IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-3, Issue-1 E-ISSN: 2347-2693

Survey on Data Hiding Techniques for Secure Image Transmission

Thanima Davis[1*], Manish T.I[2]and Dr. M. Azath[3]

[1*,2,3]*Department of CSE, Met's School of engineering, Kerala, India*

www.ijcaonline.org

Received: Dec /21/2014 Revised: Jan/2/2015 Accepted: Jan/16/2015 Published: Jan/31/2015

Abstract-Now a days, there are many possible ways to transmitting the data. Any communication of internet and networks application requires security. During the transmission confidential data can be hacked in different ways. So privacy and security are very important issues at the time of transmission over the internet. Steganography is the art of hiding information in other information. It is going to gain its importance due to the exponential growth and confidential communication of potential computer users over the internet. In image Steganography, secret communication is achieved to embed a message into cover image and generate a stego- image. There are different type data hidings techniques are used for secure data transmission. In this paper describes the different data hiding techniques for secure data transmission.

Keywords —Secure image transmission, Data hiding, Steganography

I. INTRODUCTION

The rapid growth of networks allowed large files, such as multimedia images, to be easily transmitted over the internet. These images usually contain private or confidential information. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be essential to keep the existence of the message secret. The reason for this security and confidentiality is because the underlying communication network over which the transfer of sensitive information is carried out is inaccurate and unsecured. Anybody with the proper knowledge and right applications can eavesdrop and learn of the communication and intercept the data transfer which could be very dangerous and even life threatening in some situations. Ideally the internet and the routing protocols and the communication network should exhibit the security. It is an important property of the internet. The internet should provide and preserve the confidential and sensitive information that flows through it. The security should be such that only the intended recipient of the information should gain access to it.

In this paper describes the different data hiding techniques for secure data transmission. Data hiding methods mainly utilize the techniques of LSB substitution, histogram shifting, prediction-error expansion, difference expansion, recursive histogram modification.

Data hiding is a form of steganography that embeds data into digital media for the purpose of identification and copyright [1].The technique used to implement secure transmission, is called steganography. Steganography is the art and science of invisible communication. That means hiding information in other information, then hiding the existence of the communicated information. It is the process of masking the sensitive data in any cover media like still images, audio, video over the internet. Steganography is not to alternation of structure of the secret message, but hides it inside a cover-object. After hiding, cover object and stego-object are similar. In image steganography the information is hidden in images [2].Here attacker does not realize that the data is being transmitted since it is hidden to the naked eye and impossible to distinguish from the original media.

Image steganography terminologies are as follows:-

• Cover-Image: Original image which is used as a carrier for hidden information.
• Message: Actual information which is used to hide into images. Message could be a plain text or some other image.
• Stego-Image: After embedding message into cover image is known as stego-image.
• Stego-Key: A key is used for embedding or extracting the messages from cover images and stego-images.

Steganography involves 4 steps:-

a. Selection of the cover media in which the data will be hidden.
b. The secret message or information that is needed to be masked in the cover image.
c. A function that will be used to hide the data in the cover media and its inverse to retrieve the hidden data.
d. An optional key or the password to authenticate or to hide and unhide the data.

II. VARIOUS DATA HIDING TECHNIQUES

This section we will be presenting the survey on various data hiding techniques in image to facilitate secure data transmission over the underlying communication network.

A. Spatial Domain Technique

In Spatial Domain Methods, there are many versions of spatial steganography, all directly alter some bits in the

image pixel values in hiding data. [3].The simplest and most common type of steganography is LSB (least significant bit).The data space occupied by the LSBs is suitable for data hiding. That hides a secret message in the LSBs of pixel values without introducing many perceptible distortions. The bit shifting approach is used for embedding data that is the one's bit of a byte is used to encode the hidden information and LSB replacement approach for hiding the location map. Changes in the value of the LSB are imperceptible for human eyes. So it provides less chance for degradation of the original image and also more information can be stored in an image. But it has some limitations, they are less robust, hidden data can be lost with image manipulation and Hidden data can be easily destroyed by simple attacks.

B. Transform Domain technique

Next technique is Transform Domain technique. It is a complex way of hiding information in an image. Transform domain embedding can be termed as a domain of embedding techniques for which a number of algorithms have been suggested [4]. The process of embedding data in the frequency domain of a signal is much stronger than embedding principles that operate in the time domain. Transform domain techniques have an advantage over spatial domain techniques as they hide information in areas of the image that are less exposed to compression, cropping, and image processing. But some transform domain techniques do not seem dependent on the image format and they may outrun lossless and lossy format conversions.

C. Reversible data hiding

Reversible data hiding means lossless data hiding. The existing reversible data hiding schemes can be classified into three categories: lossless compression, difference expansion (DE), and histogram shifting. Reversible or lossless data hiding techniques hide data in an image and allow extraction of the original image. There are two important requirements for reversible data hiding techniques: first one is the embedding capacity should be large and next one is distortion should be low. The reversible data hiding schemes based on lossless compression achieve high watermarked image quality; their relative payload is very low. In general, a higher embedding capacity results in a higher degree of distortion. An improved technique embeds the same capacity with lower distortion or vice versa. Among which the histogram-based reversible data hiding schemes have found wide applications for its high watermarked image quality. For lossless compression, Fridrich et al. [5] devised an invertible watermarking method by using a lossless compression algorithm.

1) Histogram modification

Another reversible data hiding technique is histogram modification. Ni et al. [6] increased the hiding capacity by extending the histogram modification technique for integer wavelet transform. The histogram modification technique involves generating histogram and finding the peak point and the zero point and shifting histogram bins to embed message bits. Jung et al. [7] proposed an improved histogram modification based reversible data hiding technique with a consideration of the human visual system (HVS) characteristics. Histogram-based reversible data hiding schemes do not work well in a case where an image having an equal histogram. The Histogram-based reversible data hiding schemes do not work well in a case where an image having an equal histogram even we use multiple pairs of peak and zero points for embedding. The histogram modification technique has an unsolved issue that multiple pairs of peak and minimum points have to be communicated to the recipient via a side channel.

Kuo et al. [8] presented a reversible technique that is based on the block division to conceal the data in the image. In this approach the cover image is divided into several equal blocks and then the histogram is generated for each of these blocks. Minimum and maximum points are computed for these histograms so that the embedding space can be generated to hide the data at the same time increasing the embedding capacity of the image. One bit change is used to record the change of the minimum points.

2) *Difference expansion*

Tian [9] devised a high capacity reversible data hiding technique that is called difference expansion (DE), where the message is embedded based on the 1-D Haar wavelet transform. The resulting high-pass bands are the differences of the neighboring pixel values. The difference expansion scheme is capable to embedding as high.
The resulting high-pass bands are the differences of the neighboring pixel values. The DE scheme is able to embedding as high as 0.15 to 1.97 bpp, which is significantly greater than other schemes proposed previously. Kamstra *et al*. [10] improved the DE scheme by using the low-pass image to find suitable expandable differences in the high-pass band. In difference expansion, their algorithms did not provide a solution to the problem of communicating threshold values and multiple pairs of peak and minimum point.

3) Prediction-error expansion

Thodi and Rodríguez [11] proposed an improved version of the DE scheme called prediction-error expansion (PEE), where the correlation inherent in the neighborhood of a pixel is better exploited than the DE scheme. Hu *et al*. [12] construct a payload dependent location map, where the

compressibility of location map is further improved. Besides, several DE-based schemes [13] recently in which they in principle differ in the employed prediction algorithms as a result, DE-based schemes can achieve high embedding capacity but low image quality. Prediction-error expansion is another type of data hiding technique.PEE-based algorithms depends heavily on image's spatial redundancy. However, one weakness of these algorithms is that the modification of pixels may distort the high correlation in their local regions, and thus involve the prediction accuracy.

D. Masking and Filtering:

It hides information by marking an image. The hidden message is more integral to the cover image. They are more integrated into the image. It has some advantage that is more robust than LSB replacement with respect to compression since the information is hidden in the visible parts of the image. Limitation of Masking and filtering Techniques is, it can be applied only to gray scale images and restricted to 24 bits.

Table 1: comparison of existing data hiding techniques

Sl..No	Method Used	Advantage	Disadvantage
1	spatial domain LSB Technique	Hiding information is less exposed to image processing.	It may lossless and lossy format conversions.
2	Reversible data hiding	Embedding capacity is large. Distortion should be low.	Their relative payload is very low.
3	histogram modification	Simple and enhance contrasts of an image.	Not work well in a case where an image having an equal histogram.
4	Prediction-error expansion	DE-based schemes can achieve high embedding capacity but low image quality	Modification of pixels may distort the high correlation in their local regions.
5	Masking and Filtering	It is robust than LSB replacement..	It can be applied only to gray scale images.

III. CONCLUSION

This survey paper gives the detail analysis of data hiding for secure transmission of data. Security of digital images in transmission, publishing and storage become more important due to ease of access to open networks and internet. There are different ways the data hiding are take place. The data hiding techniques are used to maintain confidentiality in transmitting the data. In this paper describes some important methods for secure transmission of data from source to destination, using the data hiding techniques.

IV. REFERENCES

[1]. Information Hiding: First International Workshop, R. J. Anderson, Editor, Lecture Notes in Computer Science 1174, Isaac Newton Institute, Cambridge, England, Springer-Verlag May 1996

[2]. An overview of image steganography by T. Morkel.

[3]. MamtaJuneja and Parvinder Singh Sandhu, (2013) "A New Approach for Information security using an Improved Steganography Technique", Journal of Info.Pro.Systems, Vol 9, No:3, pp.405-424

[4]. N. F. Johnson and S. Katzenbeisser, "A Survey of steganographic techniques.in Information Hiding Techniques for Steganography and Digital Watermarking", Artech House, **(2000)**, pp. 43-78

[5]. J. Fridrich, M. Goljan, and R. Du, "Invertible authentication," In Proc. of the SPIE, Security and Watermarking of Multimedia Jan. 2001.

[6]. D. Zou, Y. Q. Shi, Z. Ni, and W. Su, "A semi-fragile lossless digital watermarking scheme based on integer wavelet transform," IEEE Transactions on Circuits and Systems for Video Technology, vol. 16, no. 10, pp. 1294-1300, Oct. 2006.

[7]. S. W. Jung, L. T. Ha, and S. J. Ko, "A new histogram modification based reversible data hiding algorithm considering the human visual system," IEEE Signal Processing Letters, vol. 18, no. 2, pp 95-98, Feb. 2011 .

[8]. Wen-Chung Kuo, Dong-Jin Jiang, Yu-Chih Huang, "A Reversible Data Hiding Scheme Based on Block Division", Congress on Image and Signal Processing, Vol. 1, 27-30 May 2008.

[9]. J. Tian, "Reversible data embedding using difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896,Aug. 2003.

[10]. L. Kamstra and H. J. A. M. Heijmans, Reversible data embedding into images using wavelet techniques and

sorting," IEEE Transactions on Image Processing, vol. 14, no. 12, pp. 2082-2090, Dec. 2005.

[11].D. M. Thodi and J. J. Rodríguez, "Expansion embedding techniques for reversible watermarking," IEEE Transactions on Image Processing, vol. 16, no. 3, pp. 721-730, Mar. 2007.

[12].Y. Hu, H. K. Lee, and J. Li, "DE-based reversible data hiding with improved overflow location map," IEEE Transactions on Circuits and Systems for Video Technology, vol. 19, no. 2, pp. 250-260, Feb. 2009.

[13].Coltuc, "Improved embedding for prediction-based reversible watermarking," IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, pp. 873-882, Sept. 2011.

