ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2013

A REVIEW ON STEGANOGRAPHY METHODS

Rakhi[1], Suresh Gawande[2]

P.G Student [Digital Comm.], Dept. of ECE, Bhabha Engineering Research Institute, Bhopal, Madhya Pradesh, India [1]

Assistant Professor, Dept. of ECE, Bhabha Engineering Research Institute, Bhopal, Madhya Pradesh, India [2]

ABSTRACT: In this paper we review different Steganography techniques for hiding the data. Steganography is a technique of hiding the data in any media in such a way that it remains confidential. This paper explores the different method of data hiding: image steganography, audio steganography, video steganography, text steganography, steganography in spatial domain, transform domain and adaptive steganography. The different aspects on which the steganography method depends are: robustness, capacity, undetectability and invisibility.

Keywords: Biometric, DCT, DWT, PSNR, Steganography.

I. INTRODUCTION

Steganography is a Greek work which means the covered writing. Steganography is an art of hiding data in a covered media (image, audio, video, text). In Steganography, we hide the mere presence of that it will be undetectable. The covered media is chosen in such a manner that it has capacity to hide the data and robustness that provides quality to the stego image. As in the upcoming years the need of data hiding, copyright protection, and confidentiality increases, steganography plays an important role in this field because of its some unique features. In this paper, we focus on the different steganography methods. This review paper provides some important information about steganography methods that will help in future researches in steganography and data hiding field. This paper is divided into different sections in which we explain steganography system, related work, different steganography methods and conclusion.

II. STEGANOGRAPHY SYSTEM

From the ancient times, Steganography is used to hide the secret data. The data was hidden on the back of wax, writing tables, stomach of rabbits or on the scalp of the slaves. And now a day, hacking is used for an unauthorized access of data so, to keep the data confidential, sender uses different methods. Steganography is one of the method in which the data is hidden in the cover object with the use of secret key. The extractor should have secret key to extract the data. The secret key designed in such a manner that it can't be find out by an unusual user. In Steganography systems following terms are used:

Cover Media: The cover media is the medium in which message is embedded to hide the presence of secret data.
Stego: The media through which the data is hidden.
Secret data: The data to be hidden or extract.
Steganalysis: The process by which secret data is to be extracted.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2013

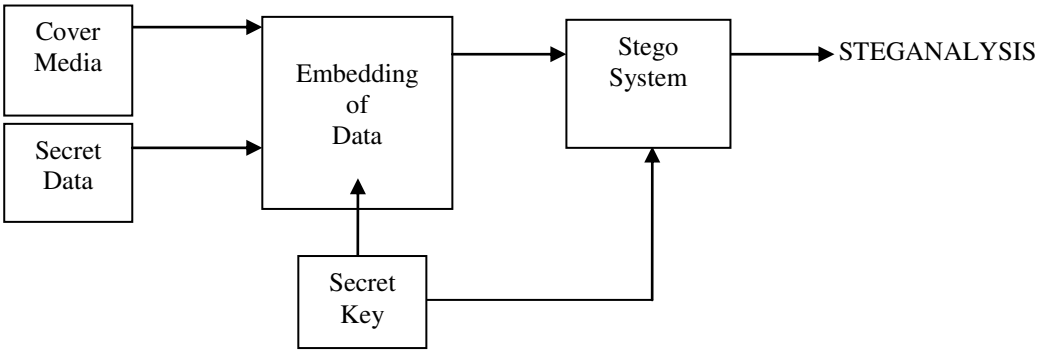

Figure 1: Steganography System

III. RELATED WORK

In related work, LSB is the most common method used to hide the message developed by Chandramouli [1] by applying the filtering, masking and transformation on the cover object. LSB matching revisited image steganography and edge adaptive scheme to which can select the embedding region according to the size of secret data is proposed by Weigi Luo [2].

Hassan Mathkour [3] use a new image steganography scheme based on LSB replacement technique and pixel value differencing. Chen Ming [4] discussed different steganography algorithms and tools into spatial domain, transform domain, document based and other categories such as spread spectrum technique and video compressing encoding. Mankun Xu [10] proposed a model based steganography technique which is based on least square method to estimate the embedding rates of secret information.

Anjali A. Shejul [7] proposed a DWT based approach for steganography using biometric features. Here, the secret data is embedded in skin region of image that provides secure location for data hiding. Secret data is hidden in one of the high frequency sub band of DWT by tracing skin pixels. All the steps of data hiding are applied on the cropped image. This provides security to the method and PSNR is used to determine the quality of stego image after embedding the secret data.

IV. STEGANOGRAPHY METHODS

Steganography is differentiated on the basis of the media in which we hide the data. These are: text, image, audio and video.

A. Text Steganography

The Steganography method uses the text media to hide the data known as text Steganography. There are different techniques to embed the secret data in text files.

- Format Based Method
- Random and Statistical Method
- Linguistics Method

Format Based Method: This method modifies the existing text to hide the data in such a manner that it involves the insertion of spaces, resizing the text, change the style of text.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2013

Random and Statistical Method: In this method characters are hidden that appeared in random sequence. Statistical method determines the statistics such as mean, variance and chi square text which measure the amount of redundant information to be hidden within the text.

Linguistics Method: It is the combination of syntax and semantics. Syntactic steganalysis ensure the correct structure as the text is generated from grammar. In semantic method value is assigned to synonyms and data can be encoded to the actual word of text.

B. Audio Steganography

When secret data is embedded into digital sound, the technique is known as audio steganography. This method embeds the secret message in WAV, AU and MP3 sound files. There are different methods through which audio steganography explored:

- Low Bit Encoding
- Phase Coding
- Spread Spectrum

Low Bit Encoding: This method is used by pitch period prediction is conducted during low bit speech encoding. Thus, maintaining synchronization between information hiding and speech encoding.

Phase Encoding: In this method, stream file splits audio into blocks and embed whole secret sequence into phase spectrum of the first block.

Spread Spectrum Encoding: One particular method of spread spectrum encoding is DSSS (Direct Sequence Spread Spectrum) which spread steganography by multiplying it by certain pseudorandom sequence.

C. Image Steganography

In this method, images are used as cover object. The image Steganography, data hiding method can be classified into different categories. These are spatial domain, frequency domain, and adaptive domain.

Spatial Domain Steganography: In spatial domain, cover image and secret data modified by using LSB and level encoding. First, the cover image is decomposed into bit planes and then LSB is of bit planes replaced with secret data fit. LSB substitution is the mostly used steganographic technique. This substitution concept includes embedding at the minimum weighting bit as it will not affect the value of original pixel. Luon Ching Lin [5] proposed a scheme of data hiding in spatial domain with tolerance of distortion. This method provides better image quality. The only drawback of the LSB insertion is the simplicity of extraction process. Thus, a secret listener can easily extract the data that we are sending.

Frequency Domain Steganography: In frequency domain, secret data is hidden in significant areas of covered image, which makes data invigorate to attacks such as compression, cropping or image processing methods than LSB approach. This provides an enhanced security level to steganography method and lead to the development of algorithms. This method transforms include DCT, DWT and DFT. A lossless and reversible scheme have been introduced that use each block of quantized DCT coefficient in JPEG image for secret data [6]. The method results in high stego image quality and achieves reversibility.DCT coefficients of an image used for embedding data bits. F5 embeds data in DCT coefficient by rounding the quantized coefficients to the nearest data bit.

It also uses matrix encoding for reducing the embedded noise in the signal. F5 is one of the most popular embedding schemes in DCT domain. Wavelet Transform (WT) converts spatial domain information to the frequency domain information. Wavelets are used in image because wavelet separately partitions the high frequency and low frequency information pixel by pixel. This scheme mainly addresses the capacity and robustness of the data hiding system.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2013

In recent year, DWT based algorithm for image has been proposed. These algorithms use CH band of cover image for hiding secret data.

Adaptive Steganography: This steganography method is a special case of two methods: spatial domain and transform domain. It is also known as "Statistics Aware Embedding" and "Masking". Global features of images are used before embedding secret data in coefficients of DCT or DWT. This statistics will decide where changes can be made.

V. CONCLUSION

In the past few years, Steganography has become an interested field of data hiding techniques. This paper provides an overview of different steganography methods that satisfy the most important factors of steganography design. These are undetectability, capacity and robustness.

ACKNOWLEDGEMENT

The authors would like to thanks to the earlier work regarding different Steganography methods that contribute the work made in this paper. All work done in this paper will surely help to the researchers for future work on Steganography methods.

REFERENCES

[1] N. F. Johnson, S. Jajodia, "Exploring Steganography: Seeing the Unseen", IEEE Computer vol. 31, issue 2, pp. 26-34, 1998.

[2] J. C. Judge, "Steganography: Past, Present, Future", SANS Institute Publications, 2001.

[3] Artz D., "Digital Steganography: Hiding Data within Data", Internet Computing IEEE, vol. 5, issue 3, pp. 75-80, 2001.

[4] Jar no Mielikainen, "LSB Matching Revisited", Signal Processing letters, IEEE, vol. 13, issue 5, pp. 285-287, May 2006.

[5] L-C. Lin, "Hiding Data in Spatial Domain with Distortion Tolerance", Computer Standard & Interfaces 31, pp. 458-464, (2009).

[6] C-C. Chang, "Reversible Hiding in DCT based Compressed Images", Information Sciences 177, pp. 2768-2786, (2007).

[7] Anjali A. Shejul, Prof. U. L. Kulkarni, "A DWT based Approach for Steganography using Biometric", International Conference On Data Storage and Data Engineering, IEEE, pp. 39-43, 2010.

[8] Provos N. and Honeyman P, "Hide and Seek: An Introduction to Steganography", IEEE Security and Privacy, vol. 01, issue 3, pp. 32-44, May-June 2003.

[9] Shaveta Mahajan, Arpinder Singh, "A Review of Methods and Approach for Secure Steganography", International Journal of Advanced Research Computer Science and Software Engineering, vol 2, issue 10, pp. 67-70, October 2012.

[10] K. Gopalan. , "Audio steganography using bit modification", IEEE International Conference on Acoustics, Speech, and Signal Processing, (ICASSP '03), vol 2, pp. 6-10, April 2003.