hiding, image encryption

I. Introduction

Steganography is the art of concealing a message, image, or file within another message, image or file. Digital steganography and watermarking are the two kinds of data hiding technology to provide hidden communication and authentication. The goal of steganography is to hide a secret message inside harmless medium in such a way that it is not possible even to detect that there is a secret message. The medium for data hiding is also called as cover, host and carrier.

Since several years, the protection of multimedia data is becoming very important. Most multimedia data embedding techniques modify, and hence distort, the host signal in order to insert the additional information. Often, this embedding distortion is small, yet irreversible, i.e. it cannot be removed to recover the original host signal. In many applications, the loss of host signal fidelity is not prohibitive as long as original and modified signals are perceptually equivalent. The protection of this multimedia data can be done with encryption or data hiding algorithms. To decrease the transmission time, the data compression is necessary. Since few years, a new problem is trying to combine in a single step, compression, encryption and data hiding. So far, few solutions have been proposed to combine image encryption and compression for example. Nowadays, a new challenge consists to embed data in encrypted images. However, in a number of domains -such as military, legal and medical imaging- although some embedding distortion is admissible, permanent loss of signal fidelity is undesirable. This highlights the need for Reversible (Lossless) Data Embedding techniques.

The block diagram of RDH is shown in Fig.1.a. Reversible steganography or watermarking can restore the original carrier without any distortion or with ignorable distortion after the extraction of hidden data. So reversible data hiding is now getting popular. In this paper two important frameworks for reversible data hiding techniques in digital images are explained.

Reversible data hiding techniques can be generally classified into two frameworks

- Vacate room after encryption
- 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. This framework is illustrated in figure 1.b.

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

ISSN: 2278 – 7798

compared with techniques from Framework VRAE. This is because in this new framework, a

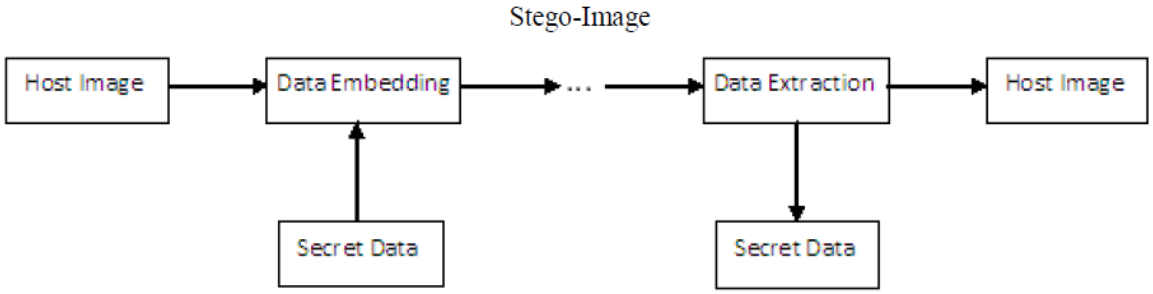

Figure 1.a

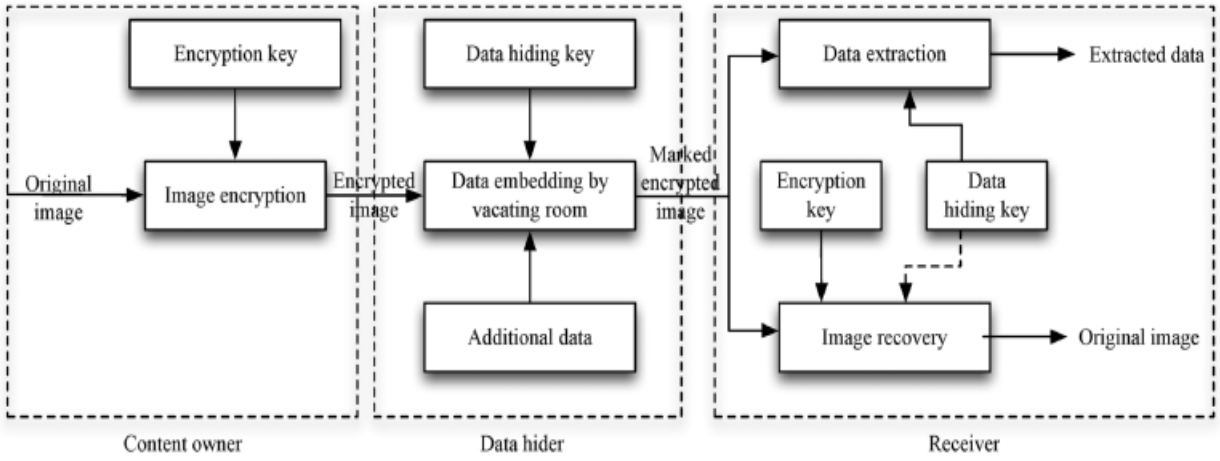

Figure 1.b

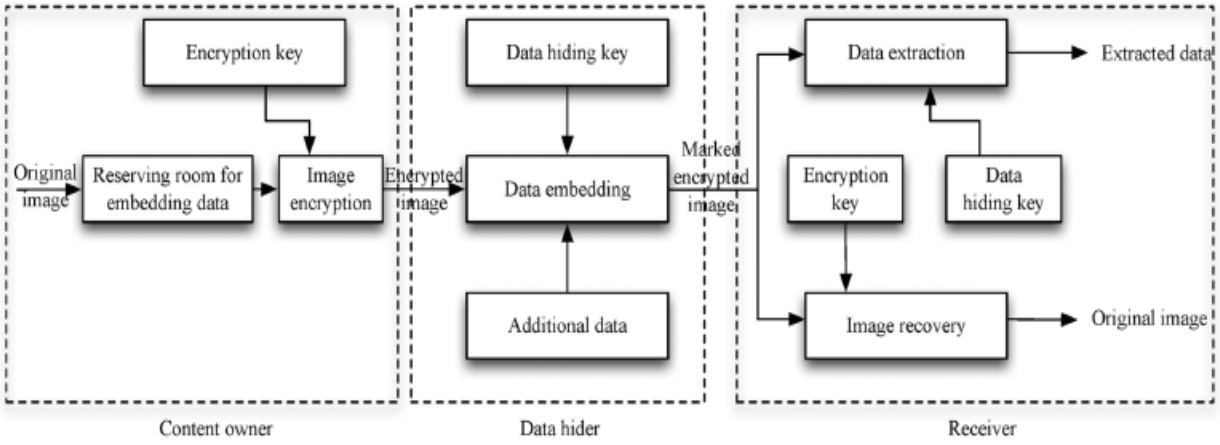

Figure 1.c

customary idea is followed in which the redundant image content is losslessly compressed and then encrypts it with respect to protecting privacy. This framework is illustrated in figure 1.c [1]

II. Related Work

Data hiding 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. The relationship between these two sets of data characterizes different applications. For instance, in covert communications, the hidden data may often be irrelevant to the cover media. In

ISSN: 2278 – 7798

authentication, however, the embedded data are closely related to the cover media. In these two types of applications, invisibility of hidden data is an important requirement. In most cases of data hiding, the cover media will experience some distortion due to data hiding and cannot be inverted back to the original media. That is, some permanent distortion has occurred to the cover media even after the hidden data have been extracted out. In some applications, such as medical diagnosis and law enforcement, it is critical to reverse the marked media back to the original cover media after the hidden data are retrieved for some legal considerations. In other applications, such as remote sensing and high energy particle physical experimental investigation, it is also desired that the original cover media can be recovered because of the required high-precision nature. The marking techniques satisfying this requirement are referred to as reversible, lossless, distortion-free, or invertible data hiding techniques. Reversible data hiding facilitates immense possibility of applications to link two sets of data in such a way that the cover media can be losslessly recovered after the hidden data have been extracted out, thus providing an additional avenue of handling two different sets of data.[1]

A number of reversible data hiding methods have been proposed in recent years. In difference expansion method, differences between two adjacent pixels are doubled to generate a new least significant bit (LSB) plane for accommodating additional data. A data hider can also perform reversible data hiding using a histogram shift mechanism, which utilizes the zero and peak points of the histogram of an image and slightly modifies the pixel grey values to embed data into the image. Another kind of method makes use of redundancy in a cover by performing lossless compression to create a spare space for data embedding. Furthermore, various skills have been introduced into the typical reversible data hiding approaches to improve the performance.

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. That means a reversible data hiding scheme for encrypted image is desirable.

In some existing joint data hiding and encryption schemes, a part of cover data is used to carry the additional message and the rest data are encrypted. For example, the intra prediction mode, motion vector difference and signs of DCT coefficients are encrypted, while a watermark is embedded into the amplitudes of DCT coefficients. In, the cover data in higher and lower bit-planes of transform domain are respectively encrypted and watermarked. In, the content owner encrypts the signs of host DCT coefficients and each content-user uses a different key to decrypt only a subset of the coefficients, so that a series of versions containing different fingerprints are generated for the users. In these joint schemes, however, only a partial encryption is involved, leading to a leakage of partial information of the cover. Furthermore, the separation of original cover and embedded data from a watermarked version is not considered. Each sample of a cover signal is encrypted by a public-key mechanism and a homo morphic property of encryption is exploited to embed some additional data into the encrypted signal. But the data amount of encrypted signal is significantly expanded and the computation complexity is high. Also, the data embedding is not reversible.

A novel reversible data hiding scheme for encrypted image, consists of three stages, image encryption, data embedding and data-extraction/image-recovery phases. The data of original cover are entirely encrypted, and the additional message is embedded by modifying a part of encrypted data. At receiver side, with the aid of spatial correlation in natural image, the embedded data are successfully extracted while the original image is perfectly recovered.

A content owner encrypts the original uncompressed image using an encryption key to produce an encrypted image, and then a data- hider embeds additional data into the encrypted image using a data-hiding key though he does not know the original con- tent. With an encrypted image containing additional data, a receiver may firstly decrypt it using the encryption key, and the decrypted version is similar to the original image. According to the data-hiding key, he can further extract the embedded data and recover the original image from the decrypted version. This method of sequential reversible data hiding is illustrated in figure2.a.[2]

ISSN: 2278 – 7798

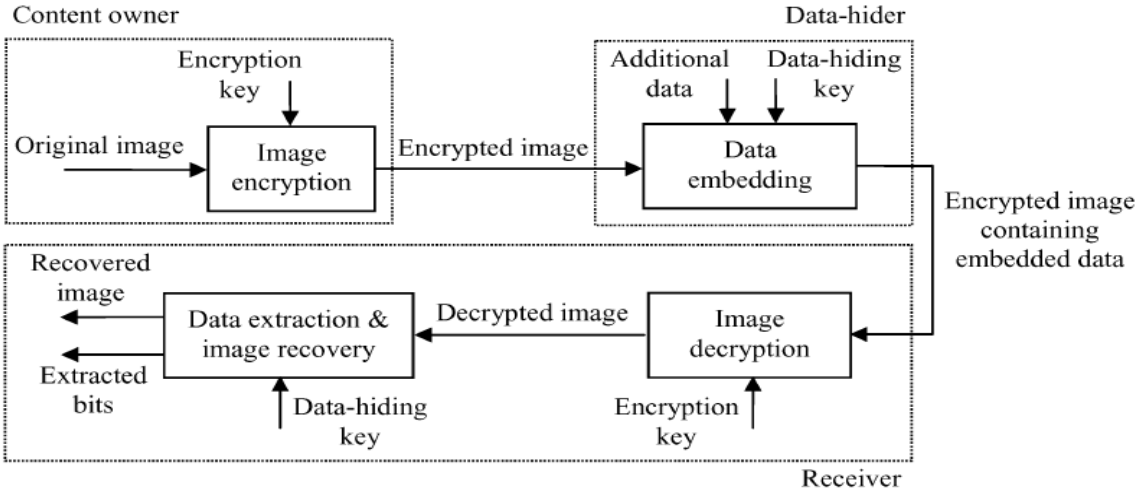

Figure 2.a

In reversible data hiding in encrypted images, the evaluation of block smoothness is crucial for obtaining a correct data extraction. However, the four borders of each block do not join the calculation of block smoothness. This may decrease the rate of correctness of data extraction, especially when the block size is small. For example, for a block of size 8 x 8, there are 64 pixels and around 43.75% of them (28 pixels) are located in the four borders. These border pixels are not employed to calculate the block smoothness, and the percentage is increased as the block size decreased. Besides it extracts the embedded bits by evaluating the smoothness of a single block. However, flipping 3 LSBs of these complex blocks will not cause a significant increase in complexness. Based on these observations, this letter proposes an improved version for a better estimation of block smoothness. In the new smoothness estimation, the summation of the absolute of two neighbouring pixels is employed. Moreover, the extraction and recovery are performed starting from the most noticeable changes in smooth- ness to the least ones. Besides, we also adopt the side-match technique to evaluate the block smoothness by concatenating the border of recovered blocks to the unrecovered blocks. The data encryption and data embedding process is the same as the previous method. Therefore, we address only the calculation of smoothness and the process of image recovery.

The smoothness of an image block can be evaluated by calculating the absolute difference of neighbouring pixels. The larger the summation of absolute differences, the more complex the image blocks is. Therefore, we estimate the block smoothness by calculating the summation of the vertical absolute differences and horizontal absolute differences of pixels in image blocks using the following equation:

$$f = \sum_{u=1}^{s2} \sum_{v=1}^{s1-1} |p_{u,v} - p_{u,v+1}| + \sum_{u=1}^{s2-1} \sum_{v=1}^{s1} |p_{u,v} + p_{u+1,v}|$$

Were $p_{u,v}$ represents the pixel values located at position (u, v) of a given image block of size s1xs2. Equation fully exploits the absolute difference between two consecutive pixels in both vertical and horizontal directions and thus, the smoothness of blocks can be better estimated.[3]

In separable reversible data hiding in encrypted images, there are two phases. In the first phase, a content owner encryptsthe original uncompressed image using an encryption key. Then, adata-hider may compress the least significant bits of the encrypted imageusing a data-hiding key to create a sparse space to accommodate some additionaldata. With an encrypted image containing additional data, if a receiverhas the data-hiding key, he can extract the additional data thoughhe does not know the image content. If the receiver has the encryption key,he can decrypt the received data to obtain an image similar to the originalone, but cannot extract the additional data. If the receiver has both thedata-hiding key and the encryption key, he can extract the additional dataand recover the original content without any error by exploiting the spatialcorrelation in natural image when the amount of additional data is not toolarge. The receiver options were illustrated in figure 2.b.[4]

ISSN: 2278 – 7798

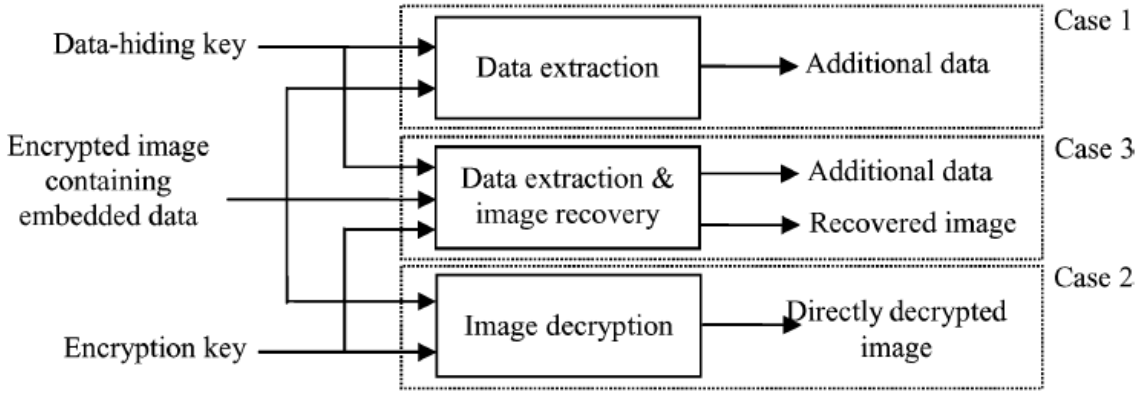

Figure 2.b

Digital watermarking is a kind of data hiding technology. Its basic idea is to embed covert information into a digital signal, like digital audio, image, or video, to trace ownership or protect privacy. Among different kinds of digital watermarking schemes, reversible watermarking has become a research hotspot recently. Compared with traditional watermarking, it can restore the original cover media through the watermark extracting process; thus, reversible water- marking is very useful, especially in applications dictating high fidelity of multimedia content, such as military aerial intelligence gathering, medical records, and management of multimedia information.reversible watermarking scheme based on additive interpolation-error expansion, which features very low distortion and relatively large capacity. Different from previous watermarking schemes, we utilize an interpolation technique to generate residual values named interpolation-errors and expand them by addition to embed bits. The strategy is efficient since interpolation-errors are good at de-correlating pixels and additive expansion is free of ex-pensive overhead information.[5]. Comparisons of papers are shown in the table 1 bellow.

III. 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:

- Generationof encrypted image.
- Data hiding in encrypted image.
- Dataextraction.
- Image recovery

A. Generation of encrypted image:

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.

B. 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 A_E. Since A_E 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.

ISSN: 2278 – 7798

Sl no	Title of paper	Year of publication	Methods used	Advantages/ disadvantages
1	Reversible data hiding	2006	Histogram modification, reversible data hiding, watermarking	Can embed more data with small distortion.
2	Reversible image watermarking using interpolation technique	2010	Additive interpolation error expansion, data hiding, interpolation error	High image quality without sacrificing embedding capacity.
3	Reversible data hiding in encrypted images	2011	Image encryption, image recovery, reversible data hiding	Low computation complexity. data can be extracted after decrypting the image
4	An improved data hiding in encrypted images using side match	2012	Encrypted image, reversible data hiding, side-match	Improved data extraction and image recovery, side match technique reduces error rate
5	Separable	2012	Image	Image

ISSN: 2278 – 7798

	reversible data hiding in encrypted image		encryption, image recovery, reversible data hiding	recovery and data extraction can be performed in parallel.

Table 1

C. Data extraction and image recovery:

Since data extraction is completely independent from image decryption, the order of them implies two different practical applications.

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.

V. Conclusion

Reversible data hiding in encrypted images is a new topic drawing attention because of the privacy preserving requirements from cloud data management. Previous methods implement RDH in encrypted images by vacating room after encryption,as opposed to which is proposed by reserving room before encryption. Thus the data hider can benefit from the extra space emptied out in previous stage to make data hiding process effort- less.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 achieve real reversibility, separate data extraction and greatly improvement on the quality of marked decrypted images.

References

[1]. 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.

[2]. L. Luo*et al.*, "Reversible image watermarking using interpolation," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 1, pp. 187–193, 2010 .

[3]. X. Zhang, "Reversible data hiding in encrypted images," *IEEE Signal Process. Lett.*, vol. 18, no. 4, pp. 255–258, Apr. 2011.

[4]. 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.

[5]. X. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 826–832, Apr. 2012.

[6]. D.R.DenslinBrabin and Dr.J.JebamalarTamilselvi. "Reversible data hiding: a survey," *International Journal of Innovative Research in Computer and Communication Engineering* Vol. 1, Issue 3, May 2013

ISSN: 2278 – 7798