ISSN No. 0976-5697

Volume 8, No. 5, May – June 2017

International Journal of Advanced Research in Computer Science

SURVEY REPORT

Available Online at www.ijarcs.info

Reversible Data Hiding In Image- A Literature Survey

Krishnapriya.K.R
P.G Scholar
Department of Computer Science & Engineering
FISAT, Mookkannoor, Kerala, India

ArunKumar.M.N
Associate Professor
Department of Computer Science & Engineering
FISAT, Mookkannoor, Kerala, India

Abstract: Security must be provided for the transmission of confidential and sensitive data over the network. To increase the security of data transmission, data hiding can be performed in encrypted image .Therefore the security of image and embedded data is maintained. The hidden data and the cover image can be restored thereby reversibility can be achieved, which is termed as Reversible Data Hiding. By using combined lossless and reversible data hiding, the embedded data and cover image can be retrieved. This paper focus on the various works in the area of reversible datahiding and various RDH techniques are discussed.

Keywords: Data Hiding ,Security, Reversible Data Hiding, Data embedding

I. INTRODUCTION

For high security of data several approaches like steganography ,Data Hiding and cryptography can be used. In Cryptography the study of various mathematical methods and various aspects of Information Security like confidentiality and authentication of data. In cryptography a plain text is encrypted into cipher text and that can be look like a meaningless string of character whereas in case of steganography, cover media contains the hidden data that looks like normal image. Such an image ,where the hidden message cannot be detected is called as stegno-image. Data hiding deals with the existence of secret information while cryptography protects the message . To increase the information security more attention is paid to reversible data hiding in encrypted images. The embedded data in the cover media data may be related to the image such as authentication data or author information.

Data hiding is the process to hide data within a cover media. Therefore, the data hiding process contains two types of data, embedded data and cover media data. The data is transmitted by embedding it within Images, which improves data security. The data hiding method in which the reversibility can be achieved is called Reversible data hiding. This technique is mainly used to improve the security of the cover Image in encryption.

Reversible image data hiding (RIDH) is one method of data hiding technique, which makes sure that the cover image is reconstructed perfectly after the extraction of the embedded message. The reversibility of this method makes the data hiding approach attractive in the critical scenarios, e.g., military and remote sensing, law forensics, medical image sharing and copyright authentication, where the original cover image is required after reconstruction.

The remainder of this paper is organized as follows: Section II introduces a brief note on Data Hiding. Related works in the literature of Reversible Data Hiding are analyzed in Section III. Finally, a brief conclusion is given in Section IV.

II. BACKGROUND DETAILS

A. *Data Hiding*

Datahiding means hiding a secret message within another message. In digital computing there are many applications for datahiding. Datahiding is the practice of concealing information or files within non secret data. The file containing the secret data is called the carrier. The modified carrier looks like original carrier. Best's carriers are images, audio, video files since everybody can send receive download them. The data is hidden not encrypted.

Datahiding techniques can be generally classified as,

1) Spatial domain technique: In spatial domain steganography bits in the pixels values are changed in order to hide the data. Spatial domain techniques can be classified into Least Significant Bit (LSB), Pixel value Differencing (PVD), Random Pixel Embedding method, histogram Shifting method, Texture Based method etc. LSB is the widely used simplest method where there is less chance for degradation of original image.

2) Transform domain technique: Transform domain embeds information in transform space. In this domain, the image is transformed from spatial domain to frequency domain by using any transforms and after a transformation process, the embedding process will be done in proper transform coefficients. The process of embedding data in the frequency of a signal is much stronger than embedding principles that operate in the time domain. Transform domain techniques include DFT, DCT, DWT and they are less exposed to compression, cropping etc [1].

3) Distortion technique: This technique store message by distorting the cover slightly and detecting the change from the original. The decoder function uses the original cover image during decoding process to find the difference between original and distorted cover image in order to restore secret message [1].

Masking and filtering: This technique is usually restricted to grayscale and 24-bit images. It doesn't hide the data in noise level but embeds it in significant areas. Masking adds redundancy to the hidden inormation. This method is more robust than LSB modification with respect to compression and different kinds of image processing since the information is hidden in the visible parts of the image.

III. RELATED WORKS

This section gives an analysis on the various works that have been proposed in the area of combination of steganography and cryptography.

In[2] a method which use of a high quality reversible watermarking scheme with high capacity based on difference expansion. Here data embedding is done using pixel differences; this is because of the possibility of high redundancies among the neighbouring pixel values in natural images. During embedding process, differences of neighbouring pixel values are calculated. In that differences the changeable bits are determined and some differences are selected to be expandable by 1-bit, thus the changeable bits increases. Then concatenated bit-stream of compressed original changeable bits. The location of increased difference numbers and the hash of original image is embedded into the changeable bits of difference numbers in a random order. The watermarked pixels are achieved by using inverse transform to from resultant differences

.

During watermark extraction, differences of neighbouring pixel values are measured. Then determine changeable bits in that calculated differences. Extract the changeable bitstream ordered by the same pseudo random order as embedding and separate the compressed original changeable bitstream. Decompress the compressed separated bit-streams and reconstruct the original image replacing the changeable bits and calculate the hash of reconstructed image and compare with extracted hash. The technique contains the following advantages. There is no loss of data due to compression decompression, this is also applicable to audio and video data. The encryption of compressed location map and changeable bit-stream of different numbers increases the security. The disadvantages included in difference expansion are there may be some round off errors. The method largely sensitive to the smoothness of the image. So this method cannot be applied to textured images, whose capacity will be very low or even zero. There is significant degradation of visual quality due to replacements of bits of gray scale pixels.

In [3] propose an analysis of the local standard deviation of the marked encrypted images in order to remove the embedded data during the decryption step. The number of digital images has increased rapidly on the Internet. Image security has high impact on several applications, e.g., video surveillance, military and medical applications. The need of fast and secure diagnosis is vital in the medical world. The transmission of images is a daily routine and it is necessary to find an efficient way to transmit them over networks. The data compression is necessary to decrease the transmission time. Two main groups of technologies have been developed for this purpose. First group based on content protection through encryption. There exist many methods to encrypt binary images or gray level images.In this, proper decryption of data requires a key. The second group based on the protection on digital watermarking or data hiding, aimed at secretly hiding a message into the cover data. These two technologies can be used complementary and mutually commutative.

.

In [4] proposes Data hiding Based On Search Order Coding for Vector Quantization Compressed Images. Vector Quantization is a popular and commonly used digital image compression technique. Since VQ significantly reduces the size of an image to a great extend, the technique can save the costs of storage space as well as image delivery. This method uses Search-Order Coding (SOC) to manipulate the randomly distributed histogram of a VQ-compressed image into locations close to zero. Then uses the encoding strategies to perform encoding and data hiding simultaneously. During encoding process, indicator is not required for indices to identify index types, which in turn helps improve compression performance. This technique can completely restore the VQ-compressed image after secret data extraction.

A novel reversible SOC-based data-hiding scheme is used to increase embedding capacity. The embedding capacity of image is increased and achieve lossless reconstruction of the cover image by using the help of SOC and hiding strategies. This technique applies SOC to a VQ-compressed image in order to achieve SOC compressed image, which can support higher capacity to embed data. During encoding process, SOC indices are modified to hide secret information and no indicator is required, and thus a low bit rate and a high embedding capacity can be obtained. In extraction process, the algorithm extracts the secret data as well as the cover image with good quality. But this technique is time consuming due to the complexity of the algorithm.

.

In [5] proposed a new simple yet effective framework for RDH in encrypted domain. In the proposed scheme, the pixels in a plain image are firstly divided into sub-blocks with the size of $m \times n$. Then with an encryption key, a key stream (a stream of random or pseudorandom bits/bytes that are combined with a plaintext message to produce the encrypted message) is produced, and then the pixels in the same sub-block are encrypted with the same key stream byte. After the encryption of the stream, the encrypted $m\times n$ sub-blocks are randomly permutated with a permutation key.

The correlation between the neighboring pixels in each sub-block is well preserved in the encrypted domain. The main advantage of the proposed framework is that the RDH scheme is independent of the image encryption algorithm. That is, the server manager does not need to design a new RDH scheme according to the encryption algorithm that has been conducted by the content owner, as it is done by embedding the data by using various RDH algorithms previously proposed to the encrypted domain directly.

In [6] proposed a method by reserving room before encryption using RDH algorithm, and thus it is easy for the data hider to reversibly embed data in the encrypted image. This method is proposed to achieve real reversibility. The scheme consists of three stages. Generate encrypted images and perform data hiding by shifting LSB planes. The quality of marked decrypted images will be high due to the separate data extraction.

IV. CONCLUSION

Reversible data hiding in encrypted image is getting more attention these days because of security maintaining requirements. Reversible data hiding in encrypted image is a powerful technique to improve the security of data. Data hiding in encrypted images provides more security for the data as cryptography and steganography are performed. By combining lossless and reversible data hiding techniques, more efficient data embedding can be done in encrypted images. The concept of data hiding and their applications in the security of digital data communication across network is studied in this paper and technical survey of recent methods in reversible data hiding is presented.

V. REFERENCES

[1] Mehdi Hussain and MureedHussain, “A Survey of Image Steganography Techniques”, International Journal of Advanced Science and Technology Vol. 54, May, 2013.

[2] Jun Tian (2003) Reversible Data Embedding Using a Difference Expansion ,IEEE Trans.video.Tech,VOL. 13, NO. 8, 890 -896, 2003.

[3] W. Puech, M. Chaumont and O. Strauss (2008)A reversible datahiding method for encrypted images Proc. SPIE, vol. 6819,
pp.68191E-1-68191E-9.

[4] Yaw-Hwang Chiou, Jiann-Der Lee, (2011)Reversible Data HidingBased on Search-order Coding for VQ-compressed, JCIT), Vol. 6.

[5] Fangjun Huang and Jiwu Huang (2016) New Framework For Reversible DataHiding In Encrypted Domain, IEEE Transactions on Information Forensics and Security.

[6] Kede Ma ,Xianfeng ZhaoandWeiming Zhang 2016)Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption, IEEETransactions on Information Forensics and Security.vol 8, No 3,553-562.