International Journal of Progressive Research in Science and Engineering
Volume-1, Issue-2, May-2020
www.ijprse.com

An Overview about a Milestone in Information Security: STEGANOGRAPHY

Chandini M. S.

Assistant Professor, Department of Computer Science and Engineering
Ballari Institute of Technology and Management, Ballari-583104, Karnataka, India

***Abstract*:** In the latest trend of booming technology across the world, Information Security is paved with major concern of evolution and invention. Information security do not focus securing information from unauthorized access but also provides an aid for preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. The Original data that need to be processed can be physical or electrical one. Generally, Information Security program works on 3 objectives, commonly known as CIA triad– Confidentiality, Integrity, Availability. Along with many successful techniques to protect the data, the one technology that recently reverberated supporting the essence of information security is Steganography. The term Steganography is derived by a Greek word, having the context "art of concealing data into other data". This paper provides further a broad insight of steganography and its methods.

Key Words— Steganography, Information security, Cryptography.

I. INTRODUCTION

Steganography is derived from the Greek word; steganos (covered or secret) and -graphy (writing or drawing). The Simple definition of Steganography could be the procedure of concealing any kind of secret information inside a normal, document or message so as to avoid from data detection; the Secret information is then extricated at its intended destination. The difference between Steganography and very well-known Cryptography is the latest steganography concept will not pull the attention of the attacker to the concealed data, it obscures the presence of data; whereas in cryptography, the secret data is visible in the encrypted form that further take attacker interest to steal it. The Steganography concept can be accompanied with standard encryption technics as an additional progression for providing a strong level of security to the concealed data. Steganography can be utilized to hide realistically any kind of digitalized content, including content, picture, video or sound substance; the actual information to be concealed is called as Secret/Hidden message, the document that conceals it is called cover file. After concealing information in to it, the cover file is called as Stego-file. This process can be achieved by various algorithm based on the type of Actual secret and carrier file. The Information to be disguised through steganography - called hidden message - is concealed into the carrier file without affecting the quality of the carrier file.

II. HISTORICAL APPROACH OF STEGANOGRAPHY

Steganography can be said as a sophisticated process for hiding an information by embedding messages within other, seemingly harmless messages, graphics or sounds. The first steganography technique was developed in ancient Greece around 440 B.C. The Greek ruler Histaeus employed an early version of steganography which involved: shaving the head of a slave, tattooing the message on the slave's scalp, waiting for the growth of hair to avoid disclose of the secret message, and sending the slave on his way to deliver the message. The recipient would have the slave's head to uncover the message. The recipient would reply in the same form of steganography. In the same time period, another early form of steganography was employed. This method involved Demerstus, who wrote a message to the Spartans warning of eminent invasions from Xerxes. The message was carved on the wood of wax tablet, and then covered with a fresh layer of wax. This seemingly blank tablet was delivered with its hidden message successfully. Steganography continued development in the early 1600s as Sir Francis Bacon used a variation in type face to carry each bit of the encoding. During times of war steganography is used at vast wage. During the American Revolutionary War both the British and American forces used various forms of Invisible Inks that involved common sources such as milk, vinegar, fruit juice, and urine, for the hidden text. To decipher these hidden messages required light or heat. During World War II the Germans introduced microdots. The microdots were complete documents, pictures, and plans reduced in size to the size of a period and attached to common paperwork. Null ciphers were

also used to pass secret messages. Null ciphers are unencrypted messages with real messages embedded in the current text. Hidden messages were hard to interpret within the innocent messages. An example of an innocent message containing a null cipher is:

Fishing freshwater bends and saltwater coasts rewards anyone feeling stressed. Resourceful anglers usually find masterful leapers fun and admit swordfish rank overwhelming any day.

By taking the third letter in each word the following message emerges:

Send Lawyers, Guns, and Money.

III. STEGANOGRAPHY TECHNIQUES

In digital steganography, data is first encrypted and then inserted, using a special algorithm, into cover file that is part of a particular file format such as image, audio or video file. The secret message can be embedded into ordinary data files in many different ways. In General Information hiding is related to two fields, Steganography and watermarking. The key aspects to be taken care in information hiding are capacity, security, and robustness; maintaining them would avoid attention of attacker on the concealed data. Capacity means the amount of information that can be hidden, security refers to the inability of an eavesdropper to detect hidden information, and robustness to the amount of modification the cover medium can resist before the hidden information is corrupted. Following describes the process intact:

1. To Identify redundant bits in a cover file: Redundant bits are those bits that can be edited without taking care of the quality of the cover medium.

2. Select a subset of the redundant bits to be replaced with data from a secret message. One common technique which is illustrated on image cover file. Here the secret data bits(digitalized) is concealed in bits that represent the same color pixels repeated in a row in an image cover file. The result will be an image file that appears identical to the original image but that has "noise" patterns of regular, unencrypted data.

The modification of redundant bits is not visibly noticeable but that changes the statistical properties of the cover file. As a result, statistical analysis may reveal the hidden content.

Advantages over cryptography

Steganography concept is distinct from cryptography, but incorporating them together can help improve the security of the information and prevent detection of the secret communication. If steganographically-hidden data is also encrypted, the data may still be safe from detection -though the channel will no longer be safe from detection.

The primary advantage of using steganography is that it helps obscure the fact that there is sensitive data hidden in the file or other content carrying the hidden text. Whereas in Cryptography, message or network packet payload is clearly marked and identifiable as such, using steganographic techniques helps to obscure the presence of the secure channel

IV. USES OF STEGANOGRAPHY

Basically, Steganography used to carry out secret exchanges. The practice of adding a watermark -- a trademark or other identifying data hidden in multimedia or other content files -- is one common use of steganography. Watermarking is a technique which is used by online publishers to identify the source of media files that have been found being shared without permission. Also there are many different uses of steganography. For example, Governments are interested in two types of communication of hidden data: first, which supports national security and second, which does not. Steganography support both types, also business have similar concerns, about trade secrets for new technologies or products information. Of course, using steganography to communicate greatly reduces the risk of information leakage. Businesses takes advantage of watermarking. Steganography is polished by those wishing to pass on a mystery message or code. While there are many real uses for steganography, malware designers have additionally been found to utilize steganography to collect the transmission of code.

For example, using invisible ink to hide secret messages in a document; hiding documents by recording on microdot which measures 1mm in diameter -- on or inside legitimate-seeming correspondence; and even by using multiplayer gaming environments to share information

V. METHOD OF STEGANOGRAPHY

The methods that are available for digital Steganography is classified based on the cover file.

1. *Image as cover file*:

One of the ways to hide data is using images, which is a good method. The difficulty to reveal the data hidden increases with

the detailed in an image, and that makes it harder to guess or to suspect that image. There method of that, that embeds data in visually insignificant parts of an image. The user however can explore image degradation with different messages and images of different length. Another way is for GIF images, that modifies an image's palette for hiding its data.

2. *Audio as cover*:

A lot of packages also available for embedding and hiding data in the audio files. One of the tools for audio file hiding data is the MP3Stego, which does not only hide information effectively, arbitrary, rather also claims to be partly strong method of watermarking the targeted MP3 audio files. The WAV format, lets users hide data using StegoWave or Steghide. These sites refer to both programs in order. Steghide modifies the LSB of data to be transmit in the carrier medium. Using an audio file as a medium is less popular than using an image as a steganography medium.

3. Document as Cover:

Steganography in text focuses on altering some of its characteristics. They can either be characteristics of text or even text formatting. Taking the first letter of each word of the previous sentence, one can see that it is possible and not very difficult. Hiding information in plain text can be done in many different ways such as by simple adding white space and tabs to the ends of the lines of the document. Another possible way of storing a secret inside a text is using a publicly available cover source, a book or a newspaper, and using a code which consists for example of a combination of a page number, a line number and a character number. Setting background color and font color is one of the mainly used staganographic approach. select predefined colors and set font and background colors of invisible characters such as space, tab or the carriage return characters. R,G,B values are 8 bits means we have allowed range of 0 to 255. Most of the viewers would not feel interested about color values of these invisible characters hence 3 bytes of information is easily hidden in each occurrence of space tab or carriage return.

4. Video as Cover

In video steganography, a video file embedded with supplementary data to hide secret messages. In the process, an intermediate signal which is a function of hidden message data and data of content signal would be generated. Video file is later combined with this intermediate signal to result encoding. The supplementary data can include copy control data which can be brains by consumer electronic device and used to disable copying.

VI. CONCLUSION

The concept of Steganography is covered in brief in this paper. The key focus is to show light process and its variants that strongly support information security. Furthermore, the algorithm working on each variety of cover can be studied.

REFERENCES

[1]. Provos, N., & Honeyman, P. (2012). Detecting Steganography Content on the Internet.

[2]. "The raise of steganography", Proceedings of Student/Faculty Research Day, CSIS, Pace University, May 6th, 2005

[3]. Artz, D. (2001). Digital steganography: Hiding data within data. IEEE Internet Computing, 75-80.

[4]. Ishwarjot Singh,J.P Raina," Advance Scheme for Secret Data Hiding System using Hop field & LSB" International al Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue 7–July 2013.

[5]. G. Manikandan, N. Sairam and M. Kamarasan "A Hybrid Approach for Security Enhancement by Compressed Crypto-Stegno Scheme ", Research Journal of Applied Sciences, Engineering and Technology 4(6): 608-614, 201

[6]. https://www.ukessays.com/essays/computer-science/the-types-and-techniques-of-steganography-computer-science-essay.php

[7]. http://en.wikipedia.org/wiki/Steganography#Network

[8]. http://www.webopedia.com/TERM/S/steganography.html

[9]. http://quickcrypto.com/free-steganography-software.htm