Data Concealing in Encrypted Images Using Reversible Data Hiding (RDH) Technique

Author
Sujith T
PG Scholar/Dept. of CSE
Karunya University

Guide
Mr Iwin Thanakumar S
Assistant Professor/Dept. of CSE
Karunya University

Abstract – In the new era of technology, more attention is needed to be given to hide some personal data or secret information, etc. This can be exactly brought out through Reversible Data Hiding, since it maintains the splendid property that the original cover can be retrieved back after data is embedded. It can be extracted while protecting the image content confidentially. We suggest a new method by method of encryption after appropriating room with a conventional method. The proposed method can achieve real concealment, that is, data revealing and image recovery with some loss in data. If the receiver has the encryption key, he/she can decrypt the data to obtain an image similar to the original, but cannot extract the extra data. Experiments show that this method can embed more number of times as large number of data for the same image quality as the conventional methods, such as for PSNR & MSE.

Keywords: Difference expansion, Histogram, Matlab, RDH, Reserve room.

I.INTRODUCTION

Reversible data hiding

Reversible data hiding (RDH) [1], [13] in images is a technique, by which the original cover can be lossless, recovered after the embedded message is extracted. This important technique is used drastically in medical imagery, military imagery and law forensics, where no disturbance of the original cover is to be achieved.

Regarding providing confidentiality for images, encrypting the data is an effective and familiar means as it converts the original and significant content to inexplicable one. Although few RDH techniques in encrypted images have been introduced yet, there are some promising applications if RDH can be applied to encrypted images.

A reversible data coloring technique based on encrypted data is preferred. Suppose a medical image data- base 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.

A person, who is having the decrypting key, can relocate the image in a reversible
manner for the purpose of further diagnosing by using the process in the reversible manner. The proposed novel method for RDH in encrypted images is encryption after allocating some space. In the proposed method, we first empty out room by embedding LSBs [2] of some pixels into other pixels with a traditional RDH method and then embed the image with some data, so the positions of the bits in the encrypted image can be used to embed data. Real data hiding with data concealment is realized, that is, data extraction and image recovery are free of any error. Forgiven embedding rates, the PSNR so encrypted image containing the embedded data can be improved and for the satisfactory error occurrences, the range of embedding rates is greatly enlarged.

The method in segments the encrypted image into a number of non-overlapping blocks sized by each block is used to carry one additional bit. To do this, pixels in each block are gathered and divided into two sets and according to a data hiding key. For data extraction and image recovery, the receiver alters the pixels in to a new decrypted block. One of them will be decrypted to the original block.

Due to spatial correlation in natural images, original block is presumed to be much smoother than interfered block and embedded bit can be extracted correspondingly. Moreover, there is a problem in bit extraction and image recovery when divided block is relatively small or has much detailed textures.

In the first approach established a rate-distortion model for RDH [13], 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.

A more popular method is based on difference expansion (DE), in which the difference of each pixel group is expanded, and thus the least significant bits (LSBs) of the difference are all-zero and can be used for embedding messages.

II. EXISTING SYSTEM

Different Expansion Technique:

Many researchers introduced Difference Expansion (DE) technique to deduce high capacity, low-disturbance reversible data hiding. This technique divided the image into pairs of pixels, and a secret message was added into the difference between the pixels of each pair which is called as embedding. The former was further divided into three categories of the blocks.

Simulation showed that the payload size and the perceived quality of the marked images generated by this technique were better than those achieved by the existing research at that time. Namely, confidential information was hidden, whereas no one should retrieve the information without proper key generation.

The overhead bits were embedded in the auxiliary information area. To increase hiding capacity, a variant Differential Expansion (DE) based technique that improved the compressibility of the location
map. In comparison, conventional DE-based schemes, this technique provided increased embedding storage and performed well with a variety of image types.

The secret message, which can be divided into two parts, was embedded into the spatial domain and/or frequency domain of a cover image. The stego-images generated by the method were, to a certain degree, resistant to manipulation.

**Histogram-based Scheme:**

By combining the peak point of a difference image with a multilevel hiding strategy, the scheme could maintain a high capacity while keeping distortion low. By using the difference between adjacent pixels rather than a single pixel, their algorithm could operate at a high capacity while maintaining low distortion.

Based on a modification of the difference histogram [5], [13] between sub-sampled images, the algorithm prevented any overflow/underflow issues and did not require overhead information during data extraction. The modification of prediction errors (MPE) and proposed a lossless data hiding method is been introduced. First, pixel values would be determined from an input image, and then error values would be obtained. MPE can keep the distortion low if few messages are embedded, and leave sufficient vacant space to hide the desired payload.

**Prediction-based Method:**

Based on forecasting expansion methods of error identification and the histogram shifting technique, simulations showed that the prediction-error expansion doubled the maximum embedding capacity as compared to the new method by difference expansion. The perceived quality of the marked images was good at a moderate embedding capacity.

**Interpolation-based Algorithm:**

The interpolation technique provides the advantages of both low-time complexity and high computing speed. Experiments indicated that this method can embed a large amount of bits into the cover image while still keeping distortion low. Owing to the only slight modification of pixels, a high perceived quality of the resulting image would be preserved.

**III.PROPOSED METHOD**

We propose a novel method for RDH in encrypted images, for which we do not “vacate room after encryption” as done in, but “reserve room before encryption”. In the proposed method, we first empty out room by embedding LSBs of some pixels into other pixels with a traditional RDH method and then encrypt the image, so the positions of these LSBs in the encrypted image can be used to embed data. 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 acceptable PSNR, range of embedding rates is greatly enlarged.

![Overall Work Flow Diagram for RDH with Encrypted Images]

Since lossless allocating room from the encrypted images is relatively difficult and sometimes inefficient. If we reverse the order of encryption and allocating room, i.e., reserving room prior to image encryption at content owner side, the RDH [5], [13] tasks in encrypted images would be more natural and much easier which leads us to the novel technique of data concealment.

The content owner first reserves enough space on original image and then convert 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.

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 compared with techniques from Framework VRAE. This is because in this new framework, we follow the customary idea that first lossless compresses the redundant image content (e.g., using excellent RDH techniques) and then encrypts it with respect to protecting privacy.
The reserving room prior to image encryption at will be at content owner side; the RDH task in encrypted image would be natural and then converts the image into its encrypted version with the encryption key. The data embedding process in encrypted images is inherently reversible for the data hider only needs to accommodate data into the spare space. The data extraction and image recovery are identical to VRAE. The standard RDH algorithm is used. Due to the similarity of neighbor pixels’ values, most differences between pairs of adjacent pixels are equal or close to zero.

![Frame separated image (A&B planes)](image)

**fig 2: Frame separated image (A&B planes)**

In this work, a histogram is constructed based on these difference statistics. In the data embedding stage, a multilevel histogram modification mechanism is employed. As more peak points are used for secret bits modulation, the hiding capacity is enhanced compared with those conventional methods based on one or two level histogram modification.

Moreover, as the differences concentricity around zero is improved, the disturbance on the cover image introduced by secret content adding by pixels i.e. embedding is extenuated. In the data extraction and image recovery stage, the embedding level instead of the peak points and zero points is used. The affiliated information is much smaller than in those methods of the kind.

A sequential recovery strategy is exploited for each pixel is reconstructed with the aid of its previously recovered neighbor. Determined results and conclusions of other methods demonstrate our method’s effectiveness and superior performance. These decomposition trees are encrypted and have to be present at the decoder to be able to reconstruct the image data properly.

![Histogram Shifted image with A,B planes](image)

**fig 3: Histogram Shifted image with A,B planes**

Furthermore, the stego-images generated by the proposed method have a certain degree of robustness which is resistant
to image processing. Here, the DPM is an injective mapping on difference-pairs.

In fact, this choice of adding pixels, the disturbance is reduced as compared to the conventional method, and the enhanced idea has a better performance. In addition, experimental results show that the novelty that outperforms some leveled algorithms. All the details of the algorithms are known, and only the key to encrypt and decrypt the data should be secret.

In this paper an analysis of the local mean square error, the values of PSNR are to be there for the marked encrypted images in order to remove the embedded data during the decryption step. Encouraged Encryption Standard algorithm is used to encrypt the images. In these methods the encrypted images are protected from statistical attacks. An improved histogram-based difference selection and shifting scheme, which our algorithm and makes it resilient to different types of images.

Compared with current algorithms, the proposed algorithm often has better embedding capacity versus image quality performance. A sequential recovery strategy is exploited for each pixel is reconstructed with the aid of its previously recovered neighbor.

Experimental results and comparisons with other methods demonstrate our method’s effectiveness and performance rate with the value of some error detection called as performance validation. This choice of adding pixels, the disturbance is thus reduced comparing with the conventional method.

**IV. CONCLUSION & DISCUSSION:**

As we discussed in this paper, we can go for the reversible data hiding which is based on the determined encrypted images. Reversible data hiding in encrypted images is a new theme that draws care of the users because of the privacy-maintaining needs from stored data. Previous methods use the implementation of RDH in encrypted images by encrypting before allocating room.

Thus everyone can benefit the extra space emptied out in previous stage to make data hiding process by some causality. 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 changeability, data extraction individually and improvement on the quality of marked decrypted images.

V. REFERENCES:

8. L. Luo et al., “Reversible imagewatermarking using interpolation technique,”