International Journal of Engineering Sciences &Research Technology

(A Peer Reviewed Online Journal)
Impact Factor: 5.164

IJESRT

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A REVIEW ON VARIOUS STEGANOGRAPHY METHODS

Athira K J*[1] & Deepa T R *[2]
[1]PG Scholar, [2]Assistant Professor
[*]Dept. of Electronics and Communication Engineering, College of Engineering Karunagappally, Kollam, India

DOI: 10.5281/zenodo.2629274

ABSTRACT

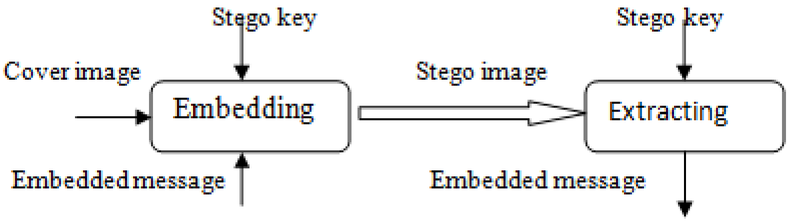
In today's life internet has played a significant role. To secure the important information for government organization, business, industries and individuals making use of cyberspace. Steganography plays a vital role in hiding the presence of the secret information. For hiding information in different cover media, different methods have been developed. The main goal of steganography is to hide information in the cover media so that other person will not notice the presence of information. . In this paper we discussed about various steganography techniques for hiding secret message or data.

KEYWORDS: Steganography, Audio Steganography, Video Steganography, Text Steganography..

1. INTRODUCTION

Communication plays a vital role in this modern world and everybody wants to hold the secrecy and safety of their communicating data. Cryptography and steganography are the two most prominent techniques used inorder to share the information in a concealed manner. Cryptography changes the appearance of the data by encrypting it but with the cryptanalysis and crypto attackers researches have looked into an alternative method like steganography. Steganography is the art of hiding message in a cover media without being suspected by a third party. Steganography and cryptography [1] both are similar in a way that they both are used to protect important information. The difference between them is that Steganography involves hiding information so it appears that there is no information is hidden at all. If a person views the object that the information is hidden inside then he will not have any idea that the information is hidden therefore the person will not attempt to decrypt the information. From the ancient times itself steganography is used to hide data. The data was hidden on back of wax, on the scalp of slaves and so on. In modern world unauthorized hacking of data is increasing so to keep data highly confidential is necessary so the sender uses different methods, steganography is one of the important method.

In steganography the actual information is not maintained in its original format, it is converted into another media file (image, video or audio) which is hidden in another object. The data is hidden in a cover media with the use of a secret key called stego key. The recipient should have the stego key to extract the data. The stego key is designed in such a manner that it can't be find out by an unusual user. Information hidden inside the files maybe public knowledge in watermarking and fingerprinting,[2] it may be visible sometimes but in case of steganography the secrecy of information is crucial. The process of steganography techniques can be defined into 4 categories such as text, image, audio and video [3].Historically the most important method of steganography is hiding information in text. Since text files have a very small redundant data so steganography using digital data is not used very often. Most widely used cover for steganography in now a day is digital image because of having large amount of redundant bits present in the digital representation of images. Similar techniques used in image files are used to hide information in audio files. Masking is one of the unique techniques used in audio. It is less popular to use because of the larger size of meaningful audio files than images. Video steganography is considered as a method of hiding information in video files.



In this paper various steganography methods are discussed.

2. MATERIALS AND METHODS

On the basis of the media in which we hide the data, steganography is differentiated. These are: text, image, audio and video [4]

2.1 Text Steganography

Text steganography is a steganography method that hides data using text media. For embedding secret data in text file, different techniques are used. They are format based method, random and statistical method and then linguistics method.

2.1.1 *Format Based Method*

This method involves the insertion of spaces, resizing the text, changing the style of text such that it modifies the existing text to hide the data.

2.1.2 *Random and Statistical Method*

In this method characters hidden are appeared in a 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.

2.1.3 *Linguistics Method*

This method is a combination of syntax and semantics. Syntactic steganalysis check the correct structure as the text is generated from grammar. In semantic method the data can be encoded to the actual word of text and the value is assigned to synonyms.

2.2 Audio Steganography

Audio steganography is a technique in which the secret data is embedded into digital sound. This method uses sound files to embed the secret message. Audio message can be explored using different methods such as Low Bit Encoding, Phase Coding and Spread Spectrum.

2.2.1 *Low Bit Encoding*

This method is conducted during low bit speech encoding which is used by pitch period prediction. Thus synchronization between speech encoding and information hiding is maintained.

2.2.2 *Phase Coding*

Here the audio is splitted into blocks by the stream files and into phase spectrum of the first block the whole secret sequence is embedded.

2.2.3 *Spread Spectrum*

Direct Sequence Spread Spectrum which spread steganography by multiplying it by certain pseudorandom sequence, which is one of a particular method of spread spectrum encoding.

2.3 Image Steganography

Image steganography method uses image as cover object. In image steganography, data hiding method can be classified into different categories such as spatial domain, frequency domain and adaptive domain.

2.3.1 *Spatial Domain Steganography*

In this method LSB and level encoding is used to modify cover image and secret data. One of the mostly used steganography technique is LSB substitution. this method provides better image quality. It has a drawback that is the simplicity in extraction process. Thus the secret data that we send can be easily extracted by a secret listener.

2.3.2 *Frequency Domain Steganography*

In frequency domain the secret data is hidden in appropriate areas of covered image. In this method the security is enhanced and this leads to the development of algorithms. This method also includes DCT, DWT and DFT. This method results in high stego image quality and reversibility is achieved.

2.3.2 *Adaptive Domain Steganography*

In adaptive domain steganography, there includes two methods, spatial domain and transform domain. Before embedding secret data in coefficients of DCT or DWT, global features of the images are used. This statistics will decide where the changes can be made.

2.4 Video Steganography

For hiding the secret information in video file, video steganography is used. Most of the presented techniques on images and audio can be applied to video files too, generally video files is the collection of images and sound. It is a moving stream of images and sound and large amount of data can be hidden inside. The video steganography is nothing but a combination of image and audio steganography [5].

3. LITERATURE REVIEW

Hiding data in images by simple LSB Substitution method has been proposed by Chan and Cheng [6] in the year 2003.In this paper enhancing the Stego image quality which is obtained by the simple LSB substitution method, which uses optimal pixel adjustment process (OPAP). For checking the embedding error between original image and Stego image OPAP is used. This method is applied on grayscale images in which 2-4 bits of original cover image pixels are used for the secret data bits embedding. From the PSNR of image, the quality of the image is calculated.

Zlii, Yang and Xian (2003) [7] has proposed LSB Steganography Detection Algorithm Gradient Energy-Flipping Rate detection (CEFR). The length of the embedded message is estimated by the analysis of the variation of the gradient energy, LSB steganography in color and grayscale image. This method conclude that it detect the presence of secret message and the embedding length when the estimation error is constraint within 10% when the embedding rate is greater than 0.05 bits per pixel. On the spatial LSB domain steganography this method is applied.

In this paper, for detecting messages hidden in WAV files, Ru, Zhang, Huang (2005) [8] proposed a steganographic tool Steghide. In this paper a linear predictor was used for the magnitude of wavelet sub band coefficients to extract significant statistics features, and employing support vector machines to detect the existence of hidden messages. To capture the faint changes of relation between neighbor samples caused by embedding, linear predictor is used.

Based on Lifting Wavelet Transform, Pooyan and Delforouzi (2007) [9] proposed LSB-based Audio Steganography method. The encrypted covert data is embedded into the wavelet coefficients of host audio signal the encrypted covert data is embedded. The calculation is done by hearing the threshold in wavelet domain. Then according to this threshold data bits are embedded in the least significant bits of lifting wavelet technique is reformed to increase the robustness coefficients. To construct stego signal in time domain the inverse lifting wavelet transform is applied to modified coefficients.

A high capacity data hiding using PVD and LSB Replacement Method was proposed by Kim, Jung and Yoo (2008) [10]. Here the calculation of the difference value between two consecutive pixels is done. The LSB substitution method is used, when the difference value is small then the LSB substitution method is used and when it is large then PVD is used. This method is very useful in grayscale images.

A steganographic communication channel using mp3 and wave audio signals was proposed by Garay, Medina, Rivera and Ponomaryov (2008)[11].Here Direct Sequence Spread Spectrum(DSSS) is used to insert highly confidential data in MP3 and WAV audio digital signals. To evaluate the proposed algorithm filtering, re-sampling, noise addition, echo addition and MPEG compression were used.

A security model for the Text steganography was proposed by Bhattacharya, Das, Bandopadhya and Kim (2009) [12]. In this model security has been imposed between cryptography and steganography which is a combination. The format of the normal encrypted message has been changed by the extra layer so that it provides more privacy and secrecy by using cryptography and steganography respectively. Two secret keys are used. For the color images, audio and video covers, this algorithm is very useful.

A general overview of the subject areas such as Steganography types, General steganography system, Characterization of steganography systems and Classification of steganography techniques have been provided by Zaidoon Kh.AL-Ani, A.A Zaidan and Hamdan (2010)[13]. Here the classification and characterization is explained deeply.

DWT based approach was proposed by Anjali A Shejul (2010) [14] using biometric features for steganography. Here, it provides a secure location for data hiding by embedding secret data in skin region. On the cropped image all the steps of data hiding are applied. The quality of the stego image is determined by the PSNR after embedding the secret data and also it provides security to the method.

Dr. Emad S. Othman (2012) [15] has proposed a paper on embedding audio into RGB 24-bit color image sporadically using linked list concept. In this paper a new approach has been proposed to overcome the drawbacks of the existing techniques for image steganography. In this project for the combination of cryptography and steganography a new robust system has been introduced.

Rosziati Ibrahim and Teoh Suk Kuan (2011)[16] proposed a new algorithm to hide data inside a image steganography technique. Here binary codes and pixels inside an image is used. Before it is converted to binary codes to maximize the storage of data inside the image the zipped file is used. By applying the proposed algorithm, a system called Steganography Imaging System (SIS) is developed. To see the viability of the proposed algorithm the system is then tested. PSNR is also captured for each of the images. The new algorithm is very efficient to keep the data confidential inside the image.

Nitin Kaul and Nikesh Bajaj (2013)[17] uses LSB technique and wavelet transform for an audio message to be embedded in an image. This paper describes, in an image how maximum speech can be embedded.The difference between original image and stego image was not detectable and the audio after reconstruction was similar to the original audio.

Devendra Singh Rao and Pankaj Singh Parihar (2014)[18] , in this paper uses PNG.JPEG,BMP and TIFF images are used as covers. In WAV data format secret data is taken from the audio. For embedding audio data into RGB components of cover images an approach is suggested.

4. CONCLUSION

In this paper we review about various steganography methods for hiding the secret messages through text, video, audio and image channels. By comparing with cryptography, steganography provides more security towards cyber attacks. It is highly imperceptible, secure and robust against various image processing attack. Steganography will play a vital role in secure transmission of secret message in the future digital world.

5. ACKNOWLEDGEMENTS

We would like to thank to our Principal Dr. Jaya V L and Head of the Department Dr. Gopakumar C for inspiring us to do this work and thank to all reference authors, reviewers who supported and helped to publish our work in this conference.

REFERENCES

[1] Rina Mishra and Praveen Bhanodiya, "A Review on Cryptography and Steganography" in IEEE International Conference, 2015

[2] Shang-Lin Hsieh,Chun-che chen and Wen-shan shen,"Combining Digital Watermarking and Fingerprinting Techniques to Identify Copyrights for Color Images"(2014) The Scientific World Journal Volume 2014, Article ID 454867

[3] Sandeep Singh and Aman Singh," A Review on the Various Recent Steganography Techniques''IJCSN International Journal of Computer Science and Network, Volume 2, Issue 6, December 2013

[4] Masoud Nosrati, Ronak Karimi and Mehdi Hariri," An introduction to steganography methods" World Applied Programming, Vol (1), No (3), August 2011. 191-195

[5] Mennatallah M. Sadek, Amal S Khalifa and Mostafa G.M.Mostafa,"Video Steganography: A comprehensive Review"Spinger Link, September 2015, volume 74.

[6] ChanK. C, Cheng L.M (2003), "hiding data in images in simple LSB substitution", Journal of pattern recognition,pp.469-474.

[7] Zlii Li,Yang S. A. F. , XianY(2003)," A LSB Steganography Detection Algorithm",The 14th IEEE 2003 International Symposium on Persona1,lndoor and Mobile Radio Communication Proceedings.pp.2780-2783.

[8] RuX. M, Zhang H. J, Huang X (2005), "Steganalysis Of Audio: Attacking The Steghide", Proceedings of the Fourth International Conference on Machine Learning and Cybernetics, Guangzhou, pp.3937-3942, pp.18-21.

[9] Pooyan M, Delforouzi A (2007), "LSB-based Audio Steganography Method Based on Lifting Wavelet Transform", 2007 IEEE International Symposium on Signal Processing and information technology, pp.600-603.

[10] Kim K. J, Jung K. H and YooK. Y (2008), "A high capacity data hiding method using PVD and LSBreplacement", International Conference on Computer Science and Software Engineering, pp.876-879.

[11] Garay S. H, Medina R. V, Rivera L. V and Ponomaryov V (2008), "Steganographic Communication Channel Using Audio Signals" ,12th International Conference on Mathematical Methods in Electromagnetic Theory,pp.427-429.

[12] BhattacharyaD, Das P, Bandyopadhyay S. K Kim T(2009),"Text Steganography: A Novel Approach ",International Journal of Advance Science and Technology,Vol.3,pp.79-86.

[13] Zaidoon Kh. AL-Ani, A.A .Zaidan, B.B .Zaidan and Hamdan.O.Alanazi,"Overview: Main Fundamentals for Steganography" JOURNAL OF COMPUTING, VOLUME 2, ISSUE 3, MARCH 2010, ISSN 2151-9617

[14] 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.

[15] Dr. Emad S. Othman, Senior Member IEEE, "Hide and Seek: Embedding Audio into RGB 24-bit Color Image Sporadically Using Linked List Concepts" IOSR Journal of Computer Engineering(2012).

[16] Rosziati Ibrahim and Teoh Suk Kuan(2011),"Steganography algorithm to hide secret message inside an image" Faculty of Computer Science and Information Technology, University Tun Hussein Onn Malaysia (UTHM), Batu Pahat 86400, Johor, Malaysia

[17] Nitin Kaul and Nikesh Bajaj (2013)," Audio in Image Steganography based on Wavelet Transform" International Journal of Computer Applications (0975 – 8887) Volume 79 – No3, October 2013.

[18] Devendra Singh Rao and Pankaj Parihar," Embedding Approach of Audio Data in RGB Images Using Circle Equation" International Journal on Recent and Innovation Trends in Computing and Communication Volume: 2 Issue: 7.