IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 20, Issue 6, Ver. I (Nov - Dec 2018), PP 16-19
www.iosrjournals.org

Steganography Techniques Used To Hide the Information

K.Priya
Assistant Professor, Islamiah Women's Art's and Science College, India

Abstract: *Steganography is a technique for hiding data behind the file such as image, audio, video etc. and that data securely transfer from sender to receiver. It serves as a better way of securing message than cryptography which only conceals the content of the message not the continuation of the message. Original message is being hidden within a file such that the changes so occurred in the file are not noticeable. To hide the secret information verity of steganography techniques can be used and are more complex than others while all of them have respective strong and weak points. The absolute invisibility of the secret information is maintained by different applications, while others require a large secret message to be hidden. This paper discussesan overview of image steganography, its uses and techniques to satisfy the need for privacy on the internet. Various steganography techniques to provide privacy while transferring data from source to destination.*

Keywords: *steganography, cryptography, secret information, digital image.*

Date of Submission: 22-10-2018 Date of acceptance: 05-11-2018

I. Introduction

The private information's need to send, store or receive frequently by the users through internet. The most common way to do this is to transform the data into a different form. The resulting data can be understood only by those who know how to return it to its original form. This method of protecting information is known asencryption. A major drawback to encryption is that the existence of data is not hidden. Data that has been encrypted, although unreadable, still exists as data. If given enough time, someone could eventually decrypt the data. A solution to this problem is steganography. The ancient art of hiding message is plain, but unsuspecting to the reader. The steganography's intent is to hide the existence of the message, while cryptography scrambles a message so that it cannot be understood.

II. History Of Steganography

Steganographic techniques have been used for ages and they date back to ancient Greece. The aim of steganographic communication back then and now, in modern applications, is the same: to hide secret data (a steganogram) in an innocently looking cover and send it to the proper recipient who is aware of the information hiding procedure. In an ideal situation the existence of hidden communication cannot be detected by third parties.

The most popular delivery service include digital images, audio and video files and Communication protocols. The latter may apply to network protocols as well as any other communication protocol (e.g. cryptographic).The way that people communicate evolved over ages and so did steganographic methods. At the same time, the general principles remained unchanged.

III. Uses Of Steganography

The uses of steganography are as varied as the uses of communication itself. Obviously we can use it to send secret messages to a friend, colleague, or co-conspirator. You can use it to transport sensitive data from point A to point B such that the transfer of the data is unknown.

- Confidential communication and secret data storing.
- Potential capability to hide the existence of confidential data.
- Hardness of detecting the hidden data.
- Enhancing the secrecy of the encrypted data.
- It is protecting the data alteration.
- Access control system for digital contents distribution, in this area embedded data is hidden but is explained to publicize the content.

IV. Types Of Steganograhy

1) Linguistic Steganography: Linguistic technique is used to hide the message within the cover text in non-obvious way such that the presence of message is imperceptible to an outsider. It is divided into two types:

A) SEMAGRAMS: It uses only symbols and signs to hide the information. It is further categorized into two ways:

- ❖ VISUAL SEMAGRAMS: A visual semagrams uses physical objects used every day to convey a message. For example: The positioning of items on a particular website.
- ❖ TEXT SEMAGRAMS: This type is used to hides a message by modify the appearance of carrier test, or by changing font size and type, or by adding extra space between words and by using different flourished in letters of handwritten text.

B) OPEN CODE: In this approach the message is embedded in legitimate paraphrases of cover text in the way such that it appears not obvious to an unsuspecting observer. It can be achieved by two ways viz., Jargon which is understood only by a group of peoples and Cipher which uses some concealed ciphers to hide a message openly in the carrier medium. A subset of jargon codes are cue codes, where certain prearranged phrases convey meaning.

2)Technical Steganography: Technical Steganography uses special tools, device or scientific methods to hide a message. In this type one can use invisible ink, microdots, computer based methods or various hiding places to keep message secret.

I)COVER: The cover message is the carrier of the message such as image, video, audio, text, or some other digital media. The cover is divided into blocks and message bits which are hidden in each block. The information is encoded by changing various properties of cover image. The cover blocks remain unchanged if message block is zero.

A)TEXT STEGANOGRAPHY: In this approach the cover text is produced by generating random character sequences, changing words within a text, using context-free grammars or by changing the formatting of an existing text to conceal the message. The cover text generated by this approach can qualify for linguistic steganography if text is linguistically driven. Although these text-based methods has its own unique characteristics for cover text but suffers from various problems from both a linguistic and security stand point.

B)IMAGE STEGANOGRAPHY: This Steganography technique is more popular in recent year than other steganography possibly because of the flood of electronic image information available with the advent of digital cameras and high-speed internet distribution. It can involve hiding information in the naturally occurred noise within the image. Most kinds of information contain some kind of noise. Noise refers to the imperfections inherent in the process of rendering an analog picture as a digital image. In image steganography we can hide message in pixels of an images. An image steganographic scheme is one kind of steganographic systems, where the secret message is hidden in a digital image with some hiding method [11]. Someone can then use a proper decoding procedure to recover the hidden message from the image. The original image is called a cover image in steganography, and the message-embedded image is called a stego image [12][13]. Various methods of image steganography are:

i)DATA HIDING METHOD : Hiding the data, a user name and password are required prior to use the system. Once the user has been login into the system, the user can use the information(data) together with the secret key to hide the data inside the chosen image. This method is used to hiding the existence of a message by hiding information into various carriers. This prevents the detections of hidden information.

ii)DATA EMBEDING METHOD: For retrieving the data, a secret key is required to retrieving back the data that have been embedded inside the image. Without the secret key, the data cannot be retrieved from the image. This is to ensure the integrity and confidentiality of the data. The process of embedding the message inside the image, a secret key is needed for retrieving the message back the image, the secret message that is extracted from the system is transfer into text file and then the text file is compressed into the zip file and zip text file is converting it into the binary codes.

iii) DATA EXTRACTING METHOD: It is used to retrieve an original message from the image, a secret key is needed for the verification. And for extracting method, a secret key is needed to check the key is correct with decodes from the series of binary code. If key is matched, the process continues by forming the binary code to a zipped text file, unzip the text file and transfer the secret message from the text file to retrieve the original secret message.

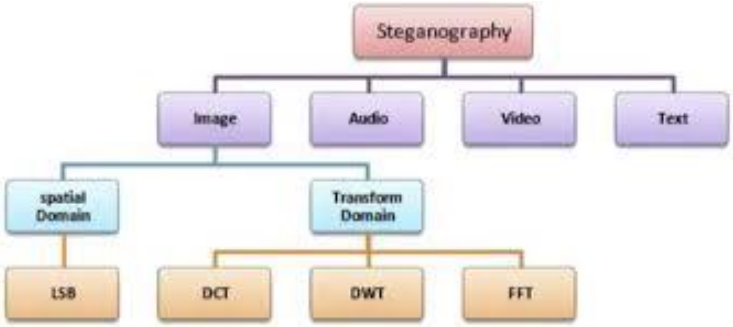

Figure 1 Types of Steganography

V. Steganalysis

The art of detecting steganography is referred to as Steganalysis. Steganalysis is the process of identifying steganography by inspecting various parameter of a stego media. The primary step of this process is to identify a suspected stego media. After that steganalysis process determines whether that media contains hidden message or not and then try to recover the message from it. The suspected media may or may not be with hidden message. The steganalysis process starts with set of suspected information streams. Then the set is reduced with the help of advance statistical methods. In the case of Visual detection steganalysis technique, a set of stego images are compared with original cover images and note the visible difference. Signature of the hidden message can be derived by comparing numerous images. Cropping or padding of image also is a visual clue of hidden message because some stego tool is cropping or padding blank spaces to fit the stego image into fixed size. Difference in file size between cover image and stego images increase or decrease of unique colors in stego images can also be used in the Visual Detection steganalysis technique. Steganalysis is the technique to detect steganography or defeat steganography.

VI. Steganography Vs Cryptography

STEGANOGRAPHY

Steganography is the practice of hiding a file, message, image, or video within another file, message, image, or video. Steganography requires two files: One is the message which has to be hidden, the other is the cover file which is used to hide the message.

CRYPTOGRAPHY

Cryptography or cryptology is the practice and study of techniques for secure message in the presence of third parties called opponents. More generally, cryptography is about construction and analyzing protocols that prevent third parties or the public from reading private messages

VII. Conclusion

Steganography is a fascinating and effective method of hiding data that has been used throughout history. This method used for hiding the information without affecting the original data.Regardless, the technology is easy to use and difficult to detect. This paper discusses the overview of a very existing and fast paced area of computer security. This technology has many in the security field worried as the possible harm that may be done to both government and private industries. There are already hundreds of steganography programs available that can be used on text, audio and graphic files. The government and many private companies are researching ways to best detect the use of steganography on files. The future work is based on finding effective technique in steganography to hide the information.

References

[1]. http://www.lia.deis.unibo.it/Courses/RetiDiCalcolatori/Progetti98/Fortini/history.html
[2]. http://stegano.net/tutorial/steg-history.html
[3]. https://null-byte.wonderhowto.com/how-to/introduction-steganography-its-uses-0155310/
[4]. Steganography and steganalysis-Robert Krenn, Internet Publication, March 2004 http://www.krenn.nl/univ/cry/steg/article.pdf
[5]. Steganography and Its Applications in Security, International Journal of Modern Engineering Research (IJMER) www.ijmer.com Vol.2, Issue.6, Nov-Dec. 2012 pp-4634-4638 ISSN: 2249-6645
[6]. https://www.quora.com/What-is-the-difference-between-cryptography-and-steganography
[7]. Singh, Nanhay, Bhoopesh Singh Bhati, and R. S. Raw. "Digital image Steganalysis for computer forensic investigation." Computer Science and Information Technology (CSIT) (2012): 161-168.
[8]. AL-Shatnawi, Atallah M., and Bader M. AlFawwaz. "An Integrated Image Steganography System with Improved Image Quality." Applied Mathematical Sciences 7.71 (2013): 3545-3553.

[9]. Bhattacharyya, Souvik and Gautam Sanyal. "A Robust Image Steganography using DWT Difference Modulation (DWTDM)." International Journal of Computer network & Information Security 4.7 (2012).
[10]. K. Bennett, "Linguistic Steganography: survey, analysis, and robustness concerns for hiding information in text" center for Education and Research in Information Assurance and Security,Purdue University 2004.
[11]. Hitesh Singh, Pradeep Kumar Singh, Kriti saroha "A Survey on Text Based Steganography" Proceedings of the 3rd National Conference; INDIACom-2009 Computing For Nation Development, February 26 – 27, 2009 Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi.
[12]. Jain, Nitin, Sachin Mesh ram, and Shikha Dubey. "Image Steganography Using LSB and Edge–Detection Technique. " International Journal of Soft Computing and Engineering (IJSCE) ISSN (2012): 2231-2307.
[13]. M. M. Amin, M. Salleh, S. Ibrahim, M.R. Katmin, M.Z.I. Shamsuddin, "Information Hiding using Steganography" Proceedings of 4th National Conference on Telecommunication Technology, Shah Alam , Malaysia, 2003.
[14]. Amin, Mohamed "Muhalim and Ibrahim, Subariah and Salleh, Mazleena and Katmin, Mohd rozi (2003) Information hiding using steganography.
[15]. Ibrahim, Rosziati, and Teoh suk Kuan. "Steganography Algorithm to hide secret message inside an Image." arXiv preprint arXiv: 1112.2809 (2011).

K.Priya. " Steganography Techniques Used To Hide the Information" IOSR Journal of Computer Engineering (IOSR-JCE) 20.6 (2018): 16-19.