Steganography Techniqes

Shivani Singh
Department of Computer Science & Engineering
Rama University, Uttar Pradesh, Kanpur, India
Email id: sthakur243@gmail.com

Abstract: ***Steganography is the science of hiding information in other information.*** Steganography provides better security than cryptography. Steganography is an encryption technique which is used alongwith cryptography to protect data.Steganography method consist of two terms- message and cover image.Message is the secret data which is used to be hide.Cover image is the carrier which hides the message in it.

Keywords: Steganograpy ,Cryptograpy,Message hiding , Privacy,Encryption,Decryption

I.INTRODUCTION

Steganography is the art of hiding information in other information. The word Steganography is formed by the two Greek words that are Stegano means Hidden or Covered and Grafia means writing. The key concept behind steganography is that the message to be transmitted is not detectable to the casual eye[4]. Steganography is defined as the process of hiding sensitive information on any multimedia cover like image, audio, video and protocol etc in a such way that unauthorized person can't be recognized the existing of sensitive information in to the cover media[1]. Steganography sometimes used in conjunction with encryption. An encrypted file may still hide information using steganography, so even if the encrypted file is deciphered,the hidden information is not seen[5]. Steganography hides the secret data in another file in such a way that only the recipient knows the existence of message. In ancient time, the data was protected by hiding it on the back of wax, writing tables, stomach of rabbits or on the scalp of the slaves. But today's most of the people transmit the data in the form of text, images, video, and audio over the medium.

Steganography equation is :

'Stego-medium = Cover medium + Secret message + Stego key'.[2]

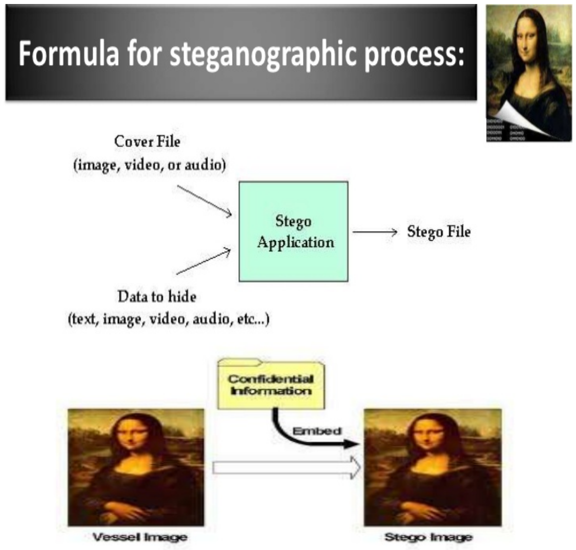

Fig.1 Steganography

The secret message is embedded inside the cover object in encrypted format by using a hiding algorithm and it sent to a receiver over a network. The receiver then decrypted the message by applying the reverse process on the cover data and reveals the secret data[6] .

II.TYPES OF STEGANORAPHY

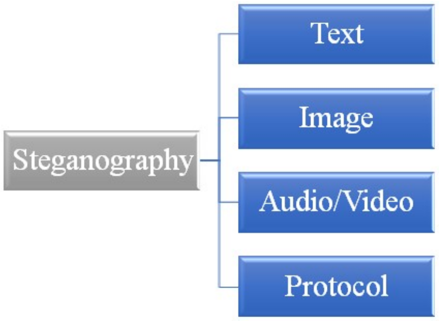

Fig.2 Types of Steganorapy

1) Linguistic Steganography:
Linguistic technique is used to hide the message within the cover text in non-
Obvious way such that the presence of
Message is imperceptible to an outsider [8]. It is divided into Two Types

A)Semagrams: It uses only symbols and signs to hide the information. It is further categorized into two ways:

i) Visual Semagrams: A visual semagrams uses physical objects used every day to convey a message. For example: the positioning of items on a particular website.

ii) Text Semagrams:
This type is used to hides a message by
Modify the appearance of the carrier text, or by changing font size and type, or by adding extra space between words and by
Using different flourished in letters or handwritten text

B) Open Code: In this approach the message is embedded in legitimate paraphrases of cover text in the way such that it appears not obvious to an unsuspecting observer. It can be achieved by two ways viz., Jargon which is understood only by a group of peoples and Cipher which uses some concealed ciphers to hide a message openly in the carrier medium. A subset of jargon codes are cue codes, where certain pre-arranged phrases convey meaning.

2) Technical Steganography: Technical steganography uses special tools, devices or scientific methods to hide a message. In this type one can use invisible ink, microdots, computer based methods or various hiding places to keep message secret

I) Cover: The cover message is the carrier of the message such as image, video, audio, text, or some other digital media [9].The cover is divided into blocks and message bits which are hidden in each block. The information is encoded by changing various properties of coverimage. The cover blocks remain unchanged if message block is zero [10].
A. Text Steganography: It consists of hiding information inside the text files. In this method, the secret data is hidden behind every nth letter of every words of text message. Numbers of methods are available for hiding data in text file.[3]
These methods are i) Format Based Method; ii) Random and Statistical Method; iii) Linguistics Method.
B. Image Steganography: Hiding the data by taking the cover object as image is referred as image steganography. In image steganography pixel intensities are used to hide the data. In digital steganography, images are widely used cover source because there are number of bits presents in digital representation of an image.[3] Various methods of image steganography are:

i) Data Hiding Method: hiding the data, a username and password are required prior to use the system. Once the user has been login into the system, the user can use the information (data) together with the secret key to hide the data inside the chosen image. This method is used to hiding the existence of a message by hiding information into various carriers. This prevents the detection of hidden information [11].

ii) Data Embedding Method: For retrieving the data, a secret key is required to retrieving back the data that have been embedded inside the image. Without the secret key, the data cannot be retrieved from the image. This is to ensure the integrity and confidentiality of the data. The process of embedding the message inside the image, a secret key is needed for retrieving the message back from the image, the secret message that is extracted from the system is transfer into text file and then the text file is compressed into the zip file and zip text file is converting it into the binary codes [12].
iii) Data Extracting Method: It is used to retrieve an original message from the image; a secret key is required to retrieving back the data that have been embedded inside the image. Without the secret key, the data cannot be retrieved from the image. This is to ensure the integrity and confidentiality of the data. The process of embedding the message inside the image, a secret key is needed for retrieving the message back from the image, the secret message that is extracted from the system is transfer into text file and then the text file is compressed into the zip file and zip text file is converting it into the binary codes [12].

iii) Data Extracting Method: It is used to retrieve an original message from the image; a secret key is needed for the verification. And for extracting method, a secret key is needed to check the key is correct with the decodes from the series of binary code. If key is matched, the process continues by forming the binary code to a zipped text file, the unzip the text file and transfer the secret message from the text file to retrieve the original secret message [12].

***C. Audio Steganography**:* It involves hiding data in audio files. This method hides the data in WAV, AU and MP3 sound files. There are different methods of audio steganography. These methods are i) Low Bit Encoding ii) Phase Coding iii) Spread Spectrum.[3]

1) Types of Audio Steganography:

i) Echo Hiding
ii) Phase Coding
iii) Parity Coding
IV) Spread Spectrum
v) Tone insertion

i) Echo Hiding: This method embeds data or text into audio signals by adding a small echo to the host signal. The Nature of the echo is a resonance added to the host audio. Then the data is invisible by varying three echo parameters: initial amplitude, decay rate, and offset. If only one echo is produced from the original signal, then only one bit of information could be encoded [13]

ii) Phase Coding: One of the most effective coding methods in terms of the signal- to perceived noise ratio. In this phase components of sound are not as perceptible to the human ear as noise is. It can be done by substituting the phase of an initial audio segment with a reference phase that represents the data. Itencodes the message bits as phase shifts in the phase spectrum of a digital signal, achieving an inaudible encoding in terms of signal-to-perceived noise ratio subsequent segments is then adjusted store the relative phase between segments. Disadvantage: It is a complex method and has low data transmission rate [14] [15]

iii) Parity Coding: This method breaks a signal down into different regions of samples and encodes each bit from the secret message in a sample region's parity bit. If the parity bit of selected region does not match the secret bit to be encoded,

Disadvantage: This method like LSB coding is not robust in nature. Advantage: The sender has more of a choice in encoding the secret bit, and the signal can be changed in a more unobtrusive manner [13]

IV) Spread Spectrum: This is analogous to a system using an implementation of the LSB coding that randomly spreads the message bits over the entire sound file. It is used to encode a category of information by spreading the encoded data across frequency spectrum. This allows the signal reception, even if there is interference on some frequencies. Disadvantage: It can introduce noise into a sound file [14] [15].

v) Tone insertion: In this inaudibility of lower power tones in the presence of significantly higher ones. Tone insertion method can resist to attacks such as low-pass filtering and bit truncation addition to low embedding capacity, embedded data could be maliciously extracted since inserted [15]

D. Video Steganography: It is a technique of hiding any kind of files or data into digital video format. In this case video (combination of pictures) is used as carrier for hiding the data. Generally discrete cosine transform (DCT) alter the values (e.g., 8.667 to 9) which is used to hide the data in each of the images in the video, which is unnoticeable by the human eye. H.264, Mp4, MPEG, AVI are the formats used by video steganography.[3]

E. Network or Protocol Steganography: It involves hiding the information by taking the network protocol such as TCP,UDP, ICMP, IP etc, as cover object. . In the OSI layer network model there exist covert channels where steganography can be used.[3]

III.STEGANOGRAPHY TECHNIQES

1) Method: In spatial domain, images are represented by pixels. Simple watermarks could be embedded by modifying the pixel values or the least significant bit (LSB) values
[16]

A. ***Spatial Domain methods*****:** These methods directly changed some bits in the image pixel values of hiding data[1].There are various spatial domain methods such as (i) Least significant bits(LSB) ,(ii) Pixel values differencing (PVD),(iii) Edges based data embedding method(EBE),(iv) Pixel intensity based.LSB is the most simple and effective method that replaces a secret message bits with the LSB of each pixel values of the cover medium.

i)Least Significant Bit (LSB): This is the most common, simple approach for embedding data in a cover image. The least significant bit (8th bit) of one or all of the bytes inside an image is changed to a bit of the secret message. When we use 24-bit image, three color bits components are used which are red, green, blue, each byte store 3 bits in every pixel. An 800 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data. For example a grid for 3 pixels of a 24-bit image can be as follows:
(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 0110001) [17]

ii)Pixel Value Differencing: It provides both high embed-ding capacity and outstanding imperceptibility for the stego-image; this segments the cover image into non overlapping [10] blocks containing two connecting pixels and it modifies the pixel difference in each pair for data embedding.

iii) Pixel Indicator: This method gives the stego images of better quality than the traditional method while maintaining a high embedding capacity and it also uses concept of hiding the data using the difference between the pixel values [16].

B) Frequency Domain:

i)Discrete Cosine Transformation: These methods convert the uncompressed image into JPEG compressed type[18] It is based on data hiding used in the JPEG compression algorithm to transform successive 8x8-pixel blocks of the image from spatial domain to 64 DCT coefficients each in frequency domain.[19]

ii)Discrete Wavelet Transformation: It gives the best result of image transformation .it splits the signal into set of basic functions .there are two types of wavelet transformation one is continuous and other is discrete [20]

2. ***Transform Domain techniques*****:** In this technique, the secret data is embedded in the transform or frequency domains of the cover file .In this many different algorithms and transformations are used for hiding information in an image. This technique is more robust and complex as compared to the spatial

domain methods. There are some transform domain techniques such as (i) Discrete Fourier transformation technique (DFT), (ii) Discrete cosine transformation technique (DCT), (iii) Discrete wavelet transformation technique (DWT).
3. ***Masking and Filtering*****:** The technique in which secret data is hidden in the more significant areas by marking an image. This method is more robust than LSB method[1]. The main drawback of this technique is that this method can be applied only to gray scale images and 24 bits images.

4. Spread Spectrum Technique: In this method the secret data is spread over a wide frequency bandwidth. The ratio of signal to noise in every frequency band must be so small that it becomes difficult to detect the presence of data. Even if parts of data are removed from several bands, there would be still enough information is present in other bands to recover the data. Thus it is difficult to remove the data completely without entirely destroying the cover .It is a very robust technique mostly used in military communication.
5. Statistical Technique: In the technique message is embedded by changing several properties of the cover. It involves the splitting of cover into blocks and then embedding one message bit in each block[3]. The cover block is modified only when the size of message bit is one otherwise no modification is required.

6. Distortion Techniques: It require original cover image during decoding process where decoder functions to check for differences between original cover image and distorted cover image in order to restore secret message[7]. In this technique the secret message is stored by distorting the signal. A sequence of modification is applied to the cover by the encoder[3]. 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.

IV. FACTORS AFFECTING STEGANOGRAPHIC TECHNIQES

1) Robustness: Robustness refers to the ability of embedded data to remain intact if the stego- image undergoes transformations, such as linear and non-linear filtering, sharpening or blurring, addition of random noise, rotations and scaling, cropping or decimation, lossy compression.
2) Imperceptibility: The imperceptibility means invisibility of a steganographic algorithm. Because it is the first and foremost requirement, since the strength of steganography lies in its ability to be unnoticed by the human eye.

3) Payload Capacity**:** It refers to the amount of secret information that can be hidden in the cover source. Watermarking usually embed only a small amount of copyright information, whereas, steganography focus at hidden communication and therefore have sufficient embedding capacity.
4) PSNR (Peak Signal to Noise Ratio): It is defined as the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. This ratio measures the quality between the original and a compressed image. The higher value of PSNR represents the better quality of the compressed image.
5) MSE (Mean Square Error): It is defined as the average squared difference between a reference image

and a distorted image. The smaller the MSE, the more efficient the image steganography technique . MSE is computed pixel-by-pixel by adding up the squared differences of all the pixels and dividing by the total pixel count.

6) SNR (Signal to Noise Ratio): It is the ratio between the signal power and the noise power. It compares the level of a desired signal to the level of background noise.

V. APPLICATION OF STEANOGRAPHY

i) Confidential Communication and Secret Data Storing
ii) Protection of Data Alteration
iii) Access Control System for Digital Content Distribution
iv) E-Commerce
v) Media
vi) Database Systems.
vii) Digital watermarking

VI. CONCLUSION

In the past few years, Steganography has become an interested field of data hiding techniques. This paper provides an overview of different steganography methods that satisfy the most important factors of steganography design like undetectability, capacity and robustness. We surveyed various types of steganography. We studied the various techniques which help to improve in security.

VII. REFERENCES

[1] http://www.ijcset.com/docs/IJCSET16-07-05-049.pdf

[2]https://arxiv.org/ftp/arxiv/papers/1401/1401.5561.pdf

[3]https://www.ermt.net/docs/papers/Volume_3/5_May2014/V3N5-190.pdf

[4]https://www.clear.rice.edu/elec301/Projects01/steganosaurus/background.html

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

[6]http://www.ijaiem.org/volume3issue2/IJAIEM-2014-02-27-062.pdf

[7]https://pdfs.semanticscholar.org/4b28/ba4f1d4bdfd751b87a6788edf4e240b4a574.pdf

[8]Singh, Nanhay, Bhoopesh Singh Bhati, and R. S. Raw. "Digital image Steganalysis for computer forensic investigation." Computer Science and Information Technology (CSIT) (2012): 161-168..

[9] AL-Shatnawi, Atallah M., and Bader M. AlFawwaz. "An Integrated Image Steganography System with Improved Image Quality." Applied Mathematical Sciences 7.71 (2013): 3545-3553.

[10] Bhattacharyya, Souvik and Gautam Sanyal. "A Robust Image Steganography using DWT Difference Modulation (DWTDM)." International Journal of Computer network & Information Security 4.7 (2012)..

[11] Amin, Mohamed "Muhalim and Ibrahim, Subariah and Salleh, Mazleena and Katmin, Mohd rozi (2003) Information hiding using steganograph

[12] Ibrahim, Rosziati, and Teoh suk Kuan. "Steganography Algorithm to hide secret message inside an Image." arXiv preprint arXiv: 1112.2809 (2011)

[13] Nosrati, Masoud, Ronak Karimi, and Mehdi Hariri. "Audio Steganography: A Survey on Recent Approaches."World Applied Programmi ng2.3 (2012): 202-205..

[14] Dutta, Poulami, Debnath Bhattacharyya, and Tai-hoon Kim. "Data hiding in audio signal: A review."International journal of database theory and application2.2 (2009): 1-8..

[15] H.B.kekre , Archana Athawale ,"Information Hiding In Audio Signal".Intertional Journal of Computer Application volume 7-No.9
October 2010.

[16] Sohag, Saeed Ahmed, Md Kabirul Islam, and Md Baharul Islam. "A Novel Approach for Image Steganography Using Dynamic Substitution and Secret key. "

[17] Morkel, Tayana, Jan HP Eloff, and Martin S. Olivier. "An overview of image steganography." ISSA. 2005.

[18] AL-Shatnawi, Atallah M.,and Bader M. AlFawwaz. "An Integrated Image Steganography System with Improved Image Quality."Applied Mathematical Sciences
7.71 (2013): 3545-3553..

[19] Bhattacharyya, Souvik, and Gautam Sanyal. "A Robust Image Steganography
using DWT Difference Modulation (DWTDM)."
International Journal of Computer Network &
Information Security4.7 (2012) .

[20] Saddaf rubab and M Younus article: Improved Image Steganography Technique for Colored Images using Wavelet Transform. International Journal of Computer Applications 39(14):29-32, February 2012. Published by Foundation of Computer Science, New York, USA