A Survey of Various Image and Audio Steganographic Techniques

Sapna Sharma[1] Hetal Dalal[2]
[1]P.G. Student [2]Assistant Professor
[1,2]Department of Electronics & Communication Engineering
[1,2]Hasmukh Goswami College of Engineering, Vahelal, Ahmedabad, Gujarat, India

Abstract— Now days sharing information over the internet has become a matter of major concern, as one has to share data over internet for various uses, which requires strong information protection techniques. Thus, cryptography is present is used for protecting data but a potential technique which provides enough security is required. Various data hiding techniques were present but steganography provides security lot more than other techniques. Steganography actually protects information by hiding information in the original messages. This paper presents a comparison between cryptography and steganography, also presents an overview of various image steganography techniques with their advantages and disadvantages which helps in data hiding.

Key words: Steganography, Cryptography, Spatial and Frequency Domain, Masking and Filtering

I. INTRODUCTION

There is a high need of secure communication over the internet because digital media is used by all for its various advantages. Therefore, security of transmitted data is needed. For this purpose, cryptography is used, which secure data over the network but still does not provide any guarantee of no leakage of data during transmission. So, steganography is the solution to above problem. Firstly, one must clear their concepts about cryptography and steganography. Both are different things with the same objective, where cryptography fails to achieve secure and leakage proof communication. The idea of hiding information is very ancient trick, has a long history. In ancient Greece, A message is to be write on the wood, then cover it with wax, to transfer information secretly. People also get their head shaved and get a message tattooed over there and cover it by new grown hair, share information using again shaved head.[2]. Invisible inks were also used in earlier ages, to hide a message. Pencil marks are also a form of steganography. Null ciphers (unencrypted messages) were also used.

II. CRYPTOGRAPHY

Cryptography is actually defined as the method of encrypting and decrypting the message in such a way that other user except sender and receiver no one is able to read the message. In short, cryptography makes the message unreadable for the third user. Cryptography process makes use of keys which helps in encryption and decryption of the message. Cryptography is all about protecting information over the network but does not ensure about its secure and safe transmission. Cryptography mixed up a message so it cannot be understood.[1]

III. STEGANOGRAPHY

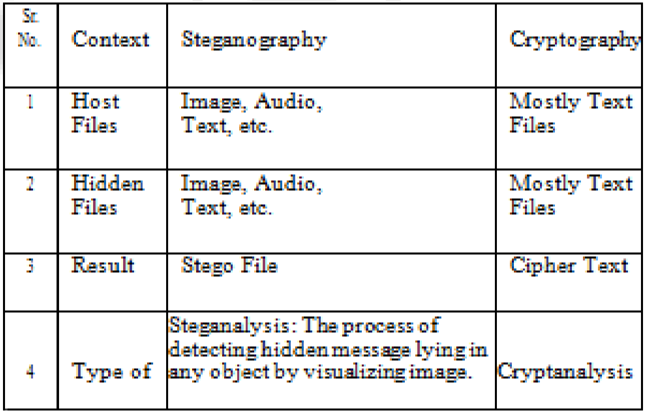
Steganography is actually a Greek word, combination of two words, steganos which means "hidden, covered or concealed" and graph in which means "writing".[2] Steganography is the way of secure transmission of message by hiding the secret message inside the original message in such a way that only the intended user knows about it. The original message is also called as cover media.

Cover media and secret message can be any kind of digital form like text, image, audio and video. Steganography is the art and science of invisible communication of messages.[2]

Cryptography mainly focuses on keeping the contents of a message secret whereas steganography focuses on keeping the existence of a message secret.[2]. There are also other techniques related to this are: watermarking and fingerprinting. In watermarking, all of instances of an object are marked so that object becomes patent of owner. The information hidden is actually a signature which shows that it is a copyright protection like patents. In fingerprinting, different and unique spots or marks are created in the carrier objects that are supplied to different customers.

This paper offers an overview regarding data hiding techniques, gave an overview of various steganographic techniques. Further section will give you a brief knowledge about image steganographic techniques used for data hiding purposes.

Below table helps you to understand the difference between both cryptography and steganography.



Sr. No.	Context	Steganography	Cryptography
1	Host Files	Image, Audio, Text, etc.	Mostly Text Files
2	Hidden Files	Image, Audio, Text, etc.	Mostly Text Files
3	Result	Stego File	Cipher Text
4	Type of	Steganalysis: The process of detecting hidden message lying in any object by visualizing image.	Cryptanalysis

Table 1: Comparison of Cryptography and Steganography

A few characteristics must be of care taken while creating any hiding algorithm. [1]

- Imperceptibility: means, extracting and detecting the secret message is either impossible or difficult by seeing or hearing a message. Therefore, high degree of imperceptibility is required for steganography. The goal is that before hiding and after hiding data, cover media should appear same as before. [1]
- Robustness: refers to the degree of difficulty required to tear down embedded information without destroying the cover object itself.
- Data embedding capacity: means the how long message can be added into any cover media [1].

The basic steganography process is shown here, which gives idea how secret message can be hidden behind any cover media.

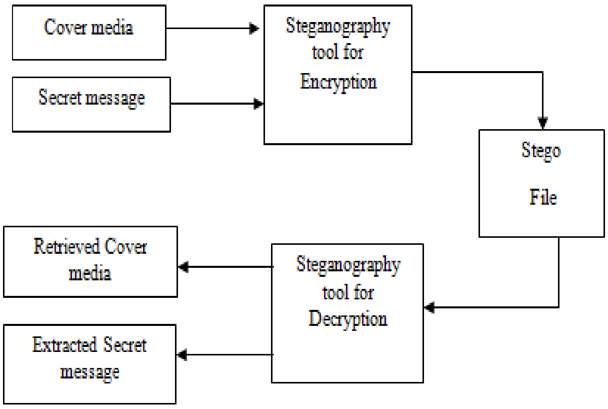


Fig. 1: Basic steganography model

Basically, steganography works on a simple principle. This principle says that to hide information, firstly choose cover media. Cover media can be any text, image, audio or video file format. Now choose secret message which one wants to hide. Now after that embed the secret message in the cover media using a steganography tool. This tool will generate a stego file. Stego file contain both cover image and secret data in it. On the receiver side, stego file will be extracted using steganography tool. Here, cover media and secret message both are extracted.

There are various types of steganography available on the basis of digital media, which are:

- Text steganography
- Image steganography
- Audio steganography
- Video steganography
- Protocol steganography

Here, in this paper Image steganography is the main point of discussion. As, image steganography is the very commonly used method of steganography.

IV. IMAGE STEGANOGRAPHY:

It allows hiding the secret message behind the cover image in a great way because image format provide a lot of redundant data and space for hiding a message. The message to be hide, is called secret message and image on which secret message is to be hide is called, cover image. Cover image physically looks same before and after implementing Steganography on it.

Various techniques are used for steganography on image, which are:

- SPATIAL DOMAIN
- TRANSFORM DOMAIN
- DISTORTION DOMAIN
- MASKING AND FILTERING

A. *Spatial Domain Method:*

This is the very commonly used technique. Here, firstly the cover image is splitted into bit planes and then LSBs of the bits planes are supersede with the new secret message.[7] There are many ways of spatial steganography, all techniques just change some bits in the image pixel values to hide 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 perceptible distortions. To our human eye, changes in the value of the LSB are imperceptible. Embedding of message bits can be done either simply or randomly. Least Significant Bit (LSB) replacement technique, Matrix embedding are some of the spatial domain techniques.

1) Least significant bit (LSB)
2) Pixel value differencing (PVD)
3) Edges based data embedding method (EBE)
4) Random pixel embedding method (RPE)
5) Texture based method
6) Histogram shifting methods and some more.

1) *Advantages:*

1) High data embedding capacity.[7]
2) Degradation of the original image is not easy.
3) Is harder to detect than other steganography techniques

2) *Disadvantage:*

1) Robustness is low.

B. *Transform Domain Technique:*

In Frequency domain technique, firstly the cover image is transformed into frequency domain then the secret message is inserted into transformed coefficients of image giving more robustness against attacks.[7] Transform domain embedding can be termed as a domain of embedding techniques for which a number of algorithms have been suggested . Most of the strong steganography systems today operate within the transform domain. Transform domain techniques have an advantage over LSB techniques as they hide information in areas of the image that are less exposed to compression, cropping, and image processing [7] Transform domain techniques are of different types:

- Discrete Fourier transformation technique (DFT).
- Discrete cosine transformation technique (DCT).
- Discrete Wavelet transformation technique (DWT)

C. *Distortion Technique:*

This technique actually measures the difference between original cover image and the distorted cover image. This is done so that secret message can be detected from the differences of above two images. The encoder adds a sequence of changes to the cover image. So, information is described as being stored by signal distortion [2].Using this technique, a stego object is created by applying a sequence of modifications to the cover image. This sequence of modifications is use to match the secret message required to transmit [3].

D. *Masking and Filtering:*

This technique actually masks the secret message on original information of cover media by varying the luminance of particular areas. [1]

It embeds information in the significant areas of cover media in such a way that it only does not hide noise levels. This technique does not destruct the image as no such major occurs in the original cover image.

1) *Advantage:*

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.

2) Disadvantage:

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

V. AUDIO STEGANOGRAPHY

When a carrier file is used as audio file and a secret message is hide behind it, is called audio steganography. Hiding text with the help of audio file is a tough task than image steganography, but provides a lot of redundant space to hide data.

A. LSB Coding:

In LSB coding technique least significant bit is modified to embed data. [10] LSB algorithm replaces the LSB with some bytes of cover file so that a group of bytes can be hide which contains hidden data [9]

B. PHASE Coding:

In Phase coding, the phase of carrier file is replaced with reference phase which represents hidden data [10] .this method works by substituting the phase of an initial audio segment with a reference phase that represents the data. The phase of subsequent segments is then adjusted in order to preserve the relative phase between segments” [9] As it is known that phase components of audio signal is not perceptible to human ears.

C. PARITY Coding:

In this method, a signal is divided into various individual samples and then parity bit of each sample is calculated and matched with secret message bit [10]

D. Spread Spectrum Technique:

In spread spectrum method secret information is spread over the audio signal's frequency spectrum as much as possible [10]

VI. LITERATURE SURVEY

X. Zhang proposed a scheme in which uncompressed image has been encrypted by main content owner using an encryption key and data hider compresses LSBs of encrypted image. When hacker only has data hiding key, he can extract additional Data and if hacker has both encryption and data hiding key he can extract additional information and recover the original image. [3]

A novel reversible data hiding scheme has been proposed for encrypted image in which data has been hide using stream cipher. Then, secret data can be added into image after modifying a little bit of encrypted data. Receiver can decrypt data using data hiding key and spatial correlation in image and recover original image perfectly. [4]

Jing-Ming Guo, and Thanh-Nam Le [5] Proposed a new scheme in which color (RGB) image is converted into YCbCR color model (luminance) and then sub-sampling is done is done in which Cb and Cr channels are sub-sampled with the rate equal to half of the rate of the Y channel. Then each channel is being partitioned into non- overlapping 8*8 blocks. In next step Discrete Cosine transformation is applied which separates low and high frequency components. This proposed scheme does not only enhances the security but also safe to use under steganalysis schemes. [5]

Here, a novel method, reserving room before encryption with reversible data hiding has been proposed in which firstly content owner reserves large space on the cover image and then encrypts it, and then secret data is embedded. This approach has advantage that it provides better performance if compared with other techniques. Also this scheme allows recovering original image and extracting data. This method can embed more than 10 times as large payloads for the same image quality as the previous methods. [6]

K Agham, Tareek M Pattewar proposed a scheme for reversible data hiding using RGB-LSB, in which RGB image has been used instead of grey scale image for encryption. The method of data hiding, encryption and decryption is same as proposed in [6]. This method allows hiding more information in cover image because here the cover image is taken as colored image. Therefore, net payload size has been increased. [7]

Zhenxing Qian, Xinpeng Zhang, and Shuozhong Wang, proposed reversible data hiding for encrypted JPEG bit stream. Earlier the bit stream of JPEG image is encrypted with the already preserved structure of bits. Then secret message is embedded into it. On the receiver side, it can decrypt message and retrieve original image. The plain data bits are encoded with the help of error correction codes so that data extraction and original image can be retrieved. Here, an Low density parity check codes are taken as an example.[8]

The author [11] has used Direct Sequence Spread Spectrum for hiding secret message on an audio file. Here, A key is used so that secret message can be embed into noise signal, further this key is used to generate pseudo-noise wave signal. The information to be embedded must first modulated using the pseudo-noise. [11]

The author [10] has Proposed a scheme in which the audio signal is divided into individual samples and embed the secret message into phase spectrum of first block. At the output side, stego file is audible and correct. There is no suspection of a secret message addition in it with compared to input carrier file. The disadvantage of this method is that it can be used only for hiding a short secret message in an audio file.

VII. CONCLUSION

This paper gave a comparison between cryptography and steganography to understand the basic difference between both techniques. Also this paper gave an overview of different techniques and categories available for image and audio steganography. After the reference of this paper, one can decide which technique you want to prefer for designing a better digital steganography algorithm. Many methods and techniques have been developed year by year according to the requirements, therefore, all techniques are based on different parameters like- robustness, embedding capacity, enhancing accuracy, Undetectability etc. Steganography ensures the secret message to be hidden behind any cover media, and provides less chances of detection. Image as cover media is more preferred over text because text format does not allow embedding more data in it because of less redundant space availability. Therefore, Steganography is all about secure and safe transmission.

References

[1] Rucha Bahirat ,Amit Kolhe , "Overview of secure data transmission using Steganography" International Journal of Emerging Technology and Advanced Engineering, Volume 4, Issue 3, March 2014

[2] Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav, " Steganography Using Least Signicant Bit Algorithm" International Journal of Engineering Research and Applications (IJERA) Vol. 2, Issue 3, pp. 338-341, May-Jun 2012

[3] X. Zhang, "Separable Reversible data hiding in encrypted image," IEEE Trans. Inform. Forensics Security, vol. 7, no. 2, pp. 826–832, April 2012

[4] X. Zhang, "Reversible data hiding in encrypted image," IEEE Signal Process. Letters, vol. 18, no. 4, pp. 255–258, April 2011

[5] Jing-Ming Guo, Member, IEEE, and Thanh-Nam Le, "Secret Communication using JPEG Double compression" IEEE signal processing letters, VOL. 17, NO. 10, October 2010

[6] Kede Ma, Weiming Zhang, Xianfeng Zhao, Member, IEEE, Nenghai Yu, and Fenghua Li, "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption" IEEE transactions on information forensics and security, VOL. 8, NO. 3, March 2013

[7] Vinit K Agham, Tareek M Pattewar, "Separable reversible data hiding technique based on RGB-LSB method" International Journal of Research in Advent Technology (IJRAT) Vol. 1, No. 3, ISSN: 2321–9637, October 2013

[8] Zhenxing Qian, Xinpeng Zhang, and Shuozhong Wang, "Reversible Data Hiding in Encrypted JPEG Bitstream", IEEE transactions on multimedia, VOL. 16, NO. 5, August 2014

[9] Jayaram P, Ranganatha H R, Anupama H S"Information Hiding Using Audio Steganography – A Survey" The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011

[10] Prof. Samir Kumar, BandyopadhyayBarnali, Gupta Banik "LSB Modification and Phase Encoding Technique of Audio Steganography Revisited" International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 4, June 2012

[11] Rupanshi, Preeti, Vandana "Audio Steganography by Direct Sequence Spread Spectrum" International Journal of Computer Trends and Technology (IJCTT) – volume 13 number 2 – Jul 2014.