



International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS)

www.iasir.net

STEGNOGRAPHY—“The Art of Hiding Information” A Study of Various Tools and Techniques along with Steganalysis

¹Aparajita, ²Prof. Ajay Rana.

¹A.P., MCA, Galgotia Institute of Management and Technology/ UPTU, Greater Noida, Uttar Pradesh, INDIA.

²Program Director, Amity School of Engineering and Technology, Amity University, Uttar Pradesh, INDIA.

Abstract: Steganography is about hiding the information whether the hiding thing is an image only. We should encrypt the information before hiding it. Many different formats of files can be used to hide the information but digital files are most widely used because of their frequency on internet. There are varieties of steganography tools available with their own strength and weaknesses. This paper is a glance at various tools and techniques of steganography and along with a brief introduction on steganalysis.

Keywords: Steganography, Cipher text, Plain text, Hiding information, Steganalysis.

I. INTRODUCTION

“We want nothing more than to connect and companies that are connecting us electronically want to know who’s saying what, where. As a result, we are more known than ever before”. ---- By Prof. Susan Crawford at Benjamin N. Cardozo School of Law. This is very clear from the statement by Prof, that privacy of the information communication is out most important in today’s world. What we share and what we communicate needs to be hidden from intruders and people not meant for that information. The first recorded use of the term was in 1499 by Johannes Trithemius in his *Steganographia*, a treatise on cryptography and steganography disguised as a book on magic. Generally, messages will appear to be something else: images, articles, shopping lists, or some other cover text and, classically, the hidden message may be in invisible ink between the visible lines of a private letter. It is a high security technique for long data transmission.

One solution to this problem is, using the techniques of steganography.

The word steganography is derived from a Greek word meaning “covered writing”. Basically it belongs to the class of “Cryptology”, which includes three techniques in it:

- a) **Cryptography:** Science of coding and decoding secret messages.
- b) **Steganography:** The art of hiding information in a way that prevents from detection.
- c) **Cryptanalysis:** Breaking cryptosystems or deciphering messages without prior knowledge of the cryptosystems.

Steganography: An art of hiding the existence of communication, in contrast to cryptography. Basically it’s a method of concealing the information in ways that prevents the detection of hidden information. We should encrypt our information before communicating. By doing this, even if the message is being found, the intruder won’t be able to learn what we are trying to send in the message. Steganography became more important as more people have chosen cyberspace as a mode of sharing the information. It includes an array of secret communication methods that hide the message from being seen or discovered. The development of Steganography has paralleled the simultaneous growth of “Cryptanalysis”—the breaking of ciphers and detecting the steganographic content in the image or text files. The advantage of steganography over cryptography alone is that messages do not attract attention to themselves. Plainly visible encrypted messages—no matter how unbreakable—will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal. Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.

But, the growing possibilities of modern communications need the special means of security especially on computer network. Consequently, the security of information has become a fundamental issue. Network security is becoming more important as the number of data being exchanged on the internet increases. Therefore, the confidentiality and the data integrity both require to be protected against unauthorized access and use. The result is the explosive growth in the field of information hiding.

Steganography hides the secret information within the host data set and reliably communicate it to a receiver. The host data set is purposely corrupted, but in a covert way, designed to be visible only to an information analysis. The process of steganography is to exploit human perception and senses to hide a file inside another file.

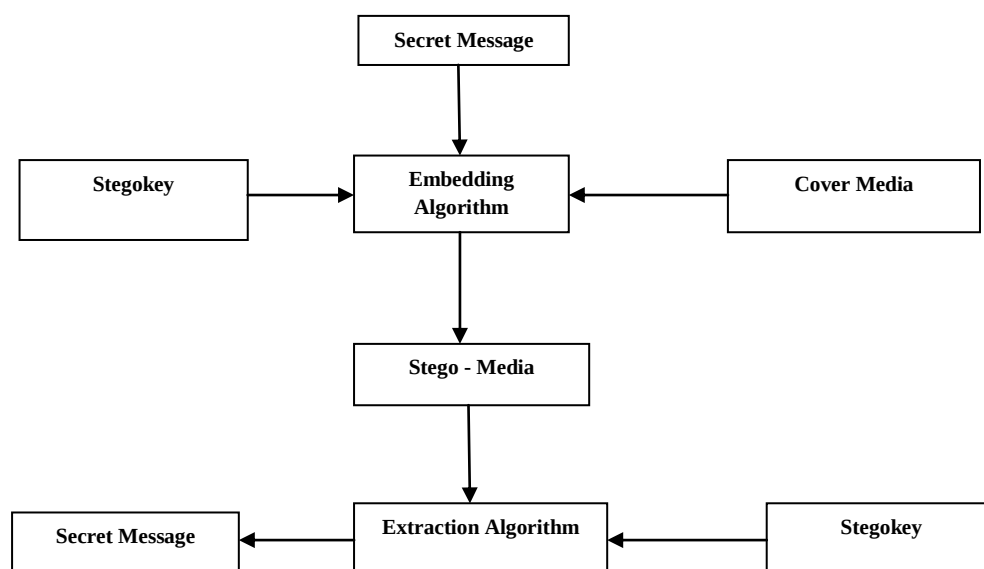
Before discussing further we should flip through the history and how steganography works.

History: Giovanni Battista Porta described how to write secret messages on the hardened surface of boiled egg with a special ink made from an ounce of *ALUMN* and a *pint of VINEGAR*. The solution leaves no trace on the surface instead penetrating the message into the porous shell which can be read when shell is removed.

The first recorded uses of steganography can be traced back to 440 BC when Herodotus mentions two examples of steganography in his *Histories*. Demaratus sent a warning about a forthcoming attack to Greece by writing it directly on the wooden backing of a wax tablet before applying its beeswax surface. Wax tablets were in common use then as reusable writing surfaces, sometimes used for shorthand.

In his work "*Polygraphiae*" Johannes Trithemius developed his so-called "*Ave-Maria-Cipher*" using which one can hide information in a Latin praise of God. "*Auctor Sapientissimus Conseruans Angelica Deferat Nobis Charitas Potentissimi Creatoris*" for example contains the concealed word *VICIPEDIA*.

The main components of a Steganography technique. Two main steps are shown in the Figure below:



Embedding the secret message inside the cover using a stegokey and extracting the secret message from the cover using the stegokey. Combining the embedded message into the cover makes a stegomedia. A stegokey is used to hide and extract the secret message. Only the holder of the stegokey can retrieve correctly the hidden secret message. Also, Steganography can be described using the following formula:

$$\text{Cover media} + \text{Embedded Message} + \text{Stegokey} = \text{Stegomedia}$$

Techniques of Steganography: Let us briefly throw some light on the various techniques used in steganography.

- 1) **Physical:** Steganography has been used widely over period of time and is evolving as the new tool for hiding the secret information. It's been in existence since 400 BC.

Example: Writing the mysterious message within wax tablets - in ancient Greece, people wrote messages on wood and then covered it with wax. Another method was also used in Greece that was to tattoo the concealed message on the shaved head of the slave and wait till hairs grow and again to decode the message they use to shave the head.

Jeremiah Denton repeatedly blinked his eyes in "Morse Code" during the 1966 televised press conference that he was forced into as an American POW by his North Vietnamese captors, spelling out the word, "T-O-R-T-U-R-E". This confirmed for the first time to the U.S. Military (naval intelligence) and Americans that American POW's were being tortured in North Vietnam.

- 2) **Digital:** Modern steganography entered the world in 1985 with the advent of computers being applied to classical steganography problems.

Example: The simplest example is modifying the echo of a sound file which is broadly termed as "ECHO STEGNOGRAPHY".

LSB (Least Significant Bit) Embedding is another used tool for hiding information. In this the LSB technique to each byte of a 24-bit image, three bits can be encoded into each pixel, as each pixel is represented by three bytes. Applying LSB technique to each byte of an 8-bit image, only one bit can be encoded into each pixel, as each pixel is represented by one byte. For example, if we use 8-bit image to hide the letter A (has the binary value 10000011), we need eight pixels. Suppose the original eight pixels are:

(00100111) (11101001) (11001000) (00100111)
 (11001000) (11101001) (11001000) (00100111)

Inserting the letter A (as a binary value) into these eight pixels will give the following
 (starting from left side):

(00100111) (11101000) (11001000) (00100110)

(11001000) (11101000) (11001001) (00100111). Only the emphasized bits are

changed.

Making text the same color as the background in word processor documents, e-mails, and forum posts.

3) Network: All information hiding techniques that may be used to exchange steganograms in telecommunication networks can be classified under the general term of network steganography.

Network steganography covers a broad spectrum of techniques, which include, among others:

Steganophony - the concealment of messages in Voice-over-IP conversations, e.g. the employment of delayed or corrupted packets that would normally be ignored by the receiver (this method is called LACK - Lost Audio Packets Steganography), or, alternatively, hiding information in unused header fields.

WLAN Steganography – the utilization of methods that may be exercised to transmit steganograms in Wireless Local Area Networks. A practical example of WLAN Steganography is the HICCUPS system (Hidden Communication System for Corrupted Networks).

Application of Steganography: Steganography is applicable to, but not limited to, the following areas.

- i) Confidential communication and secret data storing
- ii) Protection of data alteration
- iii) Access control system for digital content distribution
- iv) Media Database systems

The area differs in what feature of the steganography is utilized in each system.

1) Confidential Communication and Secret Data Storing: To keep the “secrecy” of embedded data is very important in this technique. Historically, steganography have been approached in this area. Steganography provides us with:

- (A) Potential capability to hide the existence of confidential data
- (B) Hardness of detecting the hidden (i.e., embedded) data
- (C) Strengthening of the secrecy of the encrypted data.

The simplest example of this technique is to send a “STEGO” file in the email which can only be decoded by the right receiver.

2) Protection of Data Alteration: Fragility of embedded data is the main advantage of this scheme. However, this fragility opens a new direction toward an information-alteration protective system such as a “Digital Certificate Document System.” The most novel point among others is that “no authentication bureau is needed.” If it is implemented, people can send their “digital certificate data” to any place in the world through Internet. No one can forge, alter, nor tamper such certificate data. If forged, altered, or tampered, it is easily detected by the extraction program.

3) Access Control System for Digital Content Distribution: The data is hidden in embedded area but is “Explained” to publicize the content.

4) Media Database Systems: Unifying two types of data into one is the most important part of this technique. Media data (photo picture, movie, music, etc.) have some association with other information. A photo picture, for instance, may have the following.

- (1) The title of the picture and some physical object information
- (2) The date and the time when the picture was taken
- (3) The camera and the photographer’s information.

Steganalysis: To design an algorithm for detection of stenographical encoded packages is called steganalysis. The simplest method to detect modified files is to compare them to known originals. Note that there are two aspects of steganalysis. The first relates to the attempt to break or attack a steganography; the second uses it as an effective way of evaluating and measuring steganography security performance. In general, there are two types of steganalysis: targeted and blind. Targeted steganalysis is designed to attack one particular embedding algorithm. For example, the work in [7, 49, 57, and 42] is considered targeted steganalysis. Targeted steganalysis can produce more accurate results, but it normally fails if the embedding algorithm used is not the target. Blind steganalysis can be considered a universal technique for detecting different types of steganography.

Because blind steganalysis can detect a wider class of steganographic techniques, it is generally less accurate; however, blind steganalysis can detect new steganographic techniques where there is no targeted steganalysis available yet. In other words, blind steganalysis is an irreplaceable detection tool if the embedding algorithm is unknown or secret.

II. CONCLUSION

From the above survey it is clear that to disguise our plain text we need some technique. In today's world Public Key Cryptography is used to hide the information and it uses the whole block instead of an individual alphabet. We have discussed the various techniques and tools and the main application areas of steganography. Another main topic was steganalysis where we look into the methods how to detect stego- objects. There is a lot of future research possible in this field. Steganography is a really interesting subject and outside of the mainstream cryptography and system administration that most of us deal with day after day. Steganography can be used for hidden communication. We have explored the limits of steganography theory and practice, and a comparison to cryptography

REFERENCES

- [1]. STEGNOGRAPHY—"The Art of Hiding Information" A Comparison from Cryptography. Aparajita, Prof (Dr.) Ajay Rana <http://www.ijirset.com/volume-2-issue-5.html#>
- [2]. Information hiding: steganography and watermarking—attacks and countermeasures NF Johnson, Z Duric, S Jajodia.
- [3]. Performance study of common image steganography and steganalysis techniques M Kharrazi, 2006.
- [4]. Information Hiding: Steganography and Watermarking-Attacks and ... www.springer.com
- [5]. Integrating Classical Encryption with Modern Technique F Saeed, M Rashid - IJCSNS International Journal of Computer, 2010 - paper.ijcsns.org.
- [6]. Call for attack to evaluate the cryptographic techniques - CRYPTREC www.cryptrec.go.jp/english/topics/cryptrec_20101001_callforattack.html.
- [7]. Trends of Cryptographic Techniques. sciencelinks.jp > ... > Joho Shori Gakkai Kenkyu Hokoku (2002) 2002 -by H IMAI
- [8]. Friedman, William F. (1922). "The index of coincidence and its applications in cryptology". *Department of Ciphers. Publ 22*. (Geneva, Illinois, USA: Riverbank Laboratories).
- [9]. Shannon, C.E. (1949). "[Communication Theory of Secrecy Systems]". *Bell System Technical Journal* (28-4): 656–715.
- [10]. Shamir, A. (November 1979). "How to share a secret". *Communications of the ACM* 22 (11): 612–613. doi:10.1145/359168.359176.
- [11]. Kohnfelder, Loren M. (1978). "On the Signature Reblocking Problem in Public Key Cryptography". *Communications of the ACM* 21 (2): 179
- [12]. www.ims.nus.edu.sg/Programs/imgsci/files/memon/sing_stego.pdf
- [13]. www.krenn.nl/univ/cry/steg/article.pdf
- [14]. en.wikipedia.org/wiki/Steganography_tools
- [15]. Exhaustive directory of *steganography software* by Dr. Neil Johnson;
- [16]. www.jjtc.com/Security/stegtools.htm
- [17]. Digital Image Steganography and Digital Watermarking Tool
- [18]. http://web.science.mq.edu.au/~josef/CONTENTS/PHD_THESES/Kang_Leng_Chiew_thesis.pdf
- [19]. <http://fr.slideshare.net/lailiaidi/pdf-final-report>
- [20]. http://dfcsc.uri.edu/docs/Bennett_Thesis.pdf