International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Review on Steganography in Digital Media

Barnali Gupta Banik[1], Samir K. Bandyopadhyay[2]

[1]Assistant Professor, Department of Computer Science & Engineering, St' Thomas College of Engineering & Technology

[2]Professor, Department of Computer Science & Engineering University of Calcutta India

Abstract: ***Generally, in steganography, the actual information is not maintained in its original format and thereby it is converted into an alternative equivalent multimedia file like image, video or audio which in turn is being hidden within another object. This apparent message (known as cover text in usual terms) is sent through the network to the recipient, where the actual message is separated from it.***

Keywords: Image Steganography, Audio Steganography, Video Steganography and Protocol Steganography

1. Introduction

Steganography is a technique used for hiding information, which aims to hide the existence of the secret communication and to keep any third party unaware of the presence of the steganographic information exchange - thus securing the data transfer. The steganographic algorithm is used to embed message object onto carrier object. In this digital era different types of media can be used as carrier and message object - namely image, text, audio, video, even network protocols.Steganography in the modern day sense of the word usually refers to information or a file that has been concealed inside a digital Picture, Video or Audio file. What Steganography essentially does is exploit human perception; human senses are not trained to look for files that have information hidden inside of them.

The growth of high speed computer networks and that of the Internet, in particular, has increased the ease of Information Communication. Ironically, the cause for the development is also of the apprehension - use of digital formatted data. In comparison with Analog media, Digital media offers several distinct advantages such as high quality, easy editing, high fidelity copying, compression etc. But this type advancement in the field of data communication in other sense has hiked the fear of getting the data snooped at the time of sending it from the sender to the receiver. So, Information Security is becoming an inseparable part of Data Communication. In order to address this Information Security, Steganography plays an important role. Steganography is the art and science of writing hidden messages in such a way that no one apart from the sender and intended recipient even realizes there is a hidden message. This paper is a tutorial review of the steganography techniques appeared in the literature.

2. Related Knowledge

2.1 Concept of Steganography

The word steganography comes from the Greek "steganos", meaning covered or secret, and "graphie" meaning writing or drawing - literally mean as "covered writing" [1]. Steganography is the art and science of invisible communication, accomplished through hiding secret information into a carrier object. This technique has been used since ancient times across the globe, mostly renowned during World War times.

Detection of Steganography techniques can be categorized in two types based on the mode of intervention by the supervisor who has been assigned to identify & eliminate secret communication – these are called Active and Passive modes of Steganography. In Active mode, the supervisor will try to alter the communication with the suspected hidden information deliberately, in order to remove the secret information. On the other hand in passive mode, the supervisor simply examines the communication to try and determine if it potentially contains secret information. For any suspected message containing hidden communication, he would take notes of the detected covert communication, reports this to higher authority and lets the message through to the intended receiver without blocking it.

2.2 Definitions in Digital Media

Digital media are encoded in a machine readable format which can be created, viewed, distributed, modified and preserved on computers. Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a higher degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display. The redundant bits of an object are those bits that can be altered without the alteration being detected easily. Image and audio files especially comply with this requirement, while research has also uncovered other digital media that can be used for information hiding like network protocols.

- **Audio**

Digital audio is stored in a computer as a sequence of 0's and 1's. A discrete audio signal is created by sampling a continuous analog signal at a specified rate. In the digital domain, PCM (Pulse Code Modulation) is the mostly used mechanism to store audio. The analog audio is sampled in

DOI: 10.21275/SUB151127

accordance with the Nyquest theorem and the individual samples are stored sequentially in binary format [2]

- **Image**

Digital Images are electronic snapshots taken of a scene or scanned from documents, such as photographs, manuscripts, printed texts, and artwork. The digital image is sampled and mapped as a grid of dots or picture elements (pixels). Each pixel is assigned a tonal value (black, white, shades of gray or color), which is represented in binary code (zeros and ones). The binary digits ("bits") for each pixel are stored in a sequence by a computer and often reduced to a mathematical representation (compressed format). The bits are then interpreted and read by the computer to produce an analog version for display or printing.

- **Text**

According to the Unicode Standard, plain text is a pure sequence of characters. Plain text is public, standardized, and universally readable. Whereas, styled text, also known as rich text, is any text representation containing plain text completed by information such as a language identifier, font size, color, hypertext links, etc. For instance, Rich text such as SGML, RTF, HTML, XML, and TEX relies on plain text.

- **Video**

Video signal is a highly correlated signal, this correlation is from two sources. The first one is spatial correlation that results from inter pixel correlation within each frame of the video sequence. The second one is the temporal correlation that results from the slow time varying nature of the video signals. [6]

- **Network Protocols**

A network protocol defines rules and conventions for communication between network devices. Protocols for computer networking generally use packet switching techniques (to send and receive messages in the form of packets). Network protocols include mechanisms for devices to identify and make connections with each other, as well as configuring rules that specify how data is packaged into messages sent and received. Some protocols also support message acknowledgement and data compression designed for reliable and/or high performance network communication.

2.3 Different kinds of Steganography in Digital Media

Steganography can be categorized into 5 types based on the use of different kinds of digital media as carrier:

2.3.1 Audio Steganography
2.3.2 Image Steganography
2.3.3 Text Steganography
2.3.4 Video Steganography
2.3.5 Network Steganography

2.3.1 Audio Steganography

Embedding secret messages into digital audio file is known as Audio Steganography. It is usually a more difficult process than embedding messages in other media. Audio Steganography methods can embed messages in WAV, AU, and even MP3 sound files. The properties of the human auditory system (HAS) are exploited in the process of audio Steganography. Auditory perception is based on the critical band analysis in the inner ear where a frequency-to-location transformation takes place along the basilar membrane. The power spectra of the received sounds are not represented on a linear frequency scale but on limited frequency bands called critical bands [3]

2.3.1.1 Existing methods of Audio Steganography

To embed data secretly onto digital audio file there are few techniques introduced earlier. The lists of methods are:

a) LSB Coding
b) Phase Coding
c) Parity Coding
d) Spread Spectrum
e) Echo Hiding

a) Least Significant Bit (LSB) Coding

One of the earliest techniques studied in the information hiding of digital audio (as well as other media types) is Least Significant Bit modification coding technique. In this technique LSB of binary sequence of each sample of digitized audio file is replaced with binary equivalent of secret message

Advantage: It is the simplest way to embed information in a digital audio file. It allows large amount of data to be concealed within an audio file, use of only one LSB of the host audio sample gives a capacity equivalent to the sampling rate which could vary from 8 kbps to 44.1 kbps (all samples used) [3]. This method is more widely used as modifications to LSBs usually not create audible changes to the sounds.

Disadvantage: It has considerably low robustness against attacks.

b) Phase Coding

Phase coding addresses the disadvantages of the noise-inducing methods of audio steganography. Phase coding relies on the fact that the phase components of sound are not as perceptible to the human ear as noise is. Rather than introducing perturbations, the technique encodes 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 [5].

Phase coding is explained in the following procedure:

The original sound signal is broken up into smaller segments whose lengths equal the size of the message to be encoded. A Discrete Fourier Transform (DFT) is applied to each segment to create a matrix of the phases and Fourier transform

DOI: 10.21275/SUB151127

magnitudes. Phase differences between adjacent segments are calculated.

Phase shifts between consecutive segments are easily detected. In other words, the absolute phases of the segments can be changed but the relative phase differences between adjacent segments must be preserved. Therefore the secret message is only inserted in the phase vector of the first signal segment as follows:

$$phase\_new = \begin{cases} \pi/2 & if \quad message \quad bit = 0 \\ -\pi/2 & if \quad message \quad bit = 1 \end{cases}$$

A new phase matrix is created using the new phase of the first segment and the original phase differences. Using the new phase matrix and original magnitude matrix, the sound signal is reconstructed by applying the inverse DFT and then concatenating the sound segments back together.

To extract the secret message from the sound file, the receiver must know the segment length. The receiver can then use the DFT to get the phases and extract the information.

One disadvantage associated with phase coding is a low data transmission rate due to the fact that the secret message is encoded in the first signal segment only. This might be addressed by increasing the length of the signal segment. However, this would change phase relations between each frequency component of the segment more drastically, making the encoding easier to detect. As a result, the phase coding method is used when only a small amount of data, such as a watermark, needs to be concealed.

c) Parity Encoding

Instead of breaking a signal down into individual samples, the parity coding method breaks a signal down into separate regions of samples and encodes each bit from the secret message in a sample region's parity bit. If the parity bit of a selected region does not match the secret bit to be encoded, the process flips the LSB of one of the samples in the region [5].

Advantage: The sender has more of a choice in encoding the secret bit, and the signal can be changed in a more unobtrusive manner.

Disadvantage: This method like LSB coding is not robust in nature.

d) Spread Spectrum

In the context of audio steganography, the basic spread spectrum (SS) method attempts to spread secret information across the audio signal's frequency spectrum as much as possible. Two versions of SS can be used in audio steganography: the direct-sequence and frequency-hopping schemes. In direct-sequence SS, the secret message is spread out by a constant called the chip rate and then modulated with a pseudorandom signal. It is then interleaved with the cover-signal. In frequency-hopping SS, the audio file's frequency spectrum is altered so that it hops rapidly between frequencies.

The SS method has the potential to perform better in some areas than LSB coding, parity coding, and phase coding techniques in that it offers a moderate data transmission rate while also maintaining a high level of robustness against removal techniques. However, the SS method shares a disadvantage with LSB and parity coding in that it can introduce noise into a sound file.

e) Echo Hiding

In echo hiding, information is embedded in a sound file by introducing an echo into the discrete signal. Like the spread spectrum method, it too provides advantages in that it allows for a high data transmission rate and provides superior robustness when compared to the noise inducing methods.

To hide the data successfully, three parameters of the echo are varied: amplitude, decay rate, and offset (delay time) from the original signal. All three parameters are set below the human hearing threshold so the echo is not easily resolved. In addition, offset is varied to represent the binary message to be encoded. One offset value represents a binary one, and a second offset value represents a binary zero.

2.3.2 Image Steganography

The most well-known form of steganography involves hiding messages within pictures. This is often done by altering the low order bits of an image so that the image looks unchanged, but a diff of the altered image with the original reveals a pattern corresponding to a hidden message. This form of steganography has most commonly employed bitmaps due to their simplicity of data representation (when simply flipping the low order bit, the image itself remains completely unaltered visually), but more recent research and work has been done involving the alteration of JPEG images using software such as JSteg to hide messages within seemingly ordinary photographs. JPEGs are trickier to alter due to their "layers" and embedding of data that makes them more complicated than the raw data format of bitmaps.

2.3.1.2. Existing methods of Image steganography

Steganographic techniques that modify image files for hiding information include the following:

a) Spatial domain
b) Transform domain
c) Spread spectrum
d) Statistical methods
e) Distortion techniques

DOI: 10.21275/SUB151127

Steganographic techniques that modify the image file format involve file embedding and palette embedding

a) Spatial Domain

Spatial domain steganographic techniques, also known as substitution techniques, are a group of relatively simple techniques that create a covert channel in the parts of the cover image in which changes are likely to be a bit scant when compared to the human visual system (HVS). Spatial domain techniques are broadly classified into:
1. Least significant bit (LSB)
2. Pixel value differencing (PVD)
3. Edges based data embedding method (EBE)
4. Random pixel embedding method (RPE)
5. Mapping pixel to hidden data method
6. Labeling or connectivity method
7. Pixel intensity based method
8. Texture based method
9. Histogram shifting methods

b) Transform Domain

Transform domain embedding can be defined as a domain of embedding techniques for which a number of algorithms have been suggested. The process of embedding data in the frequency domain of a signal is much stronger than embedding principles that operate in the time domain. This can be implemented by JPEG steganography (JSteg/JPHide, F5, OutGuess, MB, and YASS) and Wavelet Transform Technique. Transform domain techniques are broadly classified into:
- Discrete Fourier transformation technique (DFT).
- Discrete cosine transformation technique (DCT).
- Discrete Wavelet transformation technique (DWT).
- Lossless or reversible method (DCT)
- Embedding in coefficient bits

c) Spread Spectrum Technique

Spread spectrum transmission in radio communications transmits messages below the noise level for any given frequency. When employed with steganography, spread spectrum either deals with the cover image as noise or tries to add pseudo-noise to the cover image. This can be done by Cover image as noise and Pseudo- noise.

Spread spectrum image steganography (SSIS) described by Marvel et al., combined spread spectrum communication, error control coding, and image processing to hide information in images, is an example of this technique [6].

In SSIS, the process goes like this: the message is hidden in noise and then it is combined with the cover image to reach into a stego image. Since the power of the embedded signal is much lower than the power of the cover image, the embedded image becomes imperceptible not only to the human eye but also through computer analysis without access to the original image.

d) Statistical Methods

Also known as model-based techniques, these techniques tend to modulate or modify the statistical properties of an image in addition to preserving them in the embedding process. This modification is typically small, and it is thereby able to take advantage of the human weakness in detecting luminance variation. These techniques embed the information in the more significant areas than just hiding it into the noise level. It can be done by:
- Masking
- Filtering

This method is much more robust than LSB replacement with respect to compression since the information is hidden in the visible parts of the image. But the disadvantages of Masking and filtering Techniques are that these techniques can be applied only to gray scale images and restricted to 24 bits.

e) Distortion Techniques

Distortion techniques need knowledge of the original cover image during the decoding process where the decoder functions to check for differences between the original cover image and the distorted cover image in order to restore the secret message. The encoder adds a sequence of changes to the cover image. So, information is described as being stored by signal distortion Using this technique, a stego-object is created by applying a sequence of modifications to the cover image. This sequence of modifications is selected to match the secret message required to transmit.

f) File Embedding

Different image file formats are known for having different header file structures. In addition to the data values, such as pixels, palette, and DCT coefficients, secret information can also be hidden in either a header structure or at the end of the file. For example, the comment fields in the header of JPEG images usually contain data hidden by the invisible Secrets and Steganozorus. Camouflage, JpegX, PGE10, and PGE20 add data to the end of a JPEG image. Image storage formats such as TIFF, GIF, PNG, and WMF have a file header that can be exploited to hide arbitrary information.

g) Pallet Embedding

In a palette-based image, what matters is the fact that only a subset of colors from a particular color space is used to colorize the image. Researchers believe that every palette-based image format consists of two parts. The first part is a palette that assigns N colors as a list of indexed pairs (i , c_i) , assigning a color vector c_i to every index i , and the actual image data, which specifies a palette index for each pixel, rather than the color value itself. In some cases, the palette itself can be used to hide secret information. Because the order of the colors in the palette usually does not matter, the ordering of colors can be used to transfer information.

DOI: 10.21275/SUB151127

Performance Measure

As a performance measure for image distortion due to embedding, the well-known peak-signal-to noise ratio (PSNR), which is categorized under difference distortion metrics, can be applied to stego images. It is defined as:

$$PSNR = 10\log\left(\frac{C_{\max}^{2}}{MSE}\right)$$

where MSE denotes the mean square error, which is given as

$$MSE = \frac{I}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}(S_{xy} - C_{xy})^2$$

2.3.3 Text Steganography

A steganography technique that uses text as the cover media is called a text steganography. It is one of the most difficult types of the steganography technique. This is because text files have a very small amount of redundant data to hide a secret message.

Text steganography can be classified in three basic categories –

a) Format-based
b) Random and statistical generation
c) Linguistic method

Format-based methods used physical text formatting of text as a place in which to hide information. Generally, this method modifies existing text in order to hide the steganographic text. Insertion of spaces, deliberate misspellings distributed throughout the text, resizing the fonts are some of the many format-based methods being used in text steganography. However, Bennett has stated that those format-based methods managed to trick most of the human eyes but it cannot trick once computer systems have been used.

Random and statistical generation is generating cover text according to the statistical properties. This method is based on character sequences and words sequences. The hiding of information within character sequences is embedding the information to be appeared in random sequence of characters. This sequence must appear to be random to anyone who intercepts the message. A second approach to character generation is to take the statistical properties of word-length and letter frequency in order to create "words" (without lexical value) which will appear to have the same statistical properties as actual words in a given language. The hiding of information within word sequences, the actual dictionary items can be used to encode one or more bits of information per word using a codebook of mappings between lexical items and bit sequences, or words themselves can encode the hidden information.

The final category is linguistic method which specifically considers the linguistic properties of generated and modified text, frequently uses linguistic structure as a place for hidden messages. In fact, steganographic data can be hidden within the syntactic structure itself. [10]

2.3.1.3. Existing methods of Text steganography

Line Shifting [11]: In this method, the lines of the text are vertically shifted to some degree (for example, each line shifts 1/300 inch up or down) and information are hidden by creating a unique shape of the text. This method is proper for printed texts. However, in this method, the distances can be observed by using special instruments of distance assessment and necessary changes can be introduced to destroy the hidden information. Also if the text is retyped or if character recognition programs (OCR) are used, the hidden information would get destroyed.

a) ***Word Shifting*** [12]: In this method, by shifting words horizontally and by changing distance between words, information are hidden in the text. This method is acceptable for texts where the distance between words is varying. This method can be identified less, because change of distance between words to fill a line is quite common. But if somebody was aware of the algorithm of distances, he can compare the present text with the algorithm and extract the hidden information by using the difference. The text image can be also closely studied to identify the changed distances. Although this method is very time consuming, there is a high probability of finding information hidden in the text. The same as in the previous method, retyping of the text or using OCR programs destroys the hidden information.

b) ***Syntactic Methods*** [13]: By placing some punctuation signs such as full stop (.) and comma (,) in proper places, one can hide information in a text file. This method requires identifying proper places for putting punctuation signs. The amount of information to hide in this method is trivial.

c) ***Semantic Methods*** [15]: This method is similar to our method. In this method, the synonym of words is used for certain words thereby the information is hidden in the text. A major advantage of this method is the protection of information in case of retyping or using OCR programs (contrary to methods listed under 2-1 and 2-2). However, this method may alter the meaning of the text.

d) ***Abbreviation*** [15]: Another method for hiding information is the use of abbreviations. In this method, very little information can be hidden in the text. For example, only a few bits can be hidden in a file of several kilobytes. Also there are other text steganography methods such as Feature Coding and Open Spaces. The survey on these methods is available in [14].

Performance Measure:

Performance measure of Text Steganography can be done by Capacity Factor. In this analysis, two factors of the capacity

DOI: 10.21275/SUB151127

measurement have been used which are Embedding Ratio (ER) and Saving Space Ratio (SSR).

a) Embedding Ratio (ER): Embedding ratio is used to determine the total fitness of hidden text can be embedded in cover. This analysis is very important for steganographer to understand the fitness capability of cover text.

$$ER = \left[\frac{Total\ Bits\ of\ Stego\ Text - Total\ Bits\ of\ Cover\ Text}{Total\ Bits\ of\ Cover\ Text + Total\ Bits\ of\ Hidden\ Text} \right] X\ 100\%$$

$$ER = \left[\frac{Total\ Number\ of\ Embedded\ Bits}{Total\ Bits\ of\ Expected\ Stego\ Text} \right] X\ 100\%$$

$$Percent\ Embedded\ Bits\ (\%) = \frac{\sum_{i=1}^{1<a<100} a_i}{\sum_{i=1}^{1<b<100} b_i} \times 100\%$$

where a = Total number of embedded bits b = Total bits of cover text

b) Saving Space Ratio (SSR): Saving space ratio is used to determine the total space of hidden text that can be saved during embedding process in cover text. This analysis is very important for steganographer to understand the capability of maximum space that can be utilized in cover text in order to embed the hidden text.

$$SSR = \left[\frac{Total\ Bits\ of\ Expected\ Stego\ Text - Total\ Bits\ of\ Stego\ Text}{Total\ Bits\ of\ Expected\ Stego\ Text} \right] X\ 100\%$$

$$SSR = \left[\frac{Total\ Number\ of\ Saving\ Space\ Bits}{Total\ Bits\ of\ Expected\ Stego\ Text} \right] X\ 100\%$$

$$Percent\ Saving\ Space\ Bits\ (\%) = \frac{\sum_{i=1}^{1<a<100} a_i}{\sum_{i=1}^{1<b<100} b_i} \times 100\%$$

where a = Total number of saving space bits b = Total bits of hidden text

2.3.4 Video Steganography

Video steganography of late has also gained quite significance for researchers. The separation of video into audio and images or frames results in the efficient method for data hiding. The use of video files as a carrier medium for steganography is more eligible as compared to other techniques [8-9].Video Steganography is a technique to hide any kind of files or information into digital video format. Video (combination of pictures) is used as carrier for hidden information. Video steganography uses such as H.264, Mp4, MPEG, AVI or other video formats.

2.3.4.1. Existing methods of video steganography

Steganography in video can be divided into two main classes:

- Embedding data in uncompressed raw video, which is compressed later.
- The other, which is more difficult, tries to embed data directly in compressed video stream.

Popular technique in Video Steganography is LSB substitution method. Various techniques of LSB exist for video steganography, like:

The data is first encrypted using a key and then embedded in the carrier AVI video file in LSB keeping the key of encryption in a separate file called key file. A data hiding scheme is developed to hide the information in specific frames of the video and in specific location of the frame by LSB substitution using polynomial equation.

Hash based least significant bit technique for video steganography (HLSB) is a spatial domain technique where the secret information is embedded in the LSB of the cover frames. Eight bits of the secret information is divided into 3, 3, 2 and embedded into the RGB pixel values of the cover frames respectively. A hash function is used to select the position of insertion in LSB bits. [18]

Selected Least Significant Bit (SLSB) that improves the performance of the LSB hiding information in only one of the three colors at each pixel of the cover image. To select the color it uses a Sample Pairs analysis, given that this analysis is more effective to detect hidden information. Finally, applies a LSB Match method so that the final color is as close as possible to the original one in the scale of colors [19].

Data Hiding in Motion Vectors of Compressed Video Based on Their Associated Prediction Error deals with data hiding in compressed video. Unlike data hiding in images and raw video which operates on the images themselves in the spatial or transformed domain which are vulnerable to steganalysis. There is new method to hide the data in motion vectors of MPEG-2 compressed video. The results of this technique are evaluated on two metrics: quality distortion to reconstructed video and data size increase of the compressed video.

Performance Measure

Any Steganography technique is characterized mainly by two attributes, imperceptibility and capacity. Imperceptibility means the embedded data must be imperceptible to the observer (perceptual invisibility) and computer analysis (statistical invisibility).

The perceptual imperceptibility of the embedded data is indicated by comparing the original image or video to its stego counterpart so that their visual differences, if any, can be determined. Additionally, as an objective measure, the Mean squared Error (MSE), Peak Signal to Noise Ratio (PSNR) and Image Fidelity (IF) between the stego frame and

DOI: 10.21275/SUB151127

its corresponding cover frame are studied. The quantities are given as below,

$$MSE = \frac{1}{H * W} \sum_{i=1}^{H} (P(i,j) - S(i,j))^2$$

where, MSE is Mean Square error, H and W are height width and P(i,j) represents original frame and S(i,j) represents corresponding stego frame.

$$PSNR = 10 \log_{10} \frac{L^2}{MSE}$$

where, PSNR is peak signal to noise ratio, L is peak signal level for a grey scale image it is taken as 255.

2.3.4 Network Steganography

Network steganography is a method of hiding secret data in the normal data transmissions of users so that it ideally cannot be detected by third parties. Many new methods have been proposed and analyzed. Network steganography methods may be viewed as a threat to network security, as they may be used as a tool for confidential information leakage, for example. For this reason, it is important to identify possibilities for covert communication, as knowledge of information hiding procedures may be used to develop countermeasures [7, 9]

Network steganography may be classified into three broad groups (Figure 1):

- Steganographic methods that modify packets (MP), including network protocol headers or payload fields
- Steganographic methods that modify the structure of packet streams (MS), for example, by affecting the order of packets, modifying inter-packet delay or introducing intentional losses
- Hybrid steganographic methods (HB) that modify both the content of packets and their timing and ordering.

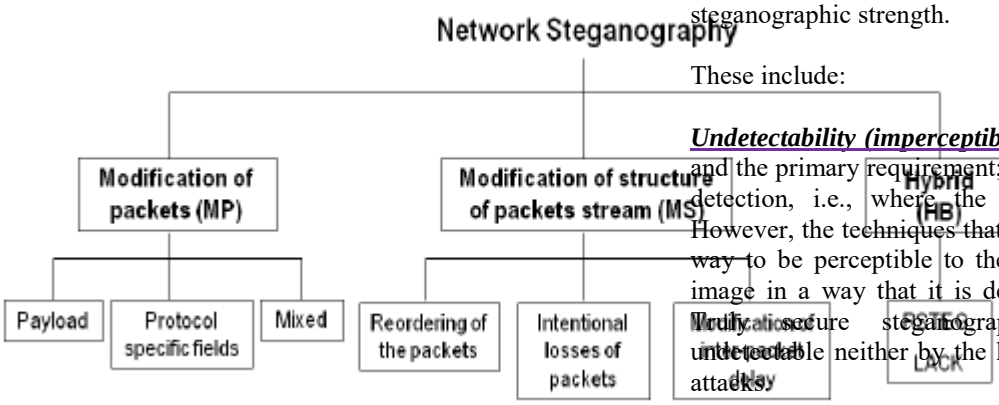

Figure 1: A network steganography classification

2.3.4.1. Existing methods of Network steganography

- SkyDe : Skype Hide
- StegTorrent: a Steganographic Method for the P2P File Sharing Service
- TranSteg: Transcoding Steganography
- Rsteg: Retransmission Steganography
- WiPad: Wireless Padding
- PadSteg: Introducing Inter-Protocol Steganography
- HICCUPS ((Hidden Communication System for Corrupted Network)
- LACK (Lost Audio Packets Steganography)
- SCTP Steganography: Multistreaming-based method
- StegSuggest

Performance Measure:

Every network steganographic methods has the following set of characteristics –

- Steganographic Bandwidth: The term "steganographic bandwidth" refers to the amount of secret data that can be sent per unit time when using a particular method
- Un-detectability: Un-detectability is defined as the inability to detect a steganogram within a certain carrier. The most popular method to detect a steganogram is to analyze the statistical properties of the captured data and compare them with values typical for that carrier.
- Robustness: Robustness is defined as the amount of alteration that a steganogram can withstand without its secret data being destroyed. A good steganographic method should be as robust and as difficult to detect as possible whilst offering the highest bandwidth.

Additionally, it is also useful to measure the steganographic cost. This is a characteristic that belongs to the sphere of carrier fidelity and has a direct impact on un detectability. It describes the degradation or distortion of the carrier caused by the application of the steganographic method.

2.4 Evaluation of different techniques

Though steganography's most obvious goal is to hide data, there are several other related goals used to judge a method's steganographic strength.

These include:

Undetectability (imperceptibility): This parameter is the first and the primary requirement; it represents the ability to avoid detection, i.e., where the human eye fail to notice it. However, the techniques that do not alter the image in such a way to be perceptible to the human eye may still alter the image in a way that it is detectable by the statistical tests. Truly secure steganographic techniques should be undetectable neither by the human eye nor by the statistical attacks.

Robustness: It is the second parameter that measures the ability of the steganographic technique to survive the attempts of removing the hidden information. Such attempts include, image manipulation (like cropping or rotating), data compression, and image filtering. Watermarks are an example of a robust steganographic technique

DOI: 10.21275/SUB151127

Payload capacity It is the third parameter that represents the maximum amount of information that can be hidden and retrieved successfully. When compared with watermarking, that requires embedding only a small amount of copyright information, steganography is seen to hide communication and consequently a sufficient embedding capacity is required. Accordingly and by using this parameter, small amounts of data could be hidden without being detected by the human eye. Larger amounts of information, on the other hand, may detect artifacts by the HVS or statistical tests.

3. My Work

After extensive study of theory of steganography, I started to implement some methods with slight modifications to get better performance and clear idea about such method. I have tried to use image and audio as cover media. All those programs are developed in MATLAB v.

3.1 LSB Modification and Phase Encoding Technique of Audio Steganography Revisited

I implemented LSB modification technique for an audio object. Here the cover object is a .wav file and the message is a text message. I also extract secret message from the stego object successfully.

Another well known method of steganography is phase encoding. I implemented this method for an audio object. Here the cover object is a .wav file and the message is a text message. I also extract secret message from the stego object successfully.

3.2 Multi-Level Steganographic Algorithm for Audio Steganography using LSB Modification and Parity Encoding Technique

I reviewed different methods of steganography and found another popular method of this domain is parity encoding. So I established a theory where two secret messages rather than one can be transmitted with a single cover file. Layering approach gives opportunity to do so. I implemented two-layered approach. At the first level, cover file (C) can be embedded with the first secret message S1.Assuming the stego file as C1 which is cover file for next level where secret message can be denoted as S2. Now the final stego file created as C12. So C12 holds both S1 and S2.Two levels of steganography can be identified as layer 1 and layer 2. At layer-1, LSB modification technique and at layer-2, parity encoding technique has been used [4].

3.3 A DWT Method for Image Steganography

I have explored the theory of Discreet Wavelet Transform (DWT) and applied to render a new method of image steganography. Here I used Haar Wavelet Transform to decompose the cover image into frequency components. Then I have generated pseudo-random number (Pn) and modified detailed coefficients like horizontal and vertical coefficients of wavelet decomposition by adding Pn when message bit = 0. After this step inverse DWT has done to generate the stego object. I also extract secret message from the stego object successfully by calculating mean correlation value between the coefficients of cover object and stego object.

3.4 A DCT Method for Image Steganography by Mid-Band frequency analysis

DCT allows an image to be broken up into different frequency bands namely the high, middle and low frequency bands thus making it easier to choose the band in which the secret message is to be inserted. The literature survey reveals that mostly the middle frequency bands are chosen because embedding the secret message in a middle frequency band does not scatter the secret information to most visual important parts of the image i.e. the low frequencies and also it do not overexpose them to removal through compression and noise attacks where high frequency components are targeted.

3.5 Steganography in edge detected image

Here I have proposed an edge based image steganography technique. Edges characterize boundaries and are therefore a problem of fundamental importance in image processing. Edges in images are areas with strong intensity contrasts – a jump in intensity from one pixel to the next. Edge detecting an image significantly reduces the amount of data and filters out useless information, while preserving the important structural properties in an image. Advantage of edge detection technique is editing in edge areas cannot be detected well by human eye, but editing in smooth areas can be detected easily. This property has been exploited to embed secret data in the edge area of an image by well-known lsb modification technique. [16-17]

There are many ways to perform edge detection. However, the majority of different methods may be grouped into two categories, gradient and Laplacian. The gradient method detects the edges by looking for the maximum and minimum in the first derivative of the image. The Laplacian method searches for zero crossings in the second derivative of the image to find edges.

3.6 BPCS analysis based Image Steganography

BPCS-Steganography is stands for Bit-Plane Complexity Segmentation Steganography. This steganographic technique uses an image as the vessel or cover data, and I have embedded secret information in the bit-planes of the vessel. This technique makes use of the characteristics of the human vision system whereby a human cannot perceive any shape information in a very complicated binary pattern. We can replace all of the “noise-like” regions in the bit-planes of the vessel image with secret data without deteriorating the image quality. Here I have divided the cover image of size 512x512

DOI: 10.21275/SUB151127

into 8 slices. Then I added message image at any one slice of cover image by lsb technique. The stego image reconstructed and analyzed.

4. Open Research Area

Although Steganography is in use literally for thousands of years but it's multitude of forms provide us opportunity to continuous research and improvement in this field. In audio steganography we can try to implement key based algorithms. In image steganography we can explore wavelet transform technique and discreet cosine technique to formalize suitable steganographic algorithm for color images. Video and Network Steganography techniques explored theoretically but not practically. Those are also open research area for me.

5. Conclusion

In this paper, I presented an overview of steganography starting with definitions and basic principles and proceeding through cover media types, specific techniques, cutting edge developments, and finally my own application of steganography in image and audio. There are many specific techniques for embedding data within these various mediums, and each has its own strengths and weaknesses. Some, such as LSB encoding, are considered especially weak, whereas transform domain and feature modification techniques may be slightly stronger. Other cutting edge developments are emerging to create new methods to both hide and uncover data, and even to completely rethink the way steganography is used.

References

[1] Bret Dunbar, SANS Institute InfoSec Reading Room "Steganography: Past, Present, Future".
[2] Cvejic, Nedeljko, Department of Electrical and Information Engineering "*Algorithms for audio watermarking and Steganography*"Information Processing Laboratory, University of Oulu, Finland 2004.
[3] Barnali, Gupta Banik, Prof. Samir Kumar, Bandyopadhyay," LSB Modification and Phase Encoding Technique of Audio Steganography Revisited",
[4] International Journal of Advanced Research in Computer and Communication Engineering, Vol. 1, Issue 4, June 2012."audio steg: methods", Internet publication on http://www.snotmonkey.com/work/school/405/methods.html
[5] L.M. Marvel, C.G. Boncelet Jr., C.T. Retter. (1999). "Spread spectrum image steganography." IEEE Trans. image processing. [On line]. 8(8), pp. 1075-1083. Available: http://www.mendeley.com/research/spread-spectrum-image-steganography-1/ [Apr., 2011].
[6] Lakshmi narayanan K, Prabakaran G, Bhavani R, Annamalai University, Annamalai Nagar, Tamil Nadu, India, "A High Capacity Video Steganography Based on Integer Wavelet Transform", Journal of Computer Applications ISSN: 0974 – 1925, Volume-5, Issue EICA2012-4, February 10, 2012
[7] Vipula Madhukar Wajgade , Dr. Suresh Kumar, SGT Institute of Technology And Management, Gurgaon, Haryana, India," Enhancing Data Security Using Video Steganography", International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 4, April 2013.
[8] W. Mazurczyk, M. Smolarczyk, K. Szczypiorski, RSTEG: Retransmission Steganography and Its Detection, In: Soft Computing in 2010, ISSN: 1432-7643 (print version) ISSN: 1433-7479 (electronic version), Journal no. 500 Springer
[9] L. Y. POR, B. Delina, Faculty of Computer Science and Information Technology, University of Malaya,MALAYSIA, "Information Hiding: A New Approach in Text Steganography", 7th WSEAS Int. Conf. on APPLIED COMPUTER & APPLIED COMPUTATIONAL SCIENCE (ACACOS '08), Hangzhou, China, April 6-8, 2008.
[10] A.M. Alattar and O.M. Alattar, "Watermarking electronic text documents containing justified paragraphs and irregular line spacing", Proceedings of SPIE -- Volume 5306, Security, Steganography, and Watermarking of Multimedia Contents VI, June 2004, pp. 685-695.
[11] 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 (ICDAR'03), 2003, pp. 775–779.
[12] K. Bennett, "Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding Information in Text", Purdue University, CERIAS Tech. Report 2004-13.
[13] M.H. Shirali-Shahreza and M. Shirali-Shahreza, "Text Steganography in Chat", Proceedings of the Third IEEE/IFIP International Conference in Central Asia on Internet the Next Generation of Mobile, Wireless and Optical Communications Networks (ICI 2007), Tashkent, Uzbekistan, September 26-28, 2007.
[14] 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
[15] Sneha Arora, Sanyam Anand, Lovely Professional University, Jalandhar, "A Proposed Method for Image Steganography Using Edge Detection", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 2, February 2013.
[16] Eiji Kawaguchi and Richard O. Eason, Kyushu Institute of Technology, Kitakyushu, Japan, "Principle and applications of BPCS-Steganography", http://www.datahide.com/BPCSe/QtechHV-program-e.html
[17] Kousik Dasgupta, J.K. Mandal and Paramartha Dutta, Department of CSE, Kalyani Govt. Engineering College,

DOI: 10.21275/SUB151127

Kalyani-741 235, India, "Hash Based Least Significant Bit Technique For Video Steganography(HLSB)", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 2, April 2012.

[18] Juan Jose Roque and Jesus Maria Minguet, SLSB: Improving the Steganographic Algorithm LSB, in the 7th International Workshop on Security in Information Systems (WOSIS 2009), Milan, Italy, pp.1-11, 2009.

DOI: 10.21275/SUB151127