International Journal of Advanced Science and Research
ISSN: 2455-4227
Impact Factor: RJIF 5.12
www.allsciencejournal.com
Volume 3; Issue 2; March 2018; Page No. 144-147

Steganography Technique: A review

Munisha Devi
Research Scholar, Department of Computer Science and Applications, Maharshi Dayanand University, Rohtak, Haryana, India

Abstract
Steganography can be defined as the study of invisible communication that usually deals with the ways of hiding the existence of the communicated message. Steganography is often confused with cryptography but they are different with respect to processed output; the output of steganography operation is not apparently visible but in cryptography the output is scrambled so that it can draw attention. Steganlysis is process to detect of presence of steganography. In this I have analyzed different steganographic techniques, overview of steganography, different methods of steganography, its applications.

Keywords: steganography, cryptography, steganlysis

1. Introduction
In computer science, information hiding is the principle of segregation of the design decisions in a computer program that are most likely to change, thus protecting other parts of the program from extensive modification if the design decision is changed [1]. In starting cryptography was used for secret transmission of message. Cryptography was used to keep the contents of a message secret, but was unable to keep the existence of the message secret. To achieve this steganography was used. Steganography is about concealing the existence of message itself. It is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels [2].

A. Classifications of Information Hiding
Depending upon the requirement and goal several information hiding techniques (Figure 1) can be defined.

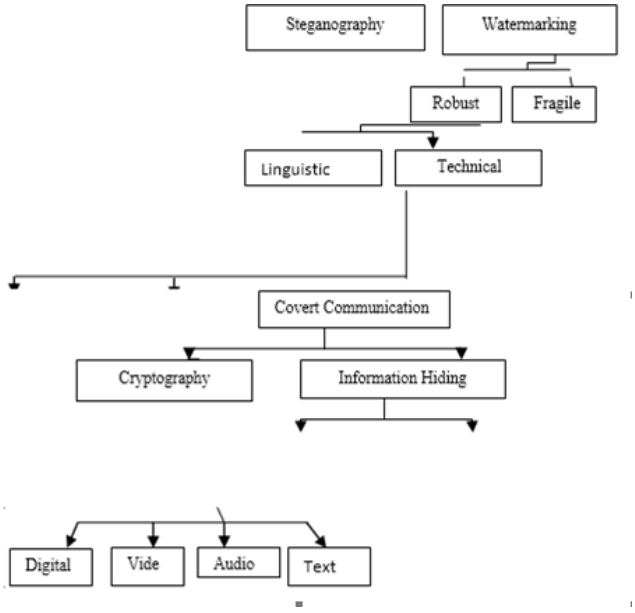

Fig 1: Different schemes of information hiding

2. Steganography
Steganography is the art of hiding information through original files in such a manner that the existence of the message is unknown. Steganography technique hides the existence of the message itself, which makes it difficult for a third person to find out where the message is. Sometimes sending encrypted information may draw attention, while invisible information will not. Accordingly, cryptography is not the good solution for secure communication; it is only part of the solution. Both techniques can be used together to better protect information. In this case, even if steganography fails, the message cannot be recovered because a cryptography

technique is used as well. The cracking of steganographic messages is called steganalysis. The purpose of steganalysis is to identify the information and determining that whether or not they have hidden messages encoded into them and if possible, extract the hidden information [3]. The goal of steganalysis is to detect hidden information from observed data with little or no information about the steganography algorithm [4]. Two other technologies that are closely related to steganography are watermarking and fingerprinting
method for protecting digital elements such as image, video and sound.

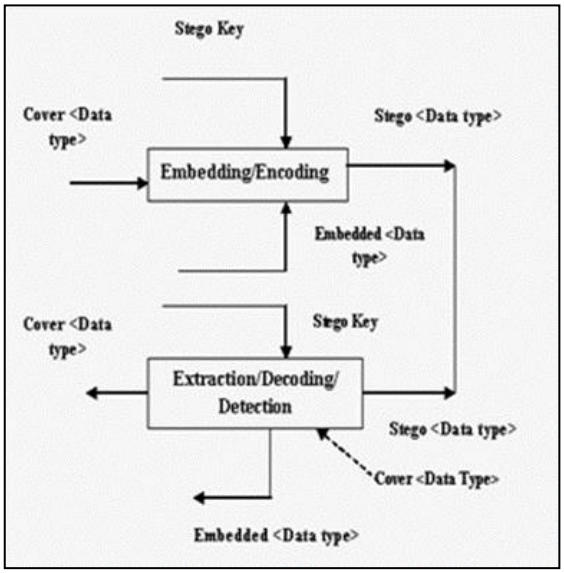

Fig 2: Steganography

B. Finger printing

Illegal copying of digital objects such as software, multimedia objects are a major problem in real world. To prevent the piracy of digital objects (especially softwares) the third information hiding technique, finger printing technique is employed, sometimes in conjunction with hardware locks. In finger printing, a distinct mark (called fingerprint) is inserted in each digital objects, which is some way related to buyer. If later on, an unauthorized copy of digital object is found then its origin can be recovered by retrieving the unique fingerprinting contained in it. The fingerprint is embedded into digital objects such that it is not easy for buyers to tamper with. However, if one has multiple copies of same object with different fingerprints, he may compare the copies and detect where the marks are different and he might be able to change the mark on the detected positions. In this way, pirates may not only redistribute the copies illegally by changing the fingerprints but can also frame innocent user.

Watermarking and fingerprinting technologies are mainly concerned with the protection of intellectual property, thus the algorithms have different requirements for steganography [2]. A digital watermark is a signal which is permanently embedded into digital data that can be detected or extracted afterwards to confirm the authenticity of the data. In fingerprinting, different and specific marks are embedded in the copies of the work that different customers are supposed to get [3].

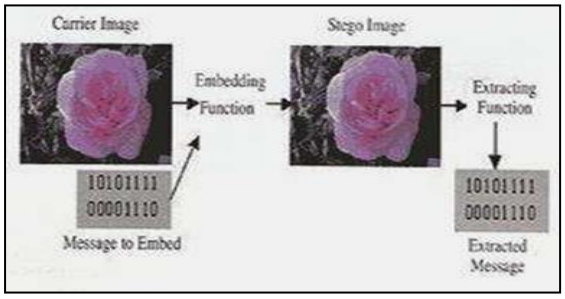

Fig 3

C. Watermarking

A special case of information hiding is digital watermarking. Water marks appeared in the art of hand made paper making nearly 700 years ago. The oldest water mark found in archives dates back to 1292 and has its origin in Febriano, Italy, which is considered as the birth place of watermarks. The idea of digital image water making came into existence in 1990 [7], [8], and 1993 [8], G. Caronni and Tirkel *et al* coined the world "water marks" which became "watermarks" later on Digital water marking is the process of embedding information into digital media content such that the information (the watermarks) can later be extracted or detected for a variety of perposts including copy prevention and control. Digital watermarks have become an active and important area of research and development. It helps in addressing some of the challenges faced by the rapid explosion of digital content. Water marking has become the key

3. History

Early steganography was messy. If you wanted to hide a message, you had two choices: have the messenger memorize it, or hide it on the messenger.

While information hiding techniques have received a tremendous attention recently. According to Greek historian Herodotus, the famous Greek tyrant Histiaeus, while in prison, used unusual method to send message to his son-in-law. He shaved the head of a slave to tattoo a message on his scalp. Histiaeus then waited until the hair grew back on slave's head prior to sending him off to his son-in law [5].

Invisible inks have always been a popular method of steganography. Ancient Romans used to write between lines using invisible inks based on readily available substances such as fruit juices, urine and milk. When heated, the invisible inks would darken, and become legible. Ovid in his "Art of Love" suggests using milk to write invisibly. Later chemically affected sympathetic inks were developed. Invisible inks were used as recently as World War II. Modern invisible inks fluoresce under ultraviolet light and are used as anti-counterfeit devices. For example, "VOID" is printed on checks and other official documents in an ink that appears under the strong ultraviolet light used for photocopies [5].

4. Different Kinds of Steganography

The four main categories that can be used for steganography are:

1. Text
2. Images

3. Audio
4. Protocol

A. Text steganography: The method was to hide a secret message in every nth letter of every word of a text message. After booming of Internet and different type of digital file formats it has decreased in importance. Text stenography using digital files is not used very often because the text files have a very small amount of redundant data.

B. Image steganography: A message is embedded in a digital image through an embedding algorithm, using the secret key. The resulting stego image is send to the receiver. On the other side, it is processed by the extraction algorithm using the same key. During the transmission of stego image unauthenticated persons can only notice the transmission of an image but can't guess the existence of the hidden message.

C. Audio steganography: It exploits the properties of the human ear to hide information unnoticeably. An audible, sound can be inaudible in the presence of another louder audible sound. This property allows to select the channel in which to hide information.

D. Protocol steganography: We hide information in the header of a TCP/IP packet in some fields that can be either optional or are never used [3].

5. How Steganography Works in Image

First you will need to read your picture as a jpg and then save it in 24-bit bmp format. You will need to use bmp files for this assignment because jpg's file may be changed slightly so that the resulting image can be stored more efficiently. Thus jpg will not work for steganography because jpg's will change the secret message when storing the file to disk. Here are some commands to save your file. You can give it the same name except be sure to put a.bmp file extension on the end.(For example, I loaded "hat.jpg" and then saved "hat.bmp")

A. Interaction

1. Prompt the user if they want to encode or decode a message.
2. Use the File Chooser dialog to prompt the user for an input file.
3. If encode, prompt the user for an input message. Encode the message into the picture (details below). Then use the File Chooser dialog to prompt the user for an output file. Save the new picture/message in this file (using bmp format).
4. If decode, extract the message from the file. Print the message. Encoding/Decoding Method.
5. You can extract the pixels of your target picture in one big array using the text tgetPixels () method.
6. Use the first pixel (at spot 0) to hide the length of your message (number of characters). You will limit yourself to messages that are between 0 and 255characters long
7. After that use every eleventh pixel to hide characters in your message. Start at pixel 11, then pixel 22, and so on until you hide all characters in your message.
8. Every thing that you need to hide in a pixel is 8-bits long. The length (in the first pixel) is a byte. You can typecast all the Unicode chars to bytes as well [10].

6. Steganography Techniques

a. Substitution Technique: It covers a redundant part with a secret message.Example – Least Significant Bit (LSB) Substitution
- Choose a subset of cover elements and substitute least significant bit(s) of each element by message bit(s)
- Message may be encrypted or compressed before hiding
- A pseudorandom number generator may be used to spread the secret message over the cover in a random manner
- Easy but vulnerable to corruption due to small changes in carrier [6].

b. Transform Domain Technique: It embeds secret message in a transform space of cover.Example-Steganography in the Discrete Cosine Transform (DCT) domain
- Split the cover image into 8 × 8 blocks. Each block is used 8 blocks. Each block is used to encode one message bit
- Blocks are chosen in a pseudorandom manner
- The relative size of two pre- defined DCT coefficients is modulated using the message bit
- The two coefficients are chosen from middle frequencies (trade off between robustness and imperceptibility) [6].

c. Spread Spectrum Techniques
- Adopt ideas from spread spectrum communication where a signal is transmitted in a bandwidth in excess f the minimum necessary to send the information
- In other words, the message is spread over a wide frequency bandwidth
- The SNR in every frequency band is small (difficult to detect)
- Even if parts of the message are removed from several bands, enough information is present in other bands to recover the message
- Thus, it is difficult to remove the message completely without entirely destroying the cover (robustness) [6].

d. Statistical Techniques
- Encode information by changing several statistical properties of a cover
- The cover is split into blocks. Each block is used to hide one message bit
- If the message bit is "1" then the cover block is modified, otherwise the cover block is not modified
- Difficult to apply in many cases, since a good test must be found which allows distinction between modified and unmodified cover blocks [6].

e. Distortion Techniques
- Store information by signal distortion Store information by signal distortion
- The encoder applies a sequence of modifications to the cover. This sequence corresponds to the secret message
- The decoder measures the differences between the original cover and the distorted cover to detect the sequence of modifications and consequently recover

the secret message
- Not useful in many applications since the decoder must have access to the original cover
- Example: vary the distance between consecutive lines or words to transmit secret information [6].

f. Cover Generation Technique
- Encode information in the way a cover is generated
- Example: Automated Generation of English Text: (1)Use a large dictionary of words categorized by different types, and a style source which describes how words of different types can be used to form a meaningful sentence(2) Transform message bits into sentences by selecting words out of the dictionary which conforms to a sentence structure given in the style source [6].

7. Steganography Applications
1. In defence organizations, military and intelligence agencies
2. In smart identity cards- personal details are embedded in photograph for copyright control of materials
3. In online voting system

8. Conclusion
In this paper I have taken an introductory look at information hiding techniques and different methods of steganography. Each method has some advantages, and also disadvantages in comparison with other methods of steganography. So it is impossible to determine the best and the worst one. We can just compare them form different aspects, which results in determining a suitable method for a specific usage. It is no way can replace cryptography, but is intended to supplement it. Steganography has its place in security. The research to device strong steganographic technique is a continuous process and still going on.

9. References

1. http://en.wikipedia.org/wiki/Information_hiding.
2. Prasad Sitaram M, Naganjaneyulu Krishna S, Ch. Gopi, Nagaraju C. A Novel Information Hiding Technique for Security by Using Image Staganography. Journal of Theoretical and Applied Information Technology, 2005-2009.
3. Mandal Chandra Pratap. International Journal of Computer Science & Engineering Technology (IJCSET).
4. Rajput Gaurav, Agrawal RK, Aggarwal Namita. Performance Evaluation of Exponential Discriminant Analysis with Feature Selection for Steganalysis. Defence Science Journal. 2012; 62(1):19-24.
5. http://arxiv.org/ftp/arxiv/papers/0802/0802.3746.pdf
6. http://vanilla47.com/PDFs/Cryptography/Steganography/Information%20Hiding%20%20Steganography%20and%20Watermarking.pdf
7. Tanka Nakamura Y, Matsui K. Embedding secret information into a dithered multilevel image, in proceeding, IEEE Military Communication Conference, 1990, pp. 216-220.
8. Tanka Nakamura Y, Matsui K. Embedding the attribute information into a dithered image, Syst. Comput. Japan, 1990, 21(7).
9. Tirkel A, Rankin G, Van Schyndel R, Ho W, Mee N, Osborne C. Electronic water mark", in Proceeding DICTA, 1993, pp. 666-672.
10. Kaur Ravneet, Singh Gagandeep, Singh Sajinder. An overview of data hiding technique: Steganography. International journal of data and network security, 2012, 1(2).