ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

Literature Survey on Reversible Data Hiding in Image with Contrast image enhancement

Ankit Choudhary, Prof. Shilpi Sharma

PG Scholar, Dept. of ECE, Bhopal Institute of Technology Bhopal, India

Professor, Dept. of ECE, Bhopal Institute of Technology Bhopal, 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 data hiding 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 stegnoimage. 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.

Data hiding is defined as the process of embedding the message signal into the host or cover of image to get the composite signal.

Following are the 3 main requirements of data hiding system,

1. Perceptual Transparency
2. Robustness
3. Capacity

Mainly data hiding techniques are classified into two techniques:

1. Reversible data hiding technique: In this technique the message signal as well as the original cover can be with no loss recovered simultaneously.
2. Irreversible data hiding technique: In this technique the message signal can be recovered with no loss but the original cover can be lost. So in general reversible data hiding techniques can be used now a day.

DOI: 10.15680/IJIRCCE.2018.0603101

Reversible Data Hiding

Reversible Data Hiding is a technique that hides data in digital images for secret communication. It is a technique used for hiding additional message into cover media with a reversible manner so that the original cover content can be perfectly restored after extraction of the hidden message. Traditionally, the data hiding technique is used for secret communication of data. In some applications, the embedded carriers are further encrypted to prevent the carrier from being analysed to reveal the presence of the embedment of data. Other applications could be for when the owner of the carrier might not want the other person, including the data hider, to know the content of the carrier before data hiding is actually performed, such as confidential medical images or military images. Here, the content owner has to encrypt the content before passing to the data hider for data hiding.

The receiver can extract the embedded message and recover the original image which was used as cover image. Many reversible data hiding methods have been proposed recently. Encryption is an effective and popular means for providing privacy. In order to securely share a secret image with other person, a content owner will encrypt the image before transmission. It may be also expected that the original content can be recovered without any error after decryption and retrieve of additional message at receiver side. Hence a reversible data hiding scheme for encrypted image is desirable.

Data hiding is referred to as a process to hide data (representing Abstract Nowadays digital communication has become an essential part of infrastructure. A lot of applications are internet-based and it is important that communication will be made secret. As a result, the security aspect of information passed over an open channel has become a fundamental issue and hence, the confidentiality and data integrity are required to protect against unauthorized access and use. This has led to an unstable growth in the field of information hiding. Cryptography and steganography are the two popular methods available to provide security. Using cryptography, the data is transformed into some other gibberish form and then the encrypted data is transmitted.

In steganography, the data will be embedded in an image and that image will be transmitted. In this paper the focus on different techniques that are existing, for steganography and comparative study all the techniques together as a literature survey. This paper will also propose a new method for embedding the data inside the image and the advantages of this technique over the previous existing techniques.

The data hiding process links two types of data, one a set of the embedded data and another set of the cover media data. In several cases of data hiding, the cover media will be distorted due to data hiding and cannot be inverted back to the original media. Means, cover media has permanent distortion even after the hidden data have been removed. In some applications, like medical diagnosis and law enforcement it is desired that the original cover media can be recovered efficiently with no loss. The techniques satisfying this requirement will be referred to as lossless, reversible, invertible, distortion-free or data hiding techniques [2]. C. Separable Reversible Data Hiding As the name indicates that it is the reversible data hiding technique but which is separable. The separable means that the information hidden can be separated using suitable criteria. The activities that can be separated are extraction of original cover image and extraction of original data which was embedded.

This separation exists based on the keys available. At the receiver side, three different cases are encountered viz., if encryption key is available, get the original image, if data extraction key is available, get the original data and if both the keys are available, get both data and the image. Hence it is called as Separable Reversible Data hiding.

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 analysed in Section III. Finally, a brief conclusion is given in Section IV.

II. RELATED WORK

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 increase.

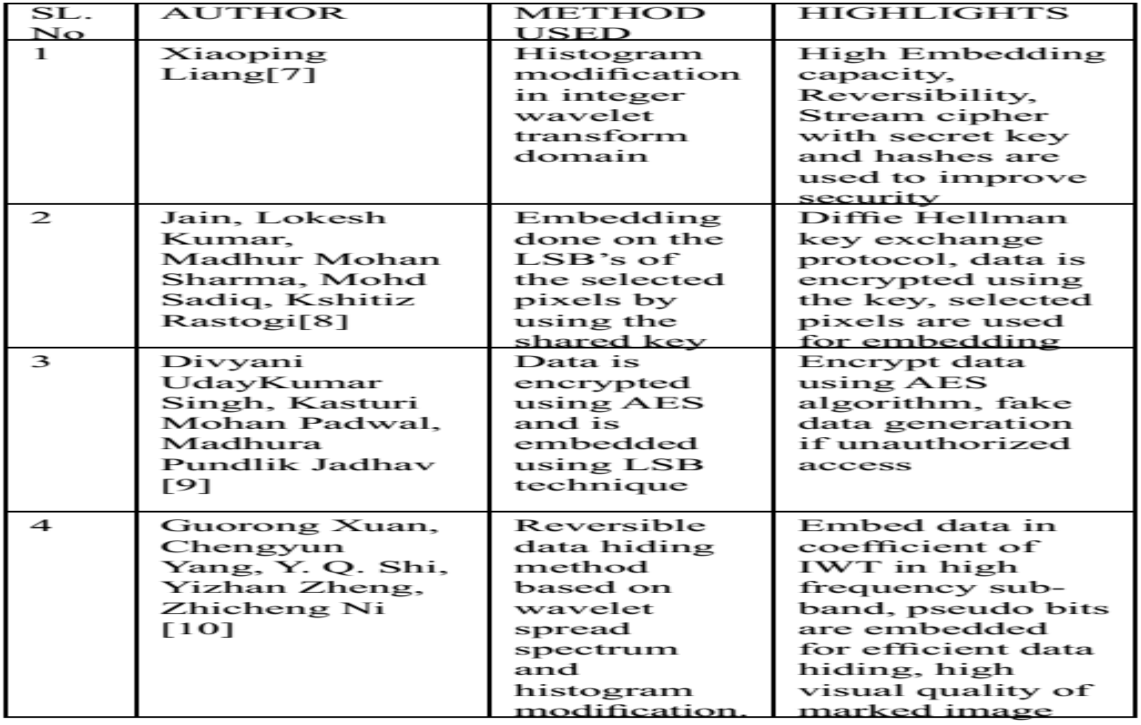
Then concatenated bit-stream of compressed original changeable bits. The location of increased difference numbers and the hash of original image is embedded into the changeable bits of difference numbers in a random order. The watermarked pixels are achieved by using inverse transform to from resultant differences. During watermark extraction, differences of neighbouring pixel values are measured. Then determine changeable bits in that calculated differences. Extract the changeable bit stream 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 extent, 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.



SL. No	AUTHOR	METHOD USED	HIGHLIGHTS
1	Xiaoping Liang[7]	Histogram modification in integer wavelet transform domain	High Embedding capacity, Reversibility, Stream cipher with secret key and hashes are used to improve security
2	Jain, Lokesh Kumar, Madhur Mohan Sharma, Mohd Sadiq, Kshitiz Rastogi[8]	Embedding done on the LSB's of the selected pixels by using the shared key	Diffie Hellman key exchange protocol, data is encrypted using the key, selected pixels are used for embedding
3	Divyani UdayKumar Singh, Kasturi Mohan Padwal, Madhura Pundlik Jadhav [9]	Data is encrypted using AES and is embedded using LSB technique	Encrypt data using AES algorithm, fake data generation if unauthorized access
4	Guorong Xuan, Chengyun Yang, Y. Q. Shi, Yizhan Zheng, Zhicheng Ni [10]	Reversible data hiding method based on wavelet spread spectrum and histogram modification.	Embed data in coefficient of IWT in high frequency sub-band, pseudo bits are embedded for efficient data hiding, high visual quality of marked image

Table 1: Highlights of the related work

A novel reversible SOC-based data-hiding scheme is used to increase embedding capacity. The embedding capacity of image is increased and achieves 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 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.

The correlation between the neighbouring pixels in each subblock 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.

III.BACKGROUND DETAILS

Data Hiding:

Data hiding means hiding a secret message within another message. In digital computing there are many applications for data hiding. Data hiding 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.

Data hiding 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].

This technique is usually restricted to gray-scale 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 information. 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.

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.

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 ,IEEETrans.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 ,XianfengZhaoandWeiming 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.

7. Xiaoping Liang,” Reversible Authentication Watermark for Image”, World Congress on Engineering and Computer Science, October 22 - 24, 2008.

8. Vivek Jain, Lokesh Kumar, Madhur Mohan Sharma, MohdSadiq, KshitizRastogi,” Public-Key Steganography Based On Modified Lsb Method”, Journal of Global Research in Computer Science, Volume 3, No. 4, April 2012.

9. DivyaniUdayKumar Singh, Kasturi Mohan Padwal, MadhuraPundlikJadhav,” Separable Reversible Data Hiding in Image Using Advanced Encryption Standard with Fake Data Generation”, International Journal of Computer Science and Information Technologies, Vol. 5 (3), 2014, 3469-3473.

10. G. Xuan, C. Yang, Y. Zheng, Y. Q. Shi and Z. Ni, “Reversible data hiding based on wavelet spread spectrum,” IEEE International workshop on multimedia signal processing (MMSP2004), Sept. 2004, Siena, Italy.

11. R. chandramouli, NasirMemon “Analysis of LSB Based Image Steganography Techniques” 2001 IEEE.

12. Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, “Reversible statistics hiding,” IEEETrans. Circuits Syst. Video Technol., vol. 16, no. Three, pp. 354–362, Mar. 2006.