EXPLORING DIFFERENT STEGANOGRAPHY TECHNIQUES ON TEXT, IMAGE, AUDIO & VIDEO FILES

Jeswin Roy Dcouth
Research Scholar
Vinayaka Missions Research Foundation
Salem, India
email: jespro89@gmail.com

Dr. K Somasundaram
Professor
Computer Science and Engineering, AVIT
Vinayaka Missions Research Foundation
Salem, India.

***Abstract*—Steganography is the art and science of concealing the existence of the message within seemingly harmless cover carrier for communication and the extraction of embedded message at the destination. The choice of the carrier used to embed the message, steganography can be classified into text, image, audio or video steganography. This paper provides a survey on different steganography techniques on text, image, audio and video and their performance comparison based on different qualitative evaluation parameters.**

I. INTRODUCTION

The word steganography literally means ”covered writing” which is derived from the Greek language. Steganography is the art and science of concealing the existence of the message within seemingly harmless carriers or cover Carrier: text, image, video, audio, etc. for communication and extracting the embedded message at the destination by the intended recipient. By doing this, it does not alter the structure of the secret message being embedded. In an Information rich environment where internet is the communication channel, it is vital to provide security to information being transferred.

Steganalysis is the art of detecting the presence of steganography.

Basic components of steganography are as follows:

1) **Embedded Data**
   The text to be concealed in a cover carrier like text, image, video, audio etc is called embedded data.
2) **Cover**
   A carrier such as text, image, audio, or video file that can be used to hide embedded data is called cover.
3) **Stego - Key**
   The key used to embed the secret information in the cover medium is called stego-key. A stego-key is used to for the detection/recovery of embedded data at the destination.
4) **Stego File**
   The cover medium which is embedded with the secret information. Depending on the cover media used to embed secret data steganography can be classified into the following:

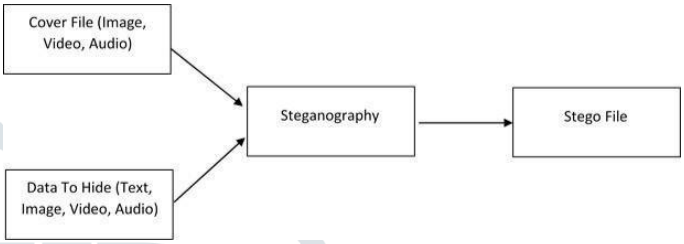

Fig.1. Process Involved in Steganography

1) Steganography In Text/Documents
2) Steganography In Images
3) Steganography In Audio
4) Steganography In Video

The factors that determine the efficiency of a steganography technique are as follows:

1) **Robustness**: It refers to the ability of embedded data to remain intact if the stego file is subjected to any trans-formations like linear and non-linear filtering, rotations, cropping, lossy compression, etc.
2) **Imperceptibility**: The concealment of a steganographic algorithm as it is the basic requirement for the strength of the steganography technique.
3) **Payload Capacity**: It is the amount of information that can be hidden in the cover source.
4) **PSNR** (Peak Signal to Noise Ratio): The term peak signal-to-noise ratio (PSNR) is the ratio between the maximum possible value (power) of a signal and the power of distorting noise that affects the quality of its representation. This ratio is used for measuring the quality between the original and a compressed image. The higher value of PSNR, 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.
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.

II. Approaches for Secure Steganography

A. Steganography In Text/Documents

Steganography in text is done by changing the formatting of the text medium, changing the words within a text, generating random character sequences etc. The information embedding in the document can be accomplished by changing the structure of the document with seemingly less change in the output. Text steganography can be broadly classified into three types as shown in Figure.

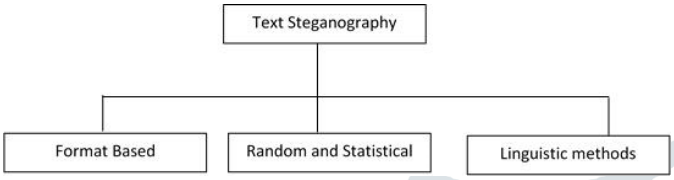

Fig. 2. Classification of Text Steganography

1) Format-based methods: Format-based methods uses formatting of the cover-text to embed the secret data. It does not tamper the value of the cover medium. It is an open space method [1]. Extra white spaces are added into the cover medium to hide the secret information. The white spaces used to embed the information can be added after end of each word, sentence or paragraph. If a single space is identified, it is interpreted as 0 and if two consecutive spaces identified, they are interpreted as 1. Two other format-based methods are word shifting and line shifting. The horizontal alignment of words are shifted to embed the information which involves the changing of distances between the words [2]. Vertical alignments of some lines of the text are shifted in line shifting method that creates a unique hidden shape which can be used to embed the secret information in it [3].

2) Random and statistical generation methods: In order to prevent the steganalysis by comparing the stego file with a known plain text, the text steganography can be done by leveraging the statistical properties of word length and letter frequencies which can be used to form words which have the same statistical properties of words in the original text document [4].

3) Linguistic methods: The linguistic method [5] leverages the linguistic properties of the text to hide information. One of the linguistic method is syntactic method. In syntactic method, the location of punctuation signs like comma (,), full-stop (.), etc in the document are used to embed the secret information. This method needs proper identification of places where the signs can be inserted. Semantic method is another linguistic steganography where the synonym of words is used. In order to hide information in it, the words are replaced by their synonyms

B. Steganography in Images

In image steganography, the cover medium used to carry the secret message is an image. The various image steganography techniques are:

- Substitution technique in Spatial Domain
- Transform domain technique
- Spread spectrum technique
- Statistical technique
- Distortion technique

1) Substitution technique in Spatial Domain: In this technique the LSB (least significant bits) of the cover image is replaced and it does not modify the complete cover object. It is the simplest image steganography method for data hiding. It is very much vulnerable to attacks such as compression, transforms, etc.

2) Transform domain technique: The various transform domains techniques are very much resistant to attacks like compression, filtering, etc. The various transform domain techniques are as follows:

- Discrete Cosine Transform (DCT)
- Discrete Wavelet Trans- form (DWT)
- Fast Fourier Transform (FFT)

These transform domain methods are used to hide information in transform coefficients of the cover images.

3) Spread spectrum technique: This method hides and recovers a message within digital imagery while maintaining the original image size. This method modulates a narrow band signal over a carrier. The frequency of the carrier is shifted continuously using a pseudorandom noise generator which is fed with a secret key. This results in the spreading of the spectral energy of the signal over a wide band and therefore its density decreases under the noise level. The embedded message extraction is can be done at the receiver end with the help of the same key and noise generator to tune on to the correct frequencies and thus demodulate the original signal.

4) Statistical technique: In statistical method, the cover image is divided into blocks and the message bits to be embedded are hidden in each block. Various numerical properties of cover image are changed for embedding the information.

5) Distortion technique: Information is stored by adding sequence of changes to result in signal distortion. At the receiver end, the distorted image is checked for the various differences from the original cover.

C. Steganography In Audio

Audio steganography is a technique in which secret message is embedded into In image steganography, the cover medium used to carry the secret message is an image. The various image steganography techniques are:

- Substitution technique in Spatial Domain
- Transform domain technique

- Spread spectrum technique
- Statistical technique
- Distortion technique

1) Substitution technique in Spatial Domain: In this technique the LSB (least significant bits) of the cover image is replaced and it does not modify the complete cover object. It is the simplest image steganography method for data hiding. It is very much vulnerable to attacks such as compression, transforms, etc.

2) Transform domain technique: The various transform domains techniques are very much resistant to attacks like compression, filtering, etc. The various transform domain techniques are as follows:

- Discrete Cosine Transform (DCT)
- Discrete Wavelet Trans- form (DWT)
- Fast Fourier Transform (FFT)

These transform domain methods are used to hide information in transform coefficients of the cover images.

3) Spread spectrum technique: This method hides and recovers a message within digital imagery while maintaining the original image size. This method modulates a narrow band signal over a carrier. The frequency of the carrier is shifted continuously using a pseudorandom noise generator which is fed with a secret key. This results in the spreading of the spectral energy of the signal over a wide band and therefore its density decreases under the noise level. The embedded message extraction is can be done at the receiver end with the help of the same key and noise generator to tune on to the correct frequencies and thus demodulate the original signal.

4) Statistical technique: In statistical method, the cover image is divided into blocks and the message bits to be embedded are hidden in each block. Various numerical properties of cover image are changed for embedding the information.

Distortion technique: Information is stored by adding sequence of changes to result in signal distortion. At the receiver end, the distorted image is checked for the various differences from the original coverdigitized audio signal in an imperceptible

which creates a slight alteration of the corresponding carrier audio file. Characteristics of audio signals such as redundancy, unpredictable nature, etc. can be utilized for covert communi-cations to hide secret information [6].

Four major audio steganography algorithms are discussed below:

- Low-bit encoding
- Phase encoding
- Spread spectrum coding
- Echo data hiding

5) Low-bit Encoding: In Low-bit encoding [7], the following steps are performed:

Step 1: Audio file chosen for carrying the secret data message is converted into bit pattern.
Step 2: Binary version of each character of the secret message is obtained.
Step 3: Check which LSB of the binary version of the audio file is to be replaced with the message bits.
Step 4: LSB of the bit pattern of the cover audio file is substituted with the characters of the secret message.

In some implementations of LSB coding, two least significant bits of the carrier binary file are replaced with two message bits which increases the amount of data that can be encoded but compromises on the amount of noise in the audio file.

6) Phase Coding: The phase components of sound are not as perceptible to the human ear as noise is. Instead of creating perturbations, the message bits encoded as shifts in phases in the phase spectrum of a digital signal which results in an inaudible encoding which is in terms of signal-to-perceived noise ratio (SPNR).

7) Spread Spectrum Coding: The Spread Spectrum (SS) coding method [9] involves spreading of the bits of the secret information across the frequency spectrum of the audio signal as much random as possible.

Two classifications of Spread Spectrum Coding used in audio steganography are as follows:

Direct-Sequence Scheme Frequency and Hopping Scheme.

In direct-sequence spread spectrum, a constant called chip rate is used to spread out the secret message and which is then modulated with a pseudorandom signal. The resultant is then interleaved with the cover audio signal. In frequency-hopping SS, the frequency of the cover audio file spectrum is altered so that it hops rapidly between frequencies.

8) Echo Hiding: Echo hiding [10] method embeds the secret information by introducing an echo into the discrete audio signal. It requires three parameters of the echo need to be altered from the original signal.to hide the secret the data:

- Amplitude
- decay rate
- offset (delay time)

The first offset value represents a one (binary), and the second offset value represents a zero (binary) in the figure.

D. Steganography In Video

Video steganography is the process by which the secret information is hidden in a video file. The existence of message in the video file cannot be recognized by humans as the change of a pixel color is negligible. In order to perform video steganography, the host video is divided into frames and each frame is an image. The secret message is embedded into frames and these frames are recombined to produce the video.

Steganography in video can be classified into two main classes:

- Embedding data in uncompressed raw video, which is compressed later [11] [12].
- Embedding data directly in compressed video stream. Some of the most well-known approaches for video steganography are as follows:

1) Least Significant Bit method (LSB): Least Significant Bit method involves modification of the least significant bit of the host video file based on the LSB of the secret message.

2) Discrete Cosine Transform (DCT) transformation: In Discrete Cosine Transform (DCT) transformation method [14], the secret message is converted into binary. The cover image is segmented into 88 block of pixels. Subtract 128 in each block of pixels and then DCT is applied to each segmented block. The resultant block is compressed through quantization table. The LSB of each DC coefficient is computed and it is replaced with bits of secret message.

3) Vector Embedding Method: Vector embedding method [13] is used with video codec standard (MPEG-I and MPEG-II). The audio information is embedded to pixels of frames in host video.

III. Comparison of Steganographic Techniques

Performance of different steganographic methods can be compared based on three parameters such as capacity, perceptibility and robustness. The amount of information that can be hidden is defined by the capacity parameter. Ideally it should be as high as possible. Imperceptibility of the stego decides the ability to detect the presence of hidden data. The Robustness of the method determines the ability of the steganographic methods to resist any transformations done on it. Table I shows the comparison of the text steganographic methods, Table II shows the comparison of image steganographic methods, Table III shows the comparison of audio steganographic methods and Table IV shows video steganographic methods. The ratings are given on a scale from 1 to 3, where 1 is the least and 3 is of the highest order.

Sl.No	Technique	Capacity	Imperceptibility	Robustness
1	Format Based	2	3	1
2	Random & Statistical	1	2	3
3	Linguistic	3	1	2

TABLE I
COMPARISON OF STEGANOGRAPHIC METHODS IN TEXT

Sl.No	Technique	Capacity	Imperceptibility	Robustness
1	Substitution	3	1	1
2	Transform domain	1	3	3
3	Spread spectrum	2	3	3
4	Statistical	1	1	2
5	Distortion	1	2	1

TABLE II
COMPARISON OF STEGANOGRAPHIC METHODS IN IMAGE

Sl.No	Technique	Capacity	Imperceptibility	Robustness
1	Low-Bit Encoding	3	1	1
2	Phase Coding	1	1	3
3	Spread spectrum Coding	2	3	3
4	Echo Hiding	3	1	3

TABLE III
COMPARISON OF STEGANOGRAPHIC METHODS IN AUDIO

Sl.No	Technique	Capacity	Imperceptibility	Robustness
1	LSB	1	3	1
2	DCT	3	3	2
3	Vector Embedding	3	3	3

TABLE IV
COMPARISON OF STEGANOGRAPHIC METHODS IN VIDEO

IV. Conclusion

This paper provides a survey of different techniques of setaganography in text documents, images, audio and video file. A comparative analysis of the techniques has been done based on 3 parameters which are capacity to embed the information, imperceptibility and robustness.

References

[1] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, *"Techniques for data hiding"*, IBM Systems Journal, vol. 35, Issues 3& 4, 1996, pp. 313-336.

[2] Y. Kim, K. Moon, and I. Oh, *"A Text Watermarking Algorithm based on Word Classification and Inter-word Space Statistics"*, Proceedings of the Seventh International Conference on Document Analysis and Recognition (ICDAR03), 2003, pp. 775779.

[3] A.M. Alattar and O.M. Alattar, *"Watermarking electronic text documents containing justified paragraphs and irregular line spacing "*, Proceedings of SPIE - Volume5306, Security, Steganography, and Watermarking of Multimedia Contents VI, June 2004, pp- 685-695.

[4] P. Wayner, *"Strong Theoretical Steganography*, Cryptologia, XIX(3), July 1995, pp. 285-299.

[5] M. Niimi, S. Minewaki, H. Noda, and E.Kawaguchi, *"A Framework of Text-based Steganography Using SD-Form Semantics Model"*, Pacific Rim Workshop on Digital Steganography 2003, Kyushu Institute of Technology, Kitakyushu, Japan, July 3-4, 2003.

[6] Natarajan Meghanathan and Lopamudra Nayak, Steganalysis Algorithms For Detecting The Hidden Information In Image, Audio And Video Cover Media at International Journal of Network Security & Its Application (IJNSA), Vol.2, No.1, January 2010.

[7] R. Sridevi, A. Damodaram and S.V.L. Narasimham, Efficient Method of Audio Steganography by Modified LSB Algorithm and Strong Encryption Key with Enhanced Security, Journal of Theoretical and Applied Information Technology, vol. 5, no. 6, pp. 768 771, June 2009.

[8] W. Bender, D. Gruhl and N. Morimoto, Techniques for Data Hiding,

[9] IBM Systems Journal, vol. 35, no. 3, pp. 313 336, 1996.

[10] D. Kirovski and H. Malvar, Spread spectrum Watermarking of Audio Signals, IEEE Transactions on Signal Processing, vol. 51, no. 4, pp. 1020 1033, April 2003.

[11] D. Huang and T. Yeo, Robust and Inaudible Multi-echo Audio Watermarking,, Proceedings of the IEEE Pacific-Rim Conference on Multimedia, pp. 615 622, Taipei, China, December 2002.

[12] F Hartung., B. Girod."Watermarking of uncompressed and compressed video, Signal Processing", Special Issue on Copyright Protection and Access Control for Multimedia Services, 1998, 66 (3): 283-301.

[13] Bin Liu., Fenlin Liu., Chunfang Yang and Yifeng Sun," Secure Steganography in Compressed Video Bitstreams, The Third International Conference on Availability,Reliability and Security,2008.

[14] D.E. Lane Video-in-Video Data Hiding, 2007.

[15] Y. Wang, E. Izquierdo, High-Capacity Data Hiding in MPEG-2 Compressed Video, 9th International Workshop on Systems, Signals and Image Processing, UK, 2002.