© 2016 IJSRSET | Volume 2 | Issue 3 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Analysis of Different Types of Steganography

Harjit Singh

Department of Computer Science, Punjabi University, Neighbourhood Campus, Dehla Seehan (Sangrur), Punjab, India

ABSTRACT

Modern era of digital communication raise many challenges in secrecy of data when it is transferred over the network. The data to be transferred over the network can be grabbed by third party on the way. Steganography is a method to hide secret data from third party. The secret data is embedded in some cover media in such a way that no one else is aware of it. Different cover media are available such as text files, image files, audio and video files etc. images are widely used as cover media. The secret data is embedded using various techniques available such as Least Significant Bit (LSB) insertion, Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) etc. But each of these techniques has its own strengths and weaknesses. This paper analyses different types of steganography and the techniques used to achieve those types of steganography.

Keywords: Steganography, Text, Image, Audio, Video, Network, Protocol, LSB, DCT, DWT.

I. INTRODUCTION

Steganography is a term related to embedding secret information into some cover media such as image, video, audio or text so that that embedded information could be transferred to the destination without being detected. It is a challenging area of research in modern times because each technique used for steganography has its own strengths and weaknesses.

Various types of cover medias can be used to embed information such as text steganography, image steganography, audio steganography, video steganography, network protocol steganography etc. Various steganography techniques such as Least Significant Bit (LSB) based steganography, Discrete Cosine Transform (DCT) based steganography and Discrete Wavelet Transform (DWT) based steganography are available.

As an example, an image can convey more than 1000 words; those remain hidden to Human Visual System (HVS). Methods hiding information in some cover media is steganography and attacks on these methods are called steganalysis.

Now a days, internet bandwidth has increased and cost of hardware has decreased. Due to the easily available hardware at low cost and increasing internet bandwidth, it is becoming difficult to transfer secure information over the internet. On the way, that information can be grabbed to use it for illegal purposes. In this situation, steganography is a way that is attracting the people to transfer information in a secure way.

II. METHODS AND MATERIAL

1. Steganography In Ancient Times

The word steganography is a greek word which means ‘concealed writing’. Historical facts show some methods of steganography even in 5th century. In those times the slaves were used to transfer information. The slave’s head was shaved and the message is tattooed on the skull. When the hair grew back, the slave was dispatched. [19, 20, 21, 22]

In Turkey and Germany, some ancient Arabic manuscripts were found on secret writing which have been written twelve hundred years ago. [23]

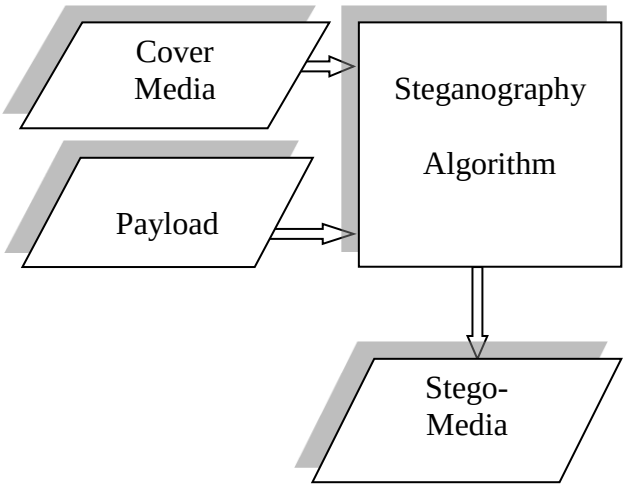
Italian mathematician reproduced a Chinese ancient method on secret writing about five hundred years ago. In this method, a paper with holes is placed over a blank

paper, the message is written in these holes. The paper with holes is taken off and blanks in between the message are filled to mix up the message. The receiver can use the paper with similar holes to read the secret message. [22] During World War II, Nazis invented some steganographic methods such as using the 3rd letter from each word to make a secret message. [20,24,25]
In 1945, a painting was used to hide some secret code in grass alongside the river. [26]

2. Steganography In Modern Times

Today is the era of digital processing, so steganography is now digital steganography. In digital steganography following terminology is used:

Cover Media: The cover media is the carrier in which the secret data is hidden such as an image file.
Payload: The secret data to be hidden in cover media.
Stego-Media: The media with embedded payload.
Steganography: The process using which the payload is embedded in the cover media.
Steganalysis: An attack on stego-media using which the hidden payload is to be extracted from it.



III. CLASSIFICATION OF STEGANOGRAPHY BASED ON COVER MEDIA

Based on the cover media used to hide the payload, the steganography can be classified into following different types:

A. Text Steganography

In this type of steganography, text is the cover media used to hide the payload. The message can be hidden in cover text by word shifting, line shifting, syntax, semantic or abbreviation based hiding techniques. These techniques can be divided into following categories:

Format based techniques: The format of text is changed to hide secret information. For example an extra space added in text is considered as '0' and two extra spaces added in text are considered as '1'. Word shifting is a way to add extra spaces between words to hide secret data. Similarly, line shifting is another similar way to hide data but it requires huge amount of text in a file. Text resizing slightly can also be used to hide secret message. Also the change in style such as bold or italic can be helpful to hide secret information in a text file.

Statistical Techniques: In these techniques the cover text is generated according the statistical properties. The character sequences or word sequences can be used for statistical generation of cover text. The character sequences which appear to be random might hide secret message. In word sequences, actual dictionary words can used to hide bits of information.

Linguistics Techniques: In these methods syntax and semantics is used to hide secret data. In syntactic methods, punctuation marks such as comma or full stop can be placed at proper places in text to hide secret message in text file. In semantic methods, the synonyms of words can be substituted to represent bits of secret information.

B. Image Steganography

When cover media is an image file, it is called image steganography. In this type of steganography, the image files such as JPEG, GIF, BMP, PNG etc. are used to embed secret bits of information. Image steganography can be accomplished by exploiting the image format, spatial domain steganography, frequency domain steganography and adaptive steganography.

The simplest method is appending the text file at the end of cover image file, thus exploiting the image format to store secret message. The message is added after the EOF (End of File) marker of image file, so when the image is viewed in some image viewer application, the file up to the EOF tag is displayed and anything after it

is ignored. It does not deteriorate the image quality, but it is very easy to attack. By just opening the image in a text editor, the message can be read.

In spatial domain steganography, Least Significant Bit (LSB) of the cover image is used to hide secret bits of information in a cover image. The method is based on the fact that changing the LSBs of an image does not affect the image because these LSBs contain random noise. Different algorithms use LSBs in their own way to store data, but it can be easily extracted using some tools.

In frequency domain steganography, the secret message is embedded in significant areas of cover image to reduce the chances of attacks and increase security of data. It includes Discrete Cosine Transform (DCT) based steganography, Discrete Wavelet Transform (DWT) based steganography. DCT is used for image and video where a block of DCT coefficients are obtained from an equation and then they are quantized with specific quantization table (QT). These DCT coefficients of image are used to embed bits of information. This method provides high quality stego-image. F5 is a popular scheme based on DCT which rounds the quantized coefficients to the nearest data bit and then embed data. In DWT, secret data is hidden CH band of cover image.

Spatial domain and frequency domain are basis for adaptive steganography. It is also called statistic aware embedding [21] or masking [19]. This technique makes use of statistical characteristics of image to find where the changes should take place in the image. Depending on the cover image, a random adaptive selection of pixels is made which is followed by the selection of pixels in a block with large standard deviation. The data to be embedded is converted to a noisy block which replaces the selected noisy block in the cover image.

C. Audio Steganography

A digital sound file such as MP3 or WAV can be used to embed secret message by shifting of binary sequence of that file. In a number of available steganography methods LSBs are modified with error diffusion. It is also possible to embed messages using inaudible frequencies.

The parity coding method encodes message bit in the parity bit of sample region after breaking the audio signal into regions.

The phase coding method encodes message bits in phase spectrum of audio signal as phase shifts because phase elements are inaudible to human.
In spread spectrum technique the secret data bits are spread across frequency spectrum.

D. Video Steganography

A video is a combination of images and optionally sound. So, huge amount of secret data can be encoded in video files. Video files such as MPEG, MP4, AVI etc. can be used for hiding secret information.

DCT which is used for image steganography, can also be applied for video steganography by hiding secret data in each image of video separately. LSB is also widely used with some variations for video steganography.

TPVD (Tri-way Pixel-Value Differencing) hides data in the I-frame.

Bit Plane Complexity Segmentation (BPCS) is also used for hiding data within MPEG Video.

E. Network Protocol Steganography

A network protocol such as TCP, UDP, IP, ICMP etc. can be used as a cover media for steganography. ISO layer network model provides covert channels which can be used for network protocol steganography.

Popular P2P services like Skype and P2P file sharing services like BitTorrent using network protocol steganography to hide secret data bits. Skype uses SkyDe (Skype Hide) steganography technique to hide secret messages. StegTorrent is a steganography technique used for P2P file sharing services.

TransSteg (Transcoding Steganography) is a steganography technique used for IP telephony services. WiPad is a network steganography technique used for WLANs.

IV. CONCLUSION AND RESEARCH SCOPE

An analysis of different types of steganography and the techniques used to achieve those types of steganography has been made though this paper. Each type of cover media has its own capacity to contain amount of data bits in it. Although, all the methods available for steganography try to assure capacity, undetectability and robustness, they have their own strengths and weaknesses. LSB method has high payload capacity but cannot prevent attacks, so low undetectability. Same is with other techniques as well.

There are many techniques available for image steganography, but very few are available for video and audio steganography. Although, image steganography methods are being used for video steganography but there is a need to develop specific techniques for video steganography which should provide improvement in visual quality, high capacity and undetectability over the existing techniques.

V. REFERENCES

[1] "An effective implementation of LSB Steganography using DWT techniques", K.P.Uday kanth and D.Vidyasagar, June2014.

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

[3] Amritha Sekhar, Manoj Kumar G., Prof. (Dr.) M. Abdul Rahiman, "A Study on Network Steganography Methods", International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE) Vol. 4, Special Issue 1, June 2015.

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

[5] "An Improved Inverted LSB Image Steganography" Nadeem Akhtar, Shahbaaz Khan, Pragati Johri, IEEE, 2014

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

[7] Vidhya Saraswathi, Mrs. Sumathy Kingslin, " Different Approaches to Text Steganography: A Comparison" International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-3, Issue-11)

[8] Sutaone M. S. and Khandare M. V. (2004) ,"Image Based Steganography Using LSB Insertion Technique", pp.146-151.

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

[10] International Journal of "Advanced Research in Computer Science and Software Engineering", Steganography Using Various Quantization Techniques",Tara Bansal,Ruuchika Lamba,Volume 3,Issue 7,July 2013.

[11] Rakhi1, Suresh Gawande, "A REVIEW ON STEGANOGRAPHY METHODS", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 2, Issue 10, October 2013

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

[13] Ru X. 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.

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

[15] Shahreza M. S and Shahreza M. H. S (2007) ,"Text Steganography in SMS", International

[16] S. Wendzel, W. Mazurczyk, L. Caviglione and M. Meier, Hidden and Uncontrolled - On the Emergence of Network Steganography Threats, ISSE, Brussels, Belgium, 2014.

[17] Steganography in mobile phone over bluetooth Shatha A. Baker1 and Dr. Ahmed S. Nori 2, August 2013. Conference on Convergence Information Technology, pp.2260-2265.

[18] 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.

[19] N.F.Johnson, S.Jajodia, Exploringsteganography : seeing the unseen, IEEE Computer31(2)(1998) 26–34.

[20] J. C. Judge, Steganography : past, present, future. SANS Institute publication, /http://www.sans.org/reading_room/whitepapers/ stenganography/552.phpS, 2001.
[21] N.Provos, P. Honeyman, Hideandseek : anintroduction to steganography, IEEE Security and Privacy1(3)(2003)32–414.
[22] P.Moulin,R.Koetter, Data-hidingcodes, Proceedings of the IEEE93 (12)(2005)2083–2126.
[23] S.B.Sadkhan,Cryptograph y: current statusand future trends, in: Proceedings of IEEE International Conference on Information & Communication Technologies : From The oryto Applications, Da- mascus. Syria, April19–23, 2004, pp.417–418.
[24] S. Lyu, H. Farid, Steganalysisusinghigher-orderimagestatistics, IEEE Transactions on Information Forensicsand Security1(1) (2006)111–119.
[25] D.Kahn,The code breakers : the comprehensive history of secret communication fromancienttimesto the Internet, Scribner, December 5,1996.
[26] J.P.Delahaye, Informationnoyee, informationcach, PourlaScience 229 (1996)142–146/ www.apprendre-en-ligne.net/crypto/stega no/229_142_146.pdfS (in French)..
[27] Abbas Cheddad, JoanCondell,KevinCurran, PaulMcKevitt “Digital image steganography: Survey and analysis of current methods”, Signal Processing 90 (2010) 727–752
[28] www.slideshare.net/jamesridgway/video-steganography