www.ijarcsse.com

Volume 2, Issue 10, October 2012 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Review of Methods and Approach for Secure Stegnography

Shaveta Mahajan, Arpinder Singh

Department of Computer Science & Engineering
B.C.E.T, Gurdaspur (Punjab)

Abstract: In this paper we survey different steganography techniques for encrypting the data. Steganography is a technique that allows the one to hide the data within an image while adding few noticeable changes. This paper discusses the concept behind the steganography by exploring firstly what is the steganography and the terms that are related to steganography. This paper explores the steganography methods –image steganography, audio steganography, video steganography, text steganography that are used to embed the information in digital carriers. The two most important aspects of image based stegnography system are the quality of stego image and the capacity of the cover image. By reviewing this paper, researchers can develop a better steganography technique to increase the MHC and PSNR value by analyzing the existing steganalysis techniques.

***Keyword**: steganography, image-audio- video -text steganography, MHC and PSNR*

1. Introduction

Steganography is derived from Greek words Steganous meaning “covered” and graphy meaning “writing”.So it is known as “covered writing”.Steganography is a technique which is used to hide the message and prevent the detection of hidden message. Image stegnography [1] is a modern way of hiding information in a way that the unwanted people may not access the information. Data used to hide data in stegnography can be text or image. In modern times, image stegnography can be helpful in a number of ways such as hiding the secret data [2], data authentication, ensuring authenticated data availability for academic usage, monitoring of data piracy, labelling electronic data/contents, copyright protection, ownership identification, providing confidentiality
and integrity enhancement control of electronic data piracy etc.[3].

Accordingly, the structure of this paper is as follows: Section 2 reviews the Steganographic Terms. Section 3 provides a state-of-art review and analysis of different existing methods of Steganography drawn from literature survey. Steganography Applications are presented in Section 4. Section 5 review the different types of Steganography. Finally, the Proposed method and conclusion is presented in Section 6.

2. Steganographic Terms

- Cover File:It is a file in which hidden information will be stored.
- Stego Medium: Medium through which the information is hidden.
- Message: The data to be hidden or extracted.
- Steganalysis: Identify the existence of message.
-

3. Related work:

In the related work, the most common method which is used to hide the message involve the usage of LSB developed by Chandramouli et al.[1],by applying the filtering, masking and transformation on the cover media. Weiqi Luo el al.,[2] proposed LSB matching revisited image steganography and edge adaptive scheme which can select the embedding regions according to the size of secret message For large embedding rates, smooth edge regions are used while for lower embedding rate, sharper regions are used.Ahn et al.,[3] propose an image steganographic method based on chaos and euler Theorem in which hidden message can be recovered using orbits which is different from the embedding orbits, and the original image is not required to extract the hidden message. Hassan Mathkour et al., [4]use a new Image steganography scheme based on LSB replacement technique and pixel value differencing. This scheme involve replacement of least significant bits in order to hide the colored message image with the advanced LSB methodology wherein the bit replacement takes place in accordance to range specified for the color images. Dobisicek et al., [5] proposed an authentication model of steganography to detect any attack on the stego image by modifies two coefficients of the Discrete Wavelet Transform in each row of cover image based on a verification code. Neil Provo et al.,[6]has proposed another method to counter the statistical attack is known as Out Guess .In this method corrections are made to the coefficients to make the stego-image histogram match the cover image histogram.Pavan et al.,[7] used entropy based technique for finding the coefficients in the image where message can be embedded with minimum distortion. Mohammad Shirali-Shahreza [8] proposed a synonym text steganographic technique in which the words in American English are substituted by the words having different terms in British English and vice-versa. Chen Ming et al., [9] discussed different steganography tool algorithms and classified the tools into spatial domain, transform domain, document based, file structure based and other categories such as spread spectrum technique and video compressing encoding.

- Mankun Xu et al., [10] proposed a Model Based steganography technique which is based on least square method to estimate the embedding rates of secret information .

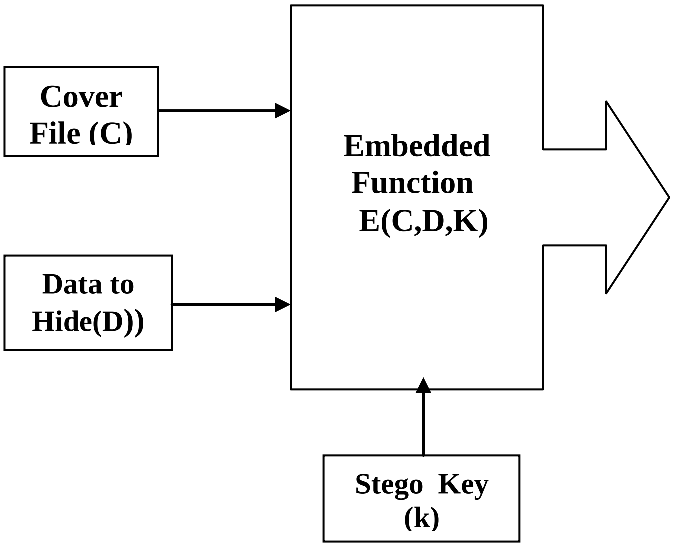

Figure1: **Steganography Diagram**

4. Steganography Applications

Steganography provide secure communication and help in storing of secret data.

It can hide a secret message in another message, be it text, image, audio or whatever media you decide to hide the secret message in it. Other applications are TV broadcasting, video-audio synchronization, protection of data alteration, companies safe circulation of secret data, Access control system for digital content distribution, TCP/IP packets(in which unique ID can be embedded into an image to analyze the network traffic of particular users.

5. Steganography Types

Steganography may be classified as pure, symmetric and asymmetric. While pure steganography does not need any exchange of information, symmetric and asymmetric need to exchange of keys prior sending the messages. Steganography is highly dependent on the type of media being used to hide the information. Medium being commonly used include text, images, audio files, and network protocols used in network transmissions .

Image Steganography is generally more preferred media because of its harmlessness and attraction. Additionally exchange of greetings through digital means is on the increase through the increased used of the internet and ease of comfort and flexibility is sending them. Technology advancement in design of cameras and digital images being saved in cameras and then transfer to PCs [12] has also enhanced many folds. Secondly, the text messages hidden in the images does not distort the image and there are techniques which only disturb only one bit of an image who's effects is almost negligible on its quality.

The major drawbacks of steganography is that one can hide very little information in the media selected.Some methods are following.

- Encoding secret message in text/documents
- Encoding secret message in audio
- Encoding secret message in images

5.1Text Steganography:

Text Steganography embed the secret data in text files through various techniques:

- **Format based Method**
- **Random and statistical method**
- **linguistic method.**

5.1.1 Format based method:

This method modifies the existing text in order to hide the steganographic text. Format Based Method involves the insertion of spaces, resizing the text, change the style of text to hide the secret message.

5.1.2 Random and statistical method:

Random method hide the characters that are appeared in random sequence.Statistical methods [13]determine the statistics such as means, variance and chi square test which can measure the amount of redundant information to be hide within the text.

5.1.3 Linguistic Method:

Linguistic method is a combination of syntax and semantics methods.Linguistic steganography considers the linguistic properties of generated and modified text, and uses linguistic structure as the space in which messages are hidden. Syntactic steganalysis is to ensure that structures are syntactically correct. Because the text is generated from the grammar, unless the grammar is syntactically flawed, the text is guaranteed to be syntactically correct.In Semantic Method you can assign the value to synonyms and data can be encoded into actual words of text.

5.2 Audio Steganography:

Embedding secret messages into digital sound is known as audio Steganography. Audio
Steganography methods can embed messages in WAV, AU, and even MP3 sound files. there are three techniques that are used in audio steganography are:

- Low bit Encoding
- Phase Encoding
- Spread Spectrum Encoding

5.2.1 Low Bit Encoding:

It is used in audio communications like mobile communications and VOIP. It performs to embed the data while pitch period prediction is conducted during low bit-rate speech encoding, thus maintaining synchronization between information hiding and speech encoding.

5.2.2 Phase Encoding:

It split the original audio stream file into blocks and embeds the whole secret sequence into the phase spectrum of the first block. One drawback of the phase encoding method is that less message capacity because message is stored in only first block.

5.2.3 Spread Spectrum Encoding:

It is a form of radio frequency communication. Data sent using the spread spectrum encoding is intentionally spread across as much of the frequency spectrum as possible.

One Particular method of Spread Spectrum Encoding is DSSS(Direct Sequence Spread Spectrum) which spread signal by multiplying it by a certain maximal length pseudorandom sequence, which is known as chip. Then the calculation of start and end quanta is taken by the discrete, sampled nature of host signal for phase locking purpose. As a result, higher chip rate occur and you can hide maximum data in that chip.

5.3 Image steganography:

Images are cover object used for steganography. Image files are used for storing of digital images. An image file may store data in compressed, uncompressed format. In Image Steganography ,data hiding method can be classified into two categories. They are spatial domain and frequency domain. Spatial [14] involve direct manipulation of pixels in an image. Frequency domain techniques is based on modifying the Fourier transform of an image.
Steganography algorithm operate on three types of images:Pallete based images(i.e.GIF images),Raw images(i.e,BMP format) and JPEG images. One of the most popular format used on the internet is JPEG(Joint Photographic Expert Group).It provide large compression ratio and maintain high image quality by measuring PSNR value.

In the JPEG compression, an image is divided into 8*8 blocks and then DCT is applied on each block. **Discrete Cosine Transformation** [15] is used for data compression. It is Similar to Fast Fourier Transform, DCT converts data (pixels, waveforms, etc.) into sets of frequencies. After that resultant DCT coefficient matrix is quantized using a quantization table.

Quantization table is a matrix just contain DCT coefficients. Finally the inverse DCT of quantized coefficients is evaluated and finally jpeg image is obtained.

5.3.1 Jpeg-Jsteg

In Steganography, there is JPEG data hiding tool jpeg-jsteg. It embed the data into least significant bits of the quantized DCT coefficients where values is not 0,1,-1.The main disadvantage of Jpeg-Jsteg has less capacity to hide the message.Also,Andreas Westfield noticed that by modifying low frequency coefficients cause a distortion detectable by a steganographic method.

6. Proposed method

As mentioned in the previous section, almost all steganography research done in the JPEG transformation domain which divides a given cover image into non-overlapping blocks of 8*8 pixels. Since the research to increase the message hiding capacity by proposing a new steganography method based on JPEG and quantization table is a continuous process.

7. Conclusion

In the past few years, the steganography is interested topic for image cover media.This paper provide an overview of steganography and introduce some techniques of steganography which help to embed the data.These techniques are more useful for detecting the stego images as well as the image media relating to security of of images and embed the data for complex image area and you can easily estimate the high embedding rate by using the quantitative steganalytic technique.

REFERENCES:

[1] N.F. Johnson, S. Jajodia, Exploring steganography: seeing the unseen, IEEE Computer 31 (2) (1998) 26–34.
[2] J.C.Judge, Steganography: past, present, future. SANS Institute publication, <http://www.sans.org/ reading room/ whitepapers/ stenganography/ 552.php>, 2001
[3] F.A.P.Petitcolas, R.J.Anderson, M.G.Kuhn:"Information Hiding- A Survey", Process of IEEE, vol.87,no.7, pp.1062-1078, July, 1999.
[4]Artz D (2001). "Digital steganography: hiding data within data" Internet Computing. IEEE, 5(3): 75-80
[5] Derek Upham, Jsteg, http://zooid.org/ Paul/crypto/jsteg.
[6] Nassir Memon R. Chandramouli. Analysis of lbs. based image steganography techniques. In *Proceedings of IEEE ICIP*, 2001.
[7] R. Chandramouli, Nassir Memon, "Analysis of LSB Based Image Steganography Techniques", IEEE 2001.
[8] K. Sullivan, Z. Bi, U. Madhow, S. Chandrasekaran, and B. S. Manjunath, Steganalysis of quantization index modulation data hiding, Proc. of 2004 IEEE International Conference on Image Processing, vol. 2, pp. 1165-1168, 2004.
[9]Jar no Mielikainen, "LSB Matching Revisited", Signal Processing Letters, IEEE, Publication Date: May 2006 Volume : 13, Issue : 5, pp. 285- 287
[10] K. Gopalan. Audio steganography using bit modification. In Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing, (ICASSP '03), volume 2, pages 421–424, 6-10 April 2003.
[11] Xuping Huang, Ryota Kawashima, Norihisa Segawa, Yoshihiko Abe. "The Real-Time Steganograph Based on Audio-o-Audio Data Bit Stream",Technical report of IEICE, ISEC, vol.106 pp.15-22, September 2006.
[12] Haz Malik, Steganalysis of qim steganography using irregularity measure, Proc. of the 10th ACM workshop on Multimedia and security, ACM Press, pp. 149-158, 2008.
[13] A. Delforouz, Mohammad Pooyan, "Adaptive Digital Audio Steganography Based on Integer wavelet transform ", IEEE Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2007, 26-28 Nov 2007, pp 283-286.
[14] M. Goljan, J. Fridrich, and T. Holotyak, New blind steganalysis and its implications, IST/SPIE Electronic Imaging: Security, Steganography of Multimedia Contents VIII, vol.
6072, pp. 1-13, 2006.
[15] Y. Wang and P. Moulin, Optimized feature extraction for learning-based image steganalysis, IEEE Trans. Information Forensics and Security, vol. 2, no. 1, pp. 31-45, 2007.
[16] Jan Kodovsky and J. Fridrich, Inuence of embedding strategies on security of steganographic methods in the jpeg domain, Proc. of IST/SPIE Electronic Imaging: Security, Forensics, Steganography Contents X, vol. 6819, pp. 1-13, 2008.
[17] M.H. Shirali-Shahreza and M. Shirali-Shahreza. Text steganography in chat. In Proceedings of the Third IEEE/IFIP International Conference in Central Asia on Interne the Next Generation of Mobile, Wireless and Optical Communications Networks (ICI 2007), Tashkent, Uzbekistan, September 26-28, 2007.
[18] C.Y. Yang, .Color Image Steganography based on Module Substitutions,. Third International Conference on International Information Hiding and Multimedia Signal Processing Year of Publication: 2007 ISBN:0-7695-2994-1.
[19] Yincheng Qi, Jianwen Fu, and Jinsha Yuan, "Wavelet domain audio steganalysis based on statistical moments of histogram", Journal of System Simulation, Vol 20, No. 7, pp. 1912-1914, April 2008.
[20] Sutaone, M.S., Khandare, M.V, "Image based steganography using LSB insertion technique", IEEE WMMN, January 2008.