Review on Reserving Room Before Encryption for Reversible Data Hiding

Akshata Malwad, Girija J. Bavare, Sofiya Mulani and Priyanka Bahadure
Department Of Computer Engineering, Pad Dr.D.Y.Patil Institute of Engg and Technology, Pimpri, Pune, Maharashtra, India

Abstract - Now a days there is very big problem of data hacking. There are number of techniques available in the industry to maintain security of data. So, data hiding in the encrypted image is comes into the picture, but the problem is the occurrence of distortion in original cover at the time of data extraction. That’s why Recently, more and more attention is paid to reversible data hiding (RDH) in encrypted images, since it offers the excellent way so that the original cover can be recovered without any loss after embedded data is extracted while protecting the image content’s confidentiality. In This paper we propose a novel method by reserving room before encryption (RRBE) with a traditional RDH algorithm, and thus it is easy for the data hider to reversibly embed data in the encrypted image. Using RRBE we can achieve real reversibility, that is, data extraction and image recovery are free of any error and also we can increase the rate of data to be hidden. This is useful in the way that these method recovers the image with its original quality with improved PSNR ratio.

Keywords – Reversible data hiding, Image encoding, Image decoding, Histogram shifting.

I. INTRODUCTION

DATA HIDING is the technique of hiding the data into cover media. That is, the data hiding process involve two sets of data, 1. A set of the embedded data and another is 2. A set of the cover media data. As when data is embedded into the image then the quality of image get disturbed. So it is expected that after the data extraction the image quality should be maintained just 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 i.e Reversible data hiding. RDH in images is a technique, due to which the original cover can be loss less 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 which can be achieved using RDH.

In this, the very first step applied is to reserve the memory space into the image for data embedding. It is beneficial because it saves the time for creating space for data on time and also we get the idea of number of vacancy available in an image. Then the image encryption is stepped in which the data is embedding in already vacated rooms. There are number of methods for the image encryption such as image partition in which image is divided into two parts. Then part A is reversibly embedded into the part B called as self reversible embedding. That is least significant bits are embedded first in part B. Then the process of data hiding is done using the separable reversible data hiding. A data-hider may compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate some additional data. This additional data may include the data, some that at receiver side these contents are restored back in image to get image with original quality. Then at the receiver side the two tasks are done as data extraction & image recovery. But to get original cover the additional task is done called as image restoration in which the original key contents are restored to the image. With an encrypted image containing extra data, if a receiver has the data-hiding key then he can extract the extra data though he does not know the image content. If the receiver has the encryption key, he can decrypt the received data to get an image similar to the original image, but cannot extract the extra data. If the receiver has both the keys i.e. data-hiding key and the encryption key, he can extract the extra data and recover the original content.

II. RELATED WORK

A. Reversible data hiding techniques

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 [1]. In this they used the encoding and decoding as, Another promising strategy for RDH is histogram shift (HS), in which space is saved for data embedding by shifting the bins of histogram of gray values. In this process the data embedding process is done in three steps as first the histogram is drawn then the peak point is taken into consideration then whole image is scanned row by row. Then once again the image is scanned & the grayscale value 154 is encountered then the embedded data sequence is checked & we get the marked image. Then the data extraction is done. To get
the original cover quality the process of histogram shift is applied again. Then the original cover is get back. Basically data hiding is the process to hide the data into some covering media. That is it is the concatenation of two blocks of data, first is embedding data & second is covering media. But in most of the cases the covering media gets distorted after the data is embedded & the covering media is not inverted back to its original form after data is removed from it. So, to maintain the quality of an image reversible data hiding i.e. RDH techniques are used.

Some reversible data hiding methods uses the concept of differential expansion transform which is based on haar wavelet transform. Another concept used is the histogram shift. The differential expansion is the difference between two neighboring pixels for hiding one bit of data. In this the histograms are drawn first. Then the peak values are taken into consideration. Then two peak values are considered & difference is calculated. Then according to the result the bit by bit data is embedded into the image. In this way the distortion analysis is done & it is helpful to remove the distortion in the covering media & to get the original cover back .

Encryption is an effective means of privacy protection. To share a secret image with strange person, a content owner may encode the image before broadcast. In some cases, a channel administrator needs to add some extra message, such as the source data, image information 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 extra message at receiver end. That means a reversible data hiding method for encrypted image is advantageous.

Some attempts on RDH in encrypted images have been made. Zhang divided the encrypted image into numerous blocks. By spinning 3 LSBs of the half of pixels in every block, space can be created for the embedded bit. The data extraction and image recovery proceed by finding which part has been spin in one block. This process can be grasped with the help of spatial correlation in decrypted image [2].

Hong et al. ameliorated Zhang’s method at the decryption side by further making use of the spatial correlation using a different estimation equation and side match method to gain much lower error rate. These two methods explained above rely on spatial correlation of original image to extract data. That is, the encrypted image should be decrypted first before data extraction [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 [4]. 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 [5].

Digital watermarking is a method of embedding useful information into a digital work (especially, thus audio, image, or video) for the purpose of copy control, content authentication, distribution tracking, broadcast monitoring, etc. The distortion introduced by embedding the watermark is often constrained so that the host and the watermarked work are perceptually equivalent. However, in some applications, especially in the medical, military, and legal domains, even the imperceptible distortion introduced in the watermarking process is unacceptable. This has led to an interest in reversible watermarking, where the embedding is done in such a way that the information content of the host is preserved. This enables the decoder to not only extract the watermark, but also perfectly reconstruct the original host signal from the watermarked work[6].

B. Performance analysis of a reversible data embedding algorithm

Data embedding in the reversible manner which is the data embedding without any loss embeds the data or payload into digital image in reversible manner. After data embedding the quality of original image may be degraded which is to be avoided. The attractive property of data embedding in reversible manner is reversibility that is after data extraction the original quality image is restored back. Reversible data embedding hides some information in a digital image in such a way that an approved party could decode the hidden information and also restore the image to its original state. The presentation of a reversible data-embedding algorithm can be measured using following,
• Data embedding capacity limit
• Visual quality
• Complexity

The data without any distortion embedding is the attractive feature 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 pleasing, particularly in military data and medical data. In such a circumstances, every small part of information is important.

From the application point of view, Since the differentiation between the implanted image and original image is almost discernible from human eyes, reversible data implanting could be thought as a top secret communication channel since reversible data implanting can be used as an information transporter.

III. PROPOSED METHOD

![Fig 1. Framework RRBE](image)

OI-original image, EI-encrypted image, MEI-marked encrypted image

Since losslessly 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? 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)”

In our approach 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. And it is also hopeful that the original content should be recovered without any error after image decryption and message extraction at receiver side. Reference [2] presents a practical scheme satisfying the above-mentioned requirements. A content owner encrypts the original image using an encryption key, and a data-hider can embed additional data into the encrypted image using a data-hiding key though 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. In the scheme, the data extraction is not separable from the content decryption. In other words, the additional data must be extracted from the decrypted image, so that the principal content of original image is revealed before data extraction, and, if someone has the data-hiding key but not the encryption key, he cannot extract any information from the encrypted image containing additional data.

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.

Since the data embedding only affects the LSB, a decryption with the encryption key can result in an image similar to the original version.

There are following steps in our approach:

- **SENDER**

Step1: Image Partition

Assume the original image is an 8 bits gray-scale image with its size $M \times N$ and pixels $c_{i,j} \in [0,255]$, $1 \leq i \leq M, 1 \leq j \leq N$. First, the content owner extracts from the original image, along the rows, several overlapping blocks whose number is determined the size of to-be-embedded messages, denoted by $l$. In detail, every block consists of $m$ rows, where $m = \lfloor l/N \rfloor$ and the number of blocks can be computed through $n = M - m + 1$.

An important point here is that each block is overlapped by pervious and/or sub sequential blocks along the rows. For each block, define a function to measure its first-order smoothness

$$f = \sum_{u=2}^{m} \sum_{v=2}^{N-1} \left| c_{u,v} - \frac{c_{u-1,v} + c_{u+1,v} + c_{u,v-1} + c_{u,v+1}}{4} \right|$$
Higher f relates to blocks, which contain relatively more complex textures
A=more complex texture
B=less complex texture

Step2: Self Reversible embedding

Embed the LSBs of more complex texture block into comparatively lower complex texture block, then interpolation of white pixels takes place.

Step3: Image Encryption

After rearranged self-embedded image, denoted by X, is generated, we can encrypts X to construct the encrypted image, denoted by E. With a stream cipher, the encryption version of X is easily obtained. For example, a gray value \( X_{ij} \) ranging from 0 to 255 can be represented by 8 bits, \( X_{ij}(0), X_{ij}(1) \ldots X_{ij}(7) \), such that

\[
X_{ij}(k) = \left[ \frac{X_{ij}}{2^k} \right] \mod 2 \quad k=0,1\ldots7
\]

The encrypted bits \( E_{ij}(k) \) can be calculated through exclusive-or operation

\[
E_{ij}(k) = X_{ij}(k) \oplus \tau_{ij}(k)
\]

Where \( \tau_{ij}(k) \) = encryption key

Step4: Using data hiding key data hider hides the data.

- RECIEVER

Step5: 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.

VI. 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 we 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 effortless. The proposed 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 improve on the quality of marked decrypted images.

V. REFERENCES


