IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified

Vol. 6, Issue 2, February 2017

A Review Paper on Steganography: Hiding Data within Data

Garima Malik

Department of Network Security Computer Science Engineering, Bhagat Phool Singh Mahila Vishwavidyalaya,

Sonipat University, Khanpur Kalan

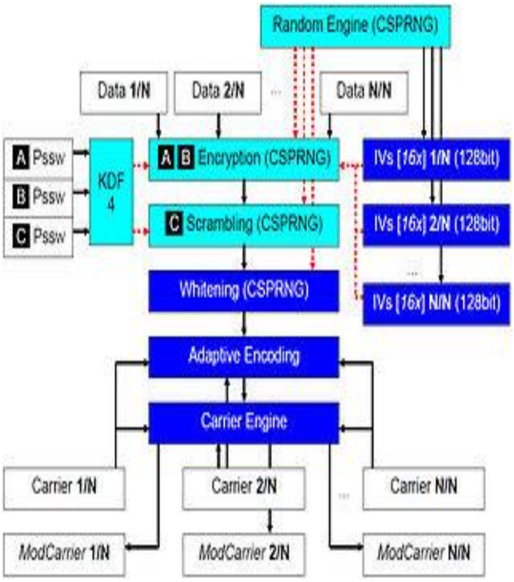
Abstract: Steganography Combine the two greek words steganoe (covered or protected), and graphein (writing). This simply implies for data hidden within data. In today's worlds, the most of the information kept electronically which create a fundamental issue of information security. This technique (steganography) used to hide the information in digital media (for example a image, video file, audio file etc), just like cryptography steganography is also used to protect the data from any third party, the only advantage of steganography over cryptography is that the intended secret message does not attract attention to itself as an object of scrutiny. So steganography also concerned with concealing the fact that the secure message being sent, whereas cryptography just protect the message. In this technology, the end user receive the data in the form of a image (which also known as carrier for data application) without anyone knowing that the image contains some critical information, so if the image is interpreted by any third party the data will not display to them, hence the data will secure during transmission. On the receiving end, the user uses a secure code to retrieve the data from the image. In this paper we discuss some application, technique of steganography, and also discuss how to detect the secret code.

Keywords: Steganography, data application, Data within Data, encryption system.

I. INTRODUCTION

Major disadvantages of using the encryption system for the security purpose is that, the existence of data can't be hidden. That's why a new a new secure purposed technique is invented to protect the data from an unauthorized user over a network. Steganography is the mostly used concept from the ancient times. Steganography concept is uses to hide the data that can be send but not the fact that two parties are communicating with each other. There are many methods and algorithms available for making an information secure under steganography, but for networks and computers there are many other technique for securing the information such as (convert channels, hiding data within the web pages, null cipher etc). As the need of technology increases it became more challenging to protect the data, so now steganography also becomes more sophisticated as compare to earlier techniques. One can now hide large amount of data within images or audio files.

Steganography uses the steganography software tools that allow a user to hide the data within a carrier file (i.e audio, video, images) and then extract the hidden data. A most widely used of steganography technique is watermarking that is commonly used for business purposes. Basically it (watermarking) is used for identifying a specific piece of information within a document that is marking by the person who is responsible for the security of the data without make it noticeable by any other person. For example if any digital image created by me, then I assign a watermark in the image file that identify me as the creator of this image. And this can be achieved by using the steganography.



Basic architecture of steganography

Carrier: In steganography carrier is a signal or a data file in which the hidden data is hidden after modification (audio, video, images file etc). Steganography uses a carrier signal (that can hide the data into a image or audio file) for sending the information to the end user which later can be extract by the receiver by using the secret key. This give a satisfaction to the user that his message is secure from any third party.

The next thing steganography architecture consist is a carrier chain, and a carrier chain is a set of files that can be splits from the hidden data. Carrier chain has a property that the all carrier are available unmodified and processed in the same order.

Steganography technique:
1. Physical: Steganography has the most widely used from the historical time, so some physical steganography includes:

- Hidden Wax messages: people wrote messages on wooden tablet and covered with wax.
- Uses of secret Inks: in ancient days people write down the messages on a paper using secret inks within a message or on the blank space of a page. Uses of postage stamps: acc. To this the message can be written in the area that can be covered by the postage stamps.

2. Digital messages: With the advent of personal computer modern steganography also introduces in 1985. Here the data can be modified into digital images, for this a no of software available :

- Messages can be concealing within lowest bits of noisy images or audio files.
- Hide the messages within the data itself.
- Changing the order of elements in a set.

Image of a tree with a hidden image

The image of cat extracting from the tree image.
The hidden image is identifying by removing all but the two least significant bits of each color.

• Making text as the same color as the background of the document in word document files.

Text before using digital steganography

• Using Unicode characters that's look like the standard ASCII.

3. Network: The data hiding technique used in telecommunication network steganography can be classified under network steganography.

Steganography sites

Data Hiding Homepage
http://nif.www.media.mit.edu/DataHiding/
Information Hiding homepage
http://www.cl.cam.ac.uk/~fapp2/steganography/
Steganalysis
http://www.jjtc.com/Steganalysis/
Steganography and Digital Watermarking
http://www.jjtc.com/Steganography/
StegoArchive.com
http://steganography.tripod.com/stego.html
Watermarking Mailing List
http://www.watermarkingworld.org/ml.html

DOI 10.17148/IJARCCE.2017.6247

Applications: Some basic application of digital steganograpgy are:

- Uses in modern printers.
- Used by intelligence services.
- Distributed steganography.
- Online challenges.

How to detect the hidden code: The art of detecting the hidden information is known as steganalysis. Two major aspect of detecting the code are information theory and statistical analysis. To protect the information the one can hide the data before transferring so the receiver on the receiving end needs to detect this hidden data by using the secret key provided to him, this process of extracting the data from the data is known as steganalysis. In other words, a set bit can represent the United States' national archives or this article, depending on how I choose to define my encoding. To a steganalysis expert unable to determine the chosen encoding, a bit is just a bit. If you don't believe me, try to find the hidden message in this sentence. I imagine you are not going to have much success, unless I tell you that I encoded the secret message "I own striped pajamas" as the text of the sentence. Steganalysis, though of great interest to businesses and governments alike, has not received the attention it deserves advantage in the market, the ability to control sensitive information is a critical part of maintaining a large institution.

II. CONCLUSION

In this system the designed tool deals with providing easy and secure information. The data is encrypted with key and embedded with an Image which is ready to send through communication channels. It is going to be reliable and secure. At the receiving end, the tool checks the availability of data and authenticates the data. It retrieves data from the stego image and decrypts it. Steganography is a fascinating and effective method of hiding data that has been used throughout history. Methods that can be employed to uncover such devious tactics, but the first step are awareness that such methods even exist. There are many good reasons as well to use this type of data hiding, including watermarking or a more secure central storage method for such things as passwords, or key processes. Regardless, the technology is easy to use and difficult to detect. The more that you know about its features and functionality, the more ahead you will be in the game.

REFERENCES

[1] S. Katzenbeisser and F.A.P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking,

[2] Artech House, Boston, 2000.

[3] B. Barán, S. Gómez, and V. Bogarín, "Steganographic Watermarking for Documents," Proc. 34th Ann. Hawaii Int'l Conf. System Sciences, IEEE CS Press, Los Alamitos, Calif., 2001.

[4] H.K. Pan, Y.Y. Chen, and Y.C. Tseng, "A Secure Data Hiding Scheme for Two-Color Images," Proc. Fifth IEEE Symp. Computers and Comm., IEEE Press, Piscataway, N.J., 2000.

[5] N.F. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen," Computer, vol. 31, no. 2, Feb. 1998,

[6] pp. 26-34.

[7] N.F. Johnson, Z. Duric, and S. Jajodia, Information Hiding: Steganography and Watermarking — Attacks and Countermeasures, Kluwer Academic Publishers, 2000. Available at http://www.jjtc.com/Steganography/.

[8] Wayner, Peter (2002). Disappearing cryptography: information hiding: steganography & watermarking. Amsterdam: MK/Morgan Kaufmann Publishers. ISBN 1-558-60769-2.

[9] Wayner, Peter (2009). Disappearing cryptography 3rd Edition: information hiding: steganography & watermarking. Amsterdam: MK/Morgan Kaufmann Publishers. ISBN 978-0-123-74479-1.

[10] Petitcolas, Fabien A.P.; Katzenbeisser, Stefan (2000). Information Hiding Techniques for Steganography and Digital Watermarking. Artech House Publishers. ISBN 1-580-53035-4.

[11] Johnson, Neil; Duric, Zoran; Jajodia, Sushil (2001). Information hiding: steganography and watermarking: attacks and countermeasures. Springer

DOI 10.17148/IJARCCE.2017.6247