iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VI **Month of publication:** June 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Complete Study on Steganography

Sheetal Deshpande[1], Shubham Mallayyanavarmath[2]
[1]Department of Computer Science & Engineering, Angadi Institute of Technology & Management,
[2]Department of Computer Science & Engineering, Angadi Institute of Technology & Management,

Abstract: ***Data hiding techniques have taken important role with the rapid growth of intensive transfer of multimedia content and secret communications. The method of steganography is used to share the data secretly and securely. It is the art of hiding the information and it serves as a better way of securing message than cryptography. In this paper we are highlighting the various study, types of steganography and the tools used in it. A lot of researches has done tremendous work in this art but there is lack of a single means to concrete all the information in single study. This paper aims to fulfill that dearth.***
Keywords: steganography,textsteganography,image steganography,audio steganography,video steganography.

I. INTRODUCTION

The word steganography when decomposed gives two greek words namely “STEGANOS” meaning “covered” and “GRAPHIE” means “writing”. The definition obtained from the literatures is very much matching the line- “steganography is the art and science of communicating in such a way that the presence of a message cannot be detected” which is very first given by cachin. In other words it is an art of writing hidden messages in such a way that no one apart from the intended recipient even knows that a message has been sent.The motivation behind this is firstly the protection of digital media and secondly the privacy of information transmitted across the world wide web.

The main goal of the steganography is to make the transmitted information invisible by embedding the information in cover media and to enhance the security and the robustness of the information against attacks.

One of the first documents describing steganography is from the Histories of Herodotus. In ancient Greece, text was written on wax covered tablets. In one story Demeratus wanted to notify Sparta that xerxes intended to invade Greece. To avoid capture, he scraped the wax off of the tablets and wrote a message on the underlying wood. He then covered the tablets with wax again. The tablets appeared to be blank and unused so they passed inspection by sentries without question. Another ingenious method was to shave the head of a messenger and tattoo a message or image on the messengers head. After allowing his hair to grow, the message would be undetected until the head was shaved again. Another common form of invisible writing is through the use of invisible inks. Such inks were used with much success as recently as WWII.

There exist two types of materials in steganography one is message which is the secret data that should be hidden from the outsiders and the other is carrier which is the material that carries message in it.

A. Types of steganography

1) Tex
2) Image
3) Audio
4) Video

II. ANALYZATION OF TECHNIQUES

A. Text steganography

The text steganography is a method of using written natural language to conceal a secret message. It can be achieved by altering the text formatting, or by altering certain characteristics of textual elements. The objective of designing coding methods was to develop alterations that are largely indiscernible to the reader and reliably decodable even in the presence of noise. General technique in text steganography is to use number of tabs, white spaces, capital, letters, just like Morse code and etc to achieve information hiding. The few coding techniques listed below can be used either jointly or separately. Each technique holds certain advantages or applicability of its own.

1) Line-Shift Coding: In this method, the lines of the text are vertically shifted to some degree(for example, each line is shifted

1/300 inch up or down) and information are hidden by creating a unique shape of text. This method is suitable for printed texts.

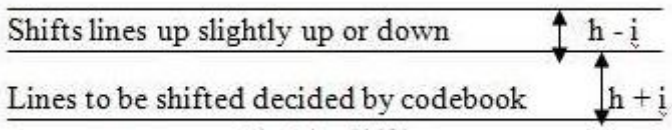


Fig: Line Shifting

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. This method hides information by shifting the text lines to some degree to represent binary bits of secret information.

a) Advantage: This method is suitable for printed text.
b) Disadvantage: When OCR(character recognition program) is applied, the hidden information gets destroyed.

2) Word-Shift Coding: In this method, by shifting words horizontally and by changing distance between words, information is 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.

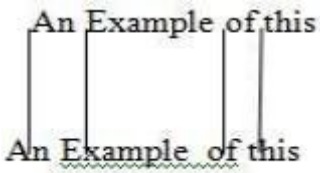


Fig: Word Shifting

But if somebody is aware of algorithm of distances, they 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. Retyping of text or using OCR programs destroys the hidden information.

a) Advantage: This method identify less because of change of distance between words to fill line is quite common.
*b) Disadvantage :*The algorithm that related to word shifted distance easily can get hidden data.

3) Feature Coding: In feature coding method, some of the features of the text are altered. For example, the end part of some characters such as h, d, b or so on are elongated and shortened a little thereby hiding information in the text. In this method, a large volume of information can be hidden in the text without making the reader aware of the existence of such information in the text.

a) Image steganography: Images are used as the popular cover medium for steganography. Hiding information in image is known as image steganography. Generally, in this technique pixel intensities are used to hide the information. The cover image can be called as Vessel or Container. The image after hiding information is called stego-image. A message is embedded in a digital image using an embedding algorithm, using the secret key. The resulting stego-image is send to the receiver. On the other side, it is processed by the extraction algorithm using the same key. During the transmission of stego-image unauthenticated persons can only notice the transmission of an image but can't predict the presence of the hidden message. To hide a message inside an image without changing its visible properties, the cover source can be altered in noisy areas with many color variations, so less attention will be drawn to the modifications. The most common methods to achieve these modifications involve the usage of the leastsignificant bit or LSB, masking, filtering and transformations on the cover image. These techniques can be used on different types of image files with varying degrees of success. Image steganography techniques can be divided into following domains.

b) Spatial Domain Methods

i) Transform Domain Technique

ii) Distortion Techniques
iii) Masking and Filtering

4) *Spatial Domain Methods:* There are many versions of spatial steganography, all directly change some bits in the image pixel values in hiding data. Least significant bit(LSB)-based steganography is one of the simplest techniques that hides a secret message in the LSBs of pixel values without introducing many perceptible distortions. Changes in the value of the LSB are imperceptible for human eyes.

a) *General advantages of spatial domain LSB technique are :*

i) There is less chance for degradation of the original image.
ii) More information can be stored in an image.

b) *Disadvantages of LSB technique are :*

i) Less robust, the hidden data can be lost with image manipulation.
ii) Hidden data can be easily destroyed by simple attacks.

5) *Transform Domain Technique:* This is a more complex way of hiding information in an image. Various algorithms and transformations are used on the image to hide information in it. Transform domain embedding can be termed 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. Most of the strong steganographic systems today operate with the transform domain. Transform domain techniques have an advantage over spatial domain techniques as they hide information in areas of the image that are less exposed to compression, cropping, and image processing.

6) *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 used to match the secret message required to transmit. The message is encoded at pseudo-randomly chosen pixels. If the stego-image is different from the cover image at the given message pixel, the message bit is a "1". Otherwise, the message bit is a "0".

7) *Masking and Filtering:* These techniques hide information by marking an image, in the same way as to paper watermarks. These techniques embed the information in the more significant areas than just hiding into the noise level. The hidden message is more integral to the cover image. Watermarking techniques can be applied without the fear of image destruction due to lossy compression as they are more integrated into the image.

a) *Advantages of Masking and filtering Techniques*

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.

c) *Disadvantades of Masking and filtering Techniques*

Techniques can be applied only to gray scale images and restricted to 24 bits.

B. Audio Steganography

In audio steganography, secret message is embedded into digitized audio signal as noise at a frequency out of human hearing range. The embedding process will result a slight alteration of binary sequence of the corresponding audio file but the alterations made to the audio file are perceptually indiscernible. The characteristics of audio signal such as unpredictable nature and characteristic redundancy make them ideal candidate to be used as a cover for covert communications to conceal secret messages. The audio steganographic process mainly consists of following two steps:

1) *Identification of redundant bits in the audio file:* Redundant bits are those bits that can be modulated without destroying the integrity or corrupting the quality of the cover media. Hence those redundant bits are chosen as the candidate for holding secret

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

information.

2) *Embedding the secret information in the audio file:* The redundant bits in the cover file is replaced by the bits of the secret information. Due to the existence of advanced audio steganography schemes and the very nature of audio signals to be highcapacity data streams, audio steganalysis is very difficult and requires scientifically challenging statistical analysis. There have been many techniques for hiding information or messages in audio. Some of the common approaches include

C. Low-Bit Encoding

It is also known as LSB encoding. The low-bit encoding replaces the least significant bit in some bytes of the digitized audio file to hide a sequence of bytes containing the secret data. Since the LSB substitution doesn't cause significant quality degradation, such as in 24-bit bitmaps, this is usually an effective technique. In computing, the least significant bit (LSB) is the bit position in a binary integer giving the units value, that is determining whether the number is even or odd. The LSB is sometimes referred to as the right-most bit, due to the convention in positional notation of writing less significant digit further to the right. Though this method is simple and have greater embedding capacity, the method cannot provide protection to the hidden message against small modifications that can arise as a result of format coversion or lossy compression.

D. Phase Coding

In phase coding technique, the phase of a cover audio segment is replaced with replaced with a reference phase that represents the secret information. In order to preserve the relative phase between segments, the remaining segments phase is adjusted. In terms of signal to noise ratio, Phase coding is one of the most effective coding methods. This method relies on the fact that the phase components of sound are not as perceptible to the human ear as noise is. Message bits are encoded as phase shifts in the phase spectrum of a digital signal. This leads to inaudible encoding in terms of the Signal-to-Perceived Noise Ratio (SPNR) and the secret message gets camouflaged in the audio signal, not detectable by the steganalysis methods based on SPNR. Thus, phase coding addresses the disadvantages of the noise-inducing methods of audio steganography. When there is a drastic change in the phase relation between each frequency component, noticeable phase dispersion will occur. However, as long as the modification of the phase is sufficiently small, an inaudible coding can be achieved.

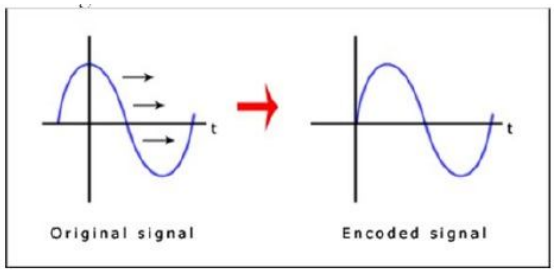


Figure 1: Phase Coding

1) *Disadvantages of Phase coding is:* Low data transmission rate owing to the fact that the secret message is encoded only in the first segment of audio signal.

E. Spread Spectrum Coding

In audio steganography, the basic spread spectrum method attempts to randomly spread bits of the secret message across the frequency spectrum of the audio signal. This is similar to a system which uses an implementation of the LSB that spreads the message bits randomly over the entire sound file. However, unlike LSB coding, the spread spectrum method spreads the secret information over the frequency spectrum of the sound file using a code which is independent of the actual signal. As a result, the final signal occupies a bandwidth which is more than what is actually required for transmission. The spectrum method is capable of contributing a better performance than LSB coding and phase coding techniques by virtue of a moderate data transmission rate coupled with a high level of robustness against steganalysis techniques.

1) *Disadvantages of Spread Spectrum coding is:* It introduces noise into a sound file like LSB coding method. This vulnerability can be tapped for steganalysis.

F. Echo Hiding

Echo hiding technique embeds secret information by introducing an echo into the discrete audio signal. To successfully hide the secret message, three parameters of the echo need to be altered. They are, amplitude, decay rate and offset or delay time from the original signal. As all the three parameters are set below the human audible threshold limit, the echo cannot be easily resolved. Also, the offset is altered to represent the binary message to be hidden. The first offset value represents a binary one, and the second offset value represents a binary zero. If only one echo was produced from the original signal, only one bit of secret information could be encoded. Hence, before the encoding process begins the original signal is broken down into blocks. Once the encoding process is done, all blocks are concatenated back together to create the final signal.

1) Advantages of Echo Hiding are:
2) High data transmission rate.
3) Superior robustness.

G. Video Steganography

As a video container file has numerous advantages not exhibited by other container formats, video steganography is now a growing area of research. Video Steganography is a technique to hide any kind of files into a video file. The Alteration in the video file is significantly more difficult to detect by the human visual system, as frames are displayed on screen in an extremely faster rate. Furthermore, since video frames are not sharply focused images or crisp, variations in pixel color induced by steganography will blend into the frame very easily. Use of the video based steganography can be more eligible than other multimedia files, because of its size and memory requirements.

The video has 2 components:

1) Audio Stream.
2) Picture Stream.

The techniques used in video steganography are:

H. LSB (Least Significant Bit) method

LSB is said to be the best method for data protection because of its simplicity and commonly used approach. It is the most easiest and effective way of embedding data. In LSB, the cover video's pixel values are extracted which are in bytes, then its LSB are substituted by the bits of the secret message that we will embed. Now since we change only the LSB bits of the host video, it doesn't gets distorted and almost looks alike as the original video.

I. Non-uniform rectangular partition

This method is for uncompressed videos. In non-uniform rectangular partition, data hiding is done by hiding an uncompressed secret video file in the host video stream. But we have to make sure that both the secret as well as the cover file should be of almost the same size. Each of the frames of both the secret as well as cover videos is applied with image steganography with some technique. The secret video file will be hidden in the leftmost four least significant bits of the frames of the host video.

J. Compressed video steganography

This method is done entirely on the compressed domain. Data can be embedded in the block of I frame with maximum scene change and in P and B block with maximum magnitude of motion vectors. The AVC encoding technique yields the maximum compressing efficiency.

K. Anti-forensics technique

Anti-forensic techniques are actions taken to destroy, hide and/or manipulate the data to attack the computer forensics. Anti-forensic provides security by preventing unauthorized access, but can also be used for criminal use also. Steganography is a kind of anti-forensic where we try to hide data under some host file. Steganography along with anti-forensics makes the system more secure.

L. Steganographic Applications

1) Steganographic technique can be used anytime to hide data. The most important reason to hide data is to prevent unauthorized persons from becoming aware of the existence of a message.

2) Steganography is employed in various useful applications such as copyright control of materials, enhancing robustness of image search engines and smart IDs where individual's details are embedded in their photographs.
3) Other applications are TV broadcasting, video-audio synchronization, TCP/IP packets and checksum embedding and safe circulation of secret data.
4) Steganography would provide an ultimate guarantee of authentication that no other security tool may ensure.
5) In the business world, data hiding can be used to hide a secret chemical formula or plans for a new invention.
6) Steganography can also be used in the non-commercial sector to hide information that someone wants to keep private.
7) It can be used in forensic applications for inserting hidden data into media files for the authentication of spoken words and other sounds, and in the music business for the monitoring of the songs over broadcast radio.
8) Steganography also have some contemporary applications, one of which is in Medical Imaging Systems where a seperation is considered necessary for confidentiality between patient's image data or DNA sequences and their captions.Eg: physician, patient's name and address. Thus, embedding the patient's information in the image could be a useful safety measure and helps in solving such problems.

III. ACKNOWLEDGEMENT

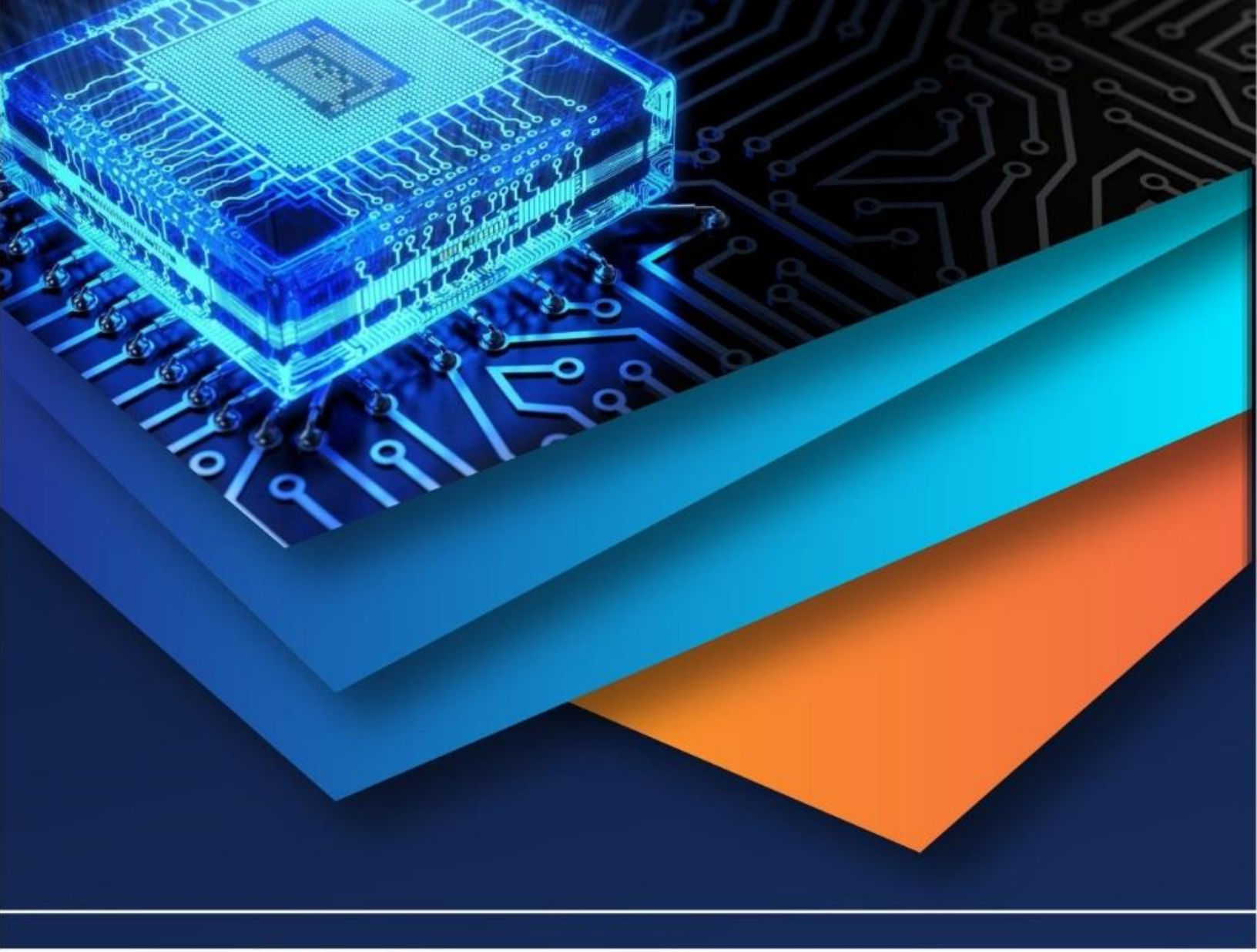
We would like to express our humble gratitude to our parents who have taken over the great task of educating and encouraging us in every phase to achieve our goal.

IV. CONCLUSION

This paper gave an overview of different steganographic techniques its major types and classification of steganography which have been proposed in the literature during last few years. Steganography plays an important role in embedding information into cover image viz., text, video, audio or multimedia content for military communication, authentication and many other purposes. It has gain more importance due to the exponential growth and secret communication of potential computer users over the internet. Steganography is the best technique to hide the data and transform it securely.

REFERENCES

[1] https://www.ijircce.com/upload/2015/october/55_A_study.pdf
[2] http://ijcem.in/wp-content/uploads/2014/08/A-comprehensive-study-of-steganography-A-method-of-hiding-information-in-other-information.pdf
[3] http://www.ijettjournal.org/volume-4/issue-7/IJETT-V4I7P186.pdf
[4] http://www.ijpttjournal.org/volume-3/issue-5/IJPTT-V3I5P103.pdf



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY