# A Case study on Steganography and its Attacks

Yashika Garg[#1], Amneet Kaur[*2]

*Computer Science Department , Thapar University, India*

***Abstract*** *— Steganographic systems work in many different ways to embed the secret data into the cover media. Digital steganographic techniques are limited in their ability to adequately adapt and respond to the increasing body of the steganographic techniques. Most of the modern steganographic attacks are highly destructive to the cover media. In order to properly combat the steganography , an attack methodology that is effective and adaptable is required. This paper includes the detail study of Steganography introduction, concept and its applications. Categories of steganography that tell which Steganography techniques should be used.*

**Keywords** *— Steganography, Digital steganography, Steganographic attacks, Cover media, Encode*

## I. Introduction

In today's world, communication is needed for transmitting the information.

Everybody needs the security and secret of the conveying information. So as to send the information in a disguised way two systems are for the most part utilized. These techniques are Cryptography and Steganography[1]. In cryptography, the information is encrypted utilizing the encryption key which is known to sender and receiver as it were. The message can not be gotten to by anybody without utilizing the encryption key. The encoded message can be changed, tempered or decoded by the attacker. Along these lines, to conquer the weaknesses of the cryptographic strategies, steganographic procedures have been sent. Steganography shrouds the information such that nobody can identify its nearness. In steganography, the covering up of the information inside any mixed media substance, for example, picture, video is alluded as "Implanting". So it is also known as the art of "covered writing". Digital steganography is practice of secretly encoding information within the cover medium as a part of covert communication. Like the many security fields , steganography is the discipline where the steganographer attempts to hide the information and steganographic attacker tries to retrieve the hidden text.

## II. Steganography Technology

Steganography comprises of the two terms that is the message and the cover picture in which the information is to be hided . Message is the secret data and the cover image act as the carrier for hiding the data. Together the cover media and the embedded message creates a stego-carrier[6]. For example , when a crucial data(secret message) is hidden within a cover image, the resulting product is the stego-image[15].

The possible formula of the process is represented as-

Cover media + embedded message + stego key = stego-medium.

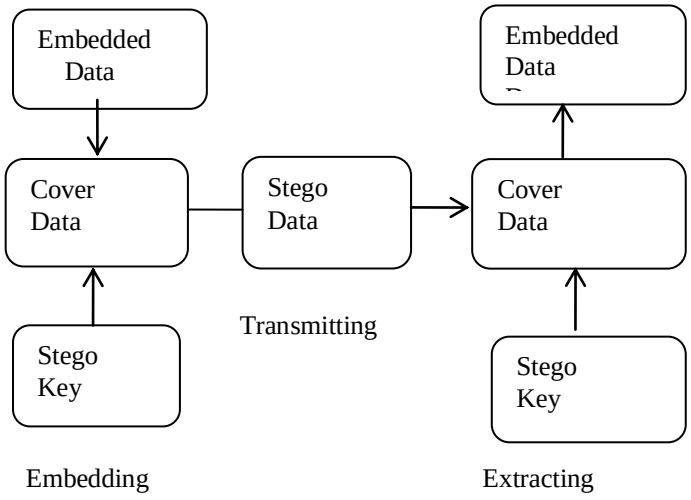


Fig1. Steganography System Scenario

### *A. Classification of Steganography*

1) ***Text Steganography***- Hiding information in the text is the most important method of the steganography. This method is used to hide the text in every nth letter of the each word of the text[5].

Different embedding techniques in text :

*1.1)* ***Modifying Spaces:***

Data can be hidden in a cover text by modifying the blank spaces in text. Appending one or two spaces to the end of each line is also a simple data hiding method[7]. A word processor can modify the interword spaces in a sentence.

*1.2)* ***Semantic Methods*:**
In this method, Data is embedded using special word usage. The sender and receiver both will agree upon using certain online thesaurus[14]. The decoder will reads the cover text word by word and searches the thesaurus for occurrence of each word. If no such word is found, the decoder assumes that no data is hidden in it[7].

**Advantages –**
They can not be detected by re typing or OCR methods

**Disadvantages–**
Smart reader having huge knowledge of words can discover it easily.

*1.3)* ***Syntactic Methods*:**
These methods are based on modifying the text such that its meaning is preserved. This approach is more safer, harder to implement as computers are notoriously bad at "understanding" the text[7].

**Advantages–**
The amount of information to be hided in this method is trivial.

**Disadvantages–**
Smart reader can easily find the hided information in this method.

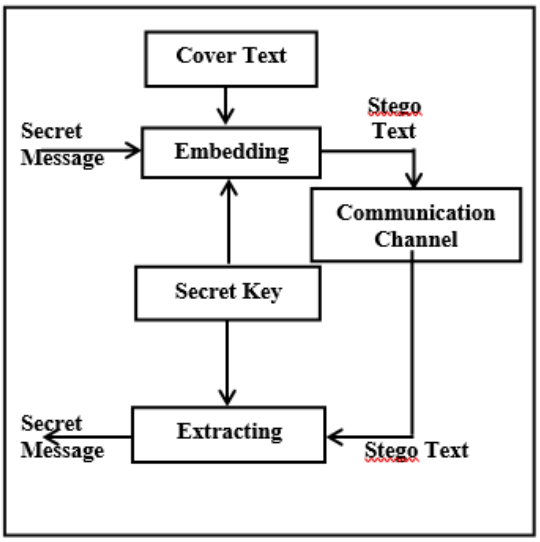


Fig 2. Text Steganography

2) ***Audio Steganography-*** It involves hiding the data in the audio files. This method hides the data in MP3 files. First the storage environment or digital representation of the signal that will be used for the transmission of the signal and second the transmission pathway the signal might travel.

Different embedding techniques for Audio:

*2.1)* ***Echo Hiding:***
It inserts the secret data in a sound document by bringing the echo into the discrete signal. Just a single bit of secret data could be encoded if just a single resound was created from the first signal[3].
It has focal points of giving the higher transmission rate and predominant robustness[8].

**Advantages–**
It is resilient to the lossy data compression algorithums used in this method.

**Disadvantages-**
It provides low security and capacity.

*2.2)* ***Parity Coding* :**
Parity coding breaks the sound signal into the areas and then hides the message in the parity bit. If the parity does not match, it adjusts the LSB of one of the samples to get the required parity[8].

**Advantages–**
In this , sender has more choices in encoding the secret bit.

**Disadvantages-**
It provides no robustness.

*2.3)* ***Spacial Domain Methods*:**
This is the technique in which the secret information is embedded in the force of pixels. It implies a few pixels are changed directly while concealing the data[8].

*2.4)* ***Spread Spectrum Technique*:**
In this technique, the secret information is spread over the extensive recurrence data transfer capacity. The proportion of clamor to signal is ascertained in each recurrence band and it must be small to the point that it ends up plainly hard to distinguish the nearness of information.

Regardless of the possibility that the information is expelled from the few groups, there will be sufficiently still data introduce in alternate groups to recuperate the information. This technique is used in military communications[8].

**Advantages-**
It provides the better robustness as compared to other methods of audio steganography.

**Disadvanatges-**
It is vulnerable to time scale modifications.

| Methods | Embedding Techniques | Strengths | Weakness |
|---|---|---|---|
| Least Significant Bit(LSB) | LSB of each sample in the audio is replaced by one bit of hidden information | Simple and easy way of hiding information with high bit rate. | Easy to extract and to destroy. |
| Echo hiding | Embeds data by introducing echo in the cover signal. | Resilient to lossy data compression algorithm. | Low security and capacity. |
| Phase coding | Modulate the phase of the cover signal. | Robust against signal processing manipulation and data retrival needs the original signal. | Low capacity. |
| Parity coding | Break the signal into seperate samples and embeds each bit from secret message in sample region parity bit. | Sender has more of a choice in encoding the secret bit. | Not robust. |
| Spread spectrum | Spread the data over all signal frequencies. | Provide better robustness. | Vulnerable to time scale modification. |

Table 1. Comparison of Audio Steganography

*3)* ***Image/Video Steganography-*** Images are often used as the popular cover objects in steganography. In this technique, a secret message is embedded into the computerized picture utilizing different installing calculations and secret key key[4]. The subsequent stego picture is send to the collector and secret message is extricated utilizing the extraction calculation and a similar secret key.

Video steganography is a process of hiding the secret message into the digital video format[2]. In this video is used as the carrier of the secret message. Mp4, AVI are the formats used in video steganography.

Different data embedding methods used for image/video:

*3.1)* ***Masking and Filtering*** :

It is the method by which data is hided by marking the image.

These procedures embed the information into the more noteworthy territories so that nearness of information can not be distinguished as opposed to concealing it into the noise level.

**Advantages-**

This method is more robust than LSB replacement in turns of compression as message is hided in the visible parts of the image.

**Disadvantages-**

This technique can be applied to grey scale images only.

*3.2)****Transform Domain Technique:***

This is the technique in which secret information is embedded into the change space of cover. It is the extremely complex method for concealing the information. This is more mind boggling type of concealing the secret information into the picture. Transform domain technique have an advantage over LSB method as they hide the data into the areas of image which are less exposed to cropping , image processing .

Transform domain techniques are broadly classified into :

A. Discrete Fourier transformation technique (DFT).

B. Discrete cosine transformation technique (DCT).

C. Discrete Wavelet transformation technique (DWT).

**Advantages-**

High bit rate data hiding.

It is Tamper resistant.

Hides secret bits on both vertical and diagonal edges of cover image.

**Disadvantages-**

Hides the data in independent frames.

The use of block DCT can result in blocking artifacts in the stego-video.

Although quantization of secret image decreases the size of the secret data but it affects the quality of the retrieved image.

*3.3)* ***Distortion Techniques****:*

Distortion techniques need the complete knowledge of the cover media amid the translating procedure on the grounds that the decoder needs to check the first cover picture and the twisted cover picture to re-establish the secret message[9]. In the event that the assailant endeavours to alters the stego-picture.

*3.4 )****Data Hiding Techniques in IPv4 Header:***
To securely transmit the data over the network the Vasudevan et al.[10] used the analogy of the jigsaw puzzle. They insinuate to fragment the data into variable sizes instead of fixed size like the jigsaw puzzle and append each fragment of data with a pre-shared message authentication code (MAC) and a sequence number so that the receiver can authenticate and combine the received fragments into a single message[11].

## III. Applications of Steganography

There are various applications of steganography described as follows[13]:

- Secret data storing
- E-Commerce
- Media
- Database Systems
- Digital Watermarking
- Protection of data alteration
- Confidential Communication

## IV. Attacks On Steganography

Following is the list of some possible attacks:

1) ***File only***

In this , the attacker have access to the file and should determine whether the data is hidden in it or not.

2) ***File and Original Copy***

If the attacker have a copy of the original file and pre-encoded file then the real question is what the attacker will do with the secret message (destroy hidden information, extract hidden information , replace it).

3) ***Compression Attack***

One of the simplest attack is to compress the file containing the hidden information. Compression algorithms try to remove the extraneous information from a file, and "hidden" is equivalent to "extraneous".

4) ***Destroy Everything Attack***

In this, attacker could simply replace the whole message.

5) ***Reformat Attack***

One of the possible attack is to change the format of the file. Different file formats don't store the data exactly in the same way (JPEG, GIF).

6) ***Random Tweaking Attacks***

An Attacker could simply add small, random tweaks in order to destroy the message.

7) ***Structural Attack***

Steganographic algorithms generally leave a characteristic structure to the data. The organization of the information document is distinctive when data is implanted into it. The assailant can without much of a stretch distinguish the nearness of the secret message by analyzing the factual profile of the bits. These progressions to the information record for the most part fall into effortlessly discernible example that gives a sign of a hidden message[7].

8) ***Visual Attack***

The visual assault is a stego-just assault that strips away piece of the question in way that takes into consideration a human to look for visual peculiarities. The most well-known assault is to show the minimum huge piece of a protest; Digital types of gear, for example, cameras are not impeccable and regularly leave echoes at all critical bits. These totally arbitrary commotions demonstrate the presence of a concealed message. The normal ear can get unobtrusive contrast in sound. Be that as it may, this is moderate and expensive attack[10].

## V. Merits Of Steganography

Steganography involves making the content of the secret message unreadable while not preventing non intended observers to learn its existence[8]. The primary goal of steganography is to hide the secret message while cryptography is to make data unreadable for the third party to understand it.

Few attributes to measure the quality of the steganography:

1) High Capacity
2) Resistance
3) Confidentiality
4) Accurateness
5) No detection
6) Visibility
7) Imperceptibility

## VI. CONCLUSION

This paper describes the short survey on steganography and its types. Different techniques for image, video, audio, text steganography is also explained in it. These techniques are very helpful for detecting the stego- images and the image media relating to the security of the information. Steganography provides a high embedding capacity to secure the data. The strong and weak points of these techniques are explained so that the researchers working in steganography field can get prior knowledge about it in brief.

## REFERENCES


[1] Dr. Fadhil Salman Abed "A Proposed Method of Information Hiding Based on Hybrid Cryptography and Steganography", IJAIEM, Volume 2, Issue 4, April 2013

[2] R. Balaji, G. Naveen, "Secure Data Transmission Using Video Steganography", International Journal of Computational Engineering Research (ijceronline.com) VOLUME 2. July-August 2012.

[3] W. Bender,D. Gruhl,N. Morimoto,A. Lu,"Techniques for data Hiding", IBM SYSTEMS JOURNAL, VOL 35, NOS 3&4, 1996.

[4] Bin Li, Junhui He, Jiwu Huang, Yun Qing Shi, "A Survey on Image Steganography and Steganalysis",Journal of Information Hiding and Multimedia Signal Processing c 2011 ISSN 2073-4212 Ubiquitous International Volume 2, Number 2, April 2011.

[5] Pratap Chandra Mandal, "Modern Steganographic technique: A Survey", International Journal of Computer Science & Engineering Technology (IJCSET).

[6] Arvind Kumar, Km. Pooja, "Steganography- A Data Hiding Technique", International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010.

[7] Salomon,D. , "Data Hiding in Text", - Springer,2003

[8] Harish Kumar, Anuradha, "Enhanced LSB technique for Audio Steganography", IEEE-20180.

[9] Neil F. Jonhson and Stefan C. Katzenbeisser, "A survey of steganographic techniques", Artech house.

[10] Rangarajan A. Vasudevan, Sugata Sanyal, Ajith Abraham, Dharma P. Agrawal, "Jigsaw-based secure data transfer over computer networks", Proceedings of International Conference on Information Technology: Coding and Computing, Las Vegas, Nevada, Vol. 1, 5-7 April 2004, pp. 2- 6.

[11] Harshavardhan Kayarkar, Sugata Sanyal, "A Survey on Various Data Hiding Techniques and their Comparative Analysis", ACTA Technica Corviniensis, Vol. 5, Issue 3, July-September 2012, pp. 35-40

[12] Gwenaël Doërr and Jean-Luc Dugelay, "Security Pitfalls of Frame-by-Frame Approaches to Video Watermarking", IEEE TRANSACTIONS ON SIGNAL PROCESSING, VOL. 52, NO. 10, OCTOBER 2004.

[13] W. Bender,D. Gruhl,N. Morimoto,A. Lu,"Techniques for data Hiding", IBM SYSTEMS JOURNAL, VOL 35, NOS 3&4, 1996.

[14] Rani, Neha, and Jyoti Chaudhary. "Text steganography techniques: A review." *International Journal of Engineering Trends and Technology (IJETT)* 4, no. 7 (2013): 3013-3015.

[15] Kaur, Navneet, and Sunny Behal. "A Survey on various types of Steganography and Analysis of Hiding Techniques." *International Journal of Engineering Trends and Technology* 11, no. 8 (2014): 387-91.