International Journal of Scientific Research and Management (IJSRM)
||Volume||5||Issue||06||Pages||5410-5414||2017||
Website: www.ijsrm.in ISSN (e): 2321-3418
Index Copernicus value (2015): 57.47 DOI: 10.18535/ijsrm/v5i6.08

Comparative Study on different Steganographic Techniques

Rashmeet Kaur Chawla[1], Gurpreet Kaur[2]

[1]IT Department
Sri Guru Tegh Bahadur Institute of Management and Information Technology
New Delhi
rashmeet_c@yahoo.com
[2]NIIT Technologies Limited,
Greater Noida
gk20gurpreet@gmail.com

Abstract: The high speed digital world of today has eased the process of data transmission. Today, large amount of data can be transferred in small amount of time which has raised a big question on the secrecy of data, since it can easily be accessed by any third party. Digital Steganography is the science that involves communicating secret data in an appropriate multimedia carrier such that the existence of communication is hidden.

The art of information hiding has gained much importance in past few years because after having solved the issue of speed and amount of data to be transferred, the other big concern is the security of that data as the information is being transmitted via common channels of communication. Steganography is a technology where data compression, cryptography and information theory like methods are brought together to provide the required amount of secrecy to transfer data.

Classification of steganography techniques into multiple categories is based on the cover modification applied in the embedding process and the type of cover used for secret communication. This is totally a review paper, in which we provide the comparison of available steganography methods of hiding text in an image file, audio file, text file or a video file using some basic techniques namely Substitution System, Transform Domain, Spread Spectrum technique, Statistical Method, Distortions Technique and Cover Generating Methods which are categorised accordingly in their respective domains. These types of files act as a cover file for sending the secret message in embedded form.

Keywords: Steganography, Crytography, robustness, imperceptibility.

1. Introduction

Modern world is completely digitized, so the need to protect digital data urged the creation of digital steganography [3]. Digital steganography is a technique using which we protect our digital data by hiding it into another piece of data so that attackers will not be able to notice it[1]. Many people misinterpret cryptography and steganography as one of the same thing, but cryptography means protecting the content of the message and steganography is to protect their very existence [1].

The main job of steganography is storing the digital data, hiding it and embedding it into a different type of data to forbid unauthorised and illegal access to someone else's data[1]. The cover media is used to implement the very concept of steganography. The type of cover media is chosen on the basis of amount of secret data to be embedded. The communication among data takes places in such a secure manner that the existing information goes completely undetectable [5]. The goal of steganography is to embed the secret data into cover media in such a way that no one apart from sender and receiver should be able to decode the message and do not even realise that it contains a secret message.

There are few properties that must be kept in mind while creating a digital data hiding system [1]. These are:-

a. Robustness
In computer science, robustness is the ability of a computer system to cope with errors during execution and cope with erroneous inputs. It is the amount of difficulty required to decode the secret message. [11]

b. Embedding Capacity
It refers to the amount of secret information that can be embedded in the cover image without affecting the quality of the cover media format.

c. Imperceptibility
It is the property by which a person cannot be able to distinguish between an original image and a stego image obtained after embedding secret message.

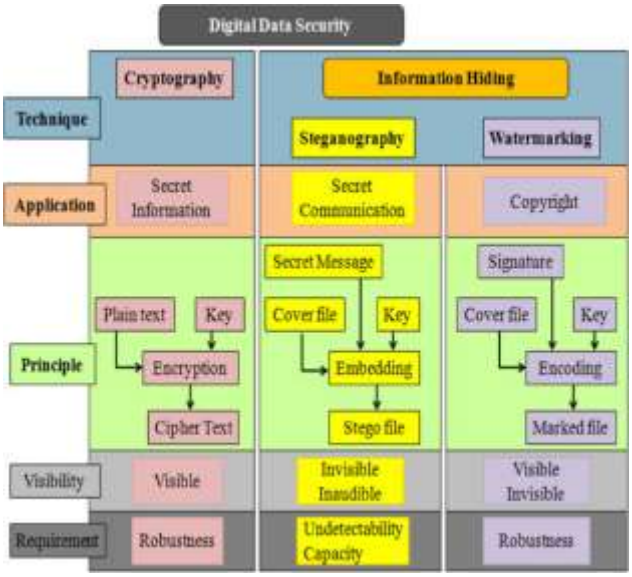

Figure 1

There are three basic types of stego systems, namely

a) Pure Key Stego systems

It is the type of steganography systems that do not require any type of prior information for communication process, such as sending some secret information for sending message [4]. It is the most preferred method of steganography because no stego key is required to be shared among the communicating partners. [6]

b) Private key Stego systems

In this type of steganography system, the sender and the receiver communicate using a secret key that the sender embeds the secret message in the cover along with the secret key [4]. At the receivers end, if the secret key is known, the receiver can extract the secret message out of the cover. The information is not at all accessible to anyone who does not know about the secret key. This is similar to symmetric cipher method for secret message transmission. [6]

c) Public Key Stego systems

This is the third type of steganography that involves two keys, one of them a private key (secret key) and a public key for transmitting the secret message [4]. The private key is used to encode the secret message and is kept safe aside while public key is available to everyone in that system. The senders and receivers usually exchange Public keys of some systems and algorithms before even the transmission takes place. The sender transmits the message using receiver's public key and at the other end, the receiver decodes the message using his private key and if the key matches, the message is received by the receiver after decoding. It would be the same message as sent by the sender. [6]

Other types of steganography that exist are:- Mobile Messaging Steganography and MMS Access Steganography[4].

The Steganography technique consists of a stego object [3] that contains the hidden message protected with a modified cover that stores and transmits the data. The type of cover that contains the secret information identifies the sego object type; for example: if the cover is a text file containing sego information then it is a sego-text object; Similarly we have stego-audio, stego-video, stego-image objects for embedded cover-audio, cover-video and cover-image respectively.

Data confidentiality and information security are improved nowadays with the help of steganography along with other data hiding techniques. Many of the digital file formats use the technique of steganography but it is suitable only for those formats that hold a high redundancy rate. The bits of an object that can go undiscovered when altered are known as redundant bits. Many of the currently used file formats are being discovered whose redundant bits go undiscovered along with the previously used audio and video file formats.

There are four major types of file formats that use steganography.

2. Image

In this type of steganography, the image is the media that carries data in hidden form. The available image formats (JPEG, PNG etc.) are used for transfer of data. Image steganography can be done using following ways:-

2.1 Exploiting Image Format

It is the simplest of all that includes adding the text file at the end of image file and then exploiting the image format to store and transmit the data. Every image file contains an EOF (end of file) marker tag [5]. The secret message is added to the image after that tag so that when the image is viewed in some image viewer application at the receiver's end then only the part of file till marker tag is opened and rest of the file is ignored and it does not deteriorate the image quality [1].

2.2 Spatial Domain Steganography

In this type of steganography, instead of all the End Of File bits only the Least Significant Bits (LSB) of the cover image are used to hide the secret information in cover image [5]. These bits are used because they contain noise and altering these bits doesn't affect the image or its quality [5].

Other method used in this technique is Hiding Grey images using Block Technique in which the cover image is divided into blocks of equal size such that pixels in those blocks are compared to each other unless a pixel with nearest value is obtained so that if secret message is embedded in that pixel then minimum altered image will be obtained as a result [3].

2.3 Transform Domain Steganography

This includes hiding the secret message in the most

significant areas of cover image to avoid the risk of attack and increase the security of data. It further consists of discrete Cosine Transformation (DCT) and Discrete Wavelet Transformation (DWT) based steganography [5]. This is one of the best methods of transforming images since large amount of data can be transferred with high security and no loss of the secret message occurs. It is one of the highly invisible ways of transmitting data [3].

2.4 Adaptive Steganography

The base of Adaptive steganography is formed by spatial domain and frequency domain steganography. The other name of adaptive steganography is statistic Aware Embedding or masking. This type of technique makes use of statistical characteristics to find out the place or pixel coordinates of the image where the designated change can be applied. Since these extra bits always contain some noisy information, so the secret data is stored in these pixels in form of noisy channels that are replaced by the original noisy data and transmitted to the receiver [5].

3. Text

In this type of steganography, the media that carries data in hidden form is text. The message can be hidden using various hiding techniques, which can be divided into further categories, which are:-

3.1 Format Based Techniques

Steganography in documents is focussed on altering the basic characteristics of the text file or text formatting. The hidden message is passed in the form of text only, by just changing the format of the text, for example, word shifting, line shifting, text resizing or change in the style etc. In word shifting, one can add tabs and spaces at the end of each line in the document and thereby encode a secret message in it [4].

3.2 Statistical Techniques

The hidden message is passed in the form of text only by generating the cover text using statistical properties, for example, by bringing out variation in character or word sequences in the sentences.

One can also use some publically available cover source such as some newspaper, journal or article whose line or page numbers can be used as a secret message that will be decoded along with the main message and hence no third party will be able to identify any type of secret message that is embedded along with the content[4].

3.3 Linguistic Techniques

The hidden message is passed in the form of text only by using the syntax and semantics, for example, by making proper use of punctuation mark in syntactic method or setting background color and font type. Color is one of the most widely used way of applying steganographic technique where we may choose predefined colors and font for some of the invisible characters like carriage return, tab or space. Since no user will be interested in color or font of these invisible characters, hence one can easily add secret message to it [4] and above all no extra information or bits are required for these data transmissions. We may also use synonyms as substitute words in semantics method like usage of context free grammar [1].

4. Audio

We have many formats of audio file available, for example MP3 and WAV. Steganography practice assumes that the cover utilized to hide messages should not raise any suspicion to opponents. In fact, the availability and the popularity of audio files make them eligible to carry hidden information. Various parameters influence the quality of audio steganographic systems. Besides the amount of the hidden data and its imperceptibility level, robustness against removal or destruction of embedded data remains the most critical property in a steganographic system [5].

The robustness criteria are assessed through the survival of concealed data to noise, compression and manipulations of the audio signal (e.g., filtering, re-sampling, re-quantization). The technique of steganography can take place in audio formats by shifting the binary sequence of the audio files or transmitting the secret data in the inaudible frequency range.

4.1 Parity Coding Method

The parity coding method is one in which the audio signal is broken into several regions then parity bits of those regions are encoded with secret message [4]. The one of the most important advantage of this method is that the sender has more options onto which bits of regions, can data be transmitted in a much more un-obstructive manner [5].

4.2 Phase Change Method

Next change that can be done in audio files is the change in phase because the phase change is inaudible to normal human ears as noise is[4], so one can alter the phase signals of the audio file by embedding the secret data into phase shifts and transmit the message.

Among all data hiding techniques, phase coding tolerates better signal distortion. The only problem with this method is that it has low data transmission rate and hence forth it is a complex method [5].

4.3 Echo Hiding

This type of encoding occurs depending on the amount of echo produced by the audio file which is directly proportional to amount of data in bits that can be secretly encoded [4].

In this, small echo is added to the data carrying signal that brought in the information and then on the basis of echo parameters (Initial amplitude, decay rate and offset) the data is made invisible [1].

4.4 Tone Insertion

Tone insertion techniques rely on the inaudibility of lower power tones in the presence of significantly higher ones. Embedding of secret data is done by inserting inaudible tones in cover audio signals [1].

Tone insertion method can resist to attacks such as low-pass filtering and bit truncation.

5. Video

Since a video file is a combination of images and sound files both, hence lots of secret data can be embedded in a video file and transferred to the decoder. The available video formats are:- MPEG, MP4, AVI etc. that can be used to store and transmit secret hidden data.

A video can be viewed as a sequence of still images. Data embedding in videos seems very similar to images. However, there are many differences between data hiding in images and videos, where the first important difference is the size of the host media. Since videos contain more sample number of pixels or the number of transform domain coefficients, a video has higher capacity than a still image and more data can be embedded in the video. [10]

5.1 DCT

Because video consists of images as well, hence we can apply Discrete Cosine Transformation (DCT) separately to each image frame of the video and embed a secret message in them. This is a highly robust and complex method. Data is embedded in the transform coefficients. [5]

When only small data are embedded in the video/image, it is not noticeable. But when large amount of data are embedded in the video, the DWT (sub Bands: LL, LH, HL, HH) are used for detection. Data is embedded in LL sub-band to avoid compression losses. [8]

5.2 LSB

Least Significant Bit (LSB) technique can be used to apply steganography in video files as well. It is one of the primitive and easily implemented embedding method. The information is embedded in the LSB of pixel colours[1]. On an average, only half of the bits in the image will need to be modified to embed a secret message using the maximal cover size.

While using a 24-bit image gives a relatively large amount of space to hide messages, it is also possible to use an 8-bit image as a cover source. The changes of LSB may not be noticeable because of the imperfect sensitivity of the human eyes. [8]

5.3 TPVD

Tri-way pixel-value differencing is used for embedding secret message in video frames. TPVD enlarges the capacity of the hidden secret information and provide an imperceptible stego-image for human vision with enhanced security. A small difference value of consecutive pixels can be located on a smooth area and the large one is located on an edged area.

According to the properties of human vision, eyes can tolerate more changes in sharp-edge blocks than in smooth blocks. That is why more data can be embedded into the edge areas than into smooth areas. [10]

5.4 Bit Plane Complexity Segmentation

Bit Plane Complexity Segmentation is one of the best techniques that are used for hiding data in MPEG formats.

BPCS Technique:-

a) Canonical Grey Code

- In PBC the major portions of the regions on the higher bit planes are relatively flat in color (mostly all 0s or all 1s).
- This is because of the "Hamming Cliffs" which occur with PBC where a small change in color affects many bits of the color value.

In binary:
127 = 01111111 & 128 = 10000000
In gray code:
127 = 01000000 & 128 = 11000000
In gray code the representation of adjacent gray levels will differ only in one bit(unlike binary format where all the bits can change).
CGC images do not suffer from Hamming Cliffs.

b) Complexity of an image
The complexity of an image(α) is defined by the following:
α =k/The maximum possible B-W changes in the image,
where, k is the total length of black-and-white border in the image.
So, value of α ranges over $0 \leq \alpha \leq 1$.

c) Conjugation of a binary image:-
It is applied when the complexity of the vessel image block is less than the threshold and cannot be used for embedding the secret data.
P * = P XOR Wc,
where P* is a conjugated 8X8 block of vessel image,
P is an informative (i.e. less complex) 8X8 block of vessel image,
Wc is a complex binary pattern

After conjugation, complexity of the vessel image blocks increases and thus can be used for embedding secret data.
$\alpha(P^*) = 1 - \alpha(P)$. [9]

6. CONCLUSION

We have done an analysis of different types of

steganography techniques that can be applied to implement the concept of steganography through this paper. The carrying capacity of each type of media is defined within it. All methods have their pros and cons in terms of capacity, security and robustness of the secret data. Some methods have higher chances of being attacked but have high carrying capacity while others have low payload capacity but cannot prevent attacks and hence low chances of being detectable. Image steganography is the widely used method of steganography as it has several methods of encoding the secret message in the various image formats as comparable to audio and video formats.

7. References

[1] Navneet Kaur, Sunny Behal, *A Survey On Various Types Of Steganography and Analysis Of Hiding Techniques*, International Journal of Engineering Trends and Technology (IJETT) – Volume 11 Number 8 - May 2014.

[2] https://www.slideshare.net/BSheghembe/steganography-presentation-47951802.

[3] Mr. Falesh M. Shelke, Miss. Ashwini A. Dongre, Mr. Pravin D. Soni, *Comparison of different techniques for Steganography in images*, International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 3, Issue 2, February 2014.

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

[5] Harjit Singh, *Analysis Of Different Types Of Steganography*, IJSRSET, Volume 2, Issue 3, 2016.

[6] C.P.Sumathi, T.Santanam, G.Umamaheswari, *A Study of Various Steganographic Techniques Used for Information Hiding*, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, December 2013.

[7] Fatiha Djebbar, Beghdad Ayad, Karim Abed Meraim and Habib Hamam, *Comparative study of digital audio steganography techniques*, EURASIP Journal on Audio, Speech, and Music Processing, licensee Springer. 2012.

[8] Souma Pal and Prof. Samir Kumar Bandyopadhyay, *Various Methods of Video Steganography*, International Journal of Information Research and Review, Vol. 03, Issue, 06, pp. 2569-2573, June, 2016.

[9] Eiji Kawaguchi and Richard O. Eason, *Principle and applications of BPCS-Steganography*,1999, SPIE 3528, Multimedia Systems and Applications, 464, Conference Volume 3528.

[10] Sherly A P and Amritha P P, *A Compressed Video Steganography using TPVD*, International Journal of Database Management Systems (IJDMS) Vol.2, No.3, August 2010.

[11] https://en.wikipedia.org/wiki/Robustness_(computer_science)

Author Profile

Ms. Rashmeet Kaur Chawla, received the B.Sc(Hons) Computer Science and M.Sc. Computer Science degrees from University of Delhi in 2014 and 2016 respectively. Her field of specialization is Information Security.

Ms. Gurpreet Kaur, received the B.sc(Hons)Computer Science degree from University of Delhi and MCA degree from Guru Gobind Singh Indraprastha University in 2014 and 2017 respectively. Her field of specialization is Core and Advanced JAVA.