International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 10 Issue: 02 | Feb 2023 www.irjet.net p-ISSN: 2395-0072

STEGANOGRAPHY: COMPLETE OVERVIEW OF RELEVANT TECHNIQUES AND METHODS

S M Ali Zaidi[1], Piyush Kumar Gupta[2]

[1]Department of Computer Science and Engineering, Jamia Hamdard, New Delhi, India
[2]Assistant Professor, department of Computer Science and Engineering, Jamia Hamdard, New Delhi, India

---

Abstract - *With the exponential rise of digital multimedia content, the data hiding techniques came into popular demands in order to securely transmit information around. This review paper focusses on one such technique of data hiding i.e., steganography. It is the art and science of embedding secret messages in a normal message in a way that anyone without knowledge of hidden message cannot suspect the presence of the message, except sender and receiver. Proper analysis has been done and the data collection for review were taken from several research databases namely, Springer, ScienceDirect, Google Scholar and IEEE Explorer to increase the scope of objectivity of this paper.*

Key Words: Steganography, Cryptography, Image, Audio and Video Steganography, Steganalysis, Data Hiding, Embedding, LSB.

1. INTRODUCTION

Steganography, the word itself is derived from the Greek words 'stegos' and 'grafia' which means cover and writing respectively, thus making it covered writing or hidden writing [1]. It is the practice of concealing a file, a message, image or audio/video in another file in order to safeguard and protect the information being hidden. The concealed message is present in the file in a way such that it cannot be recovered without the help of sender/receiver who knows how to extract the hidden message. images, audio, video, and texts can be represented as digital data . However, new issues also arose and have been explored(Art. 2001;Zhao et al., 1998), such as data security in digital communications, copyright protection of digitized properties, invisible communication via digital media, etc. Stega-image is the name of the cover document that contains the hidden message. Steganography and steganalysis are terms used to describe this technique and its vice-versa respectively. This system is depicted in Figure 1 as hiding data or messages in the cover medium at the sender or source end and retrieving the concealed data from the steganographic document at the receiver end. Steganography can be used in four different ways:

1.Using text

2.Image Steganography

3.Audio Steganography

4.Video Steganography

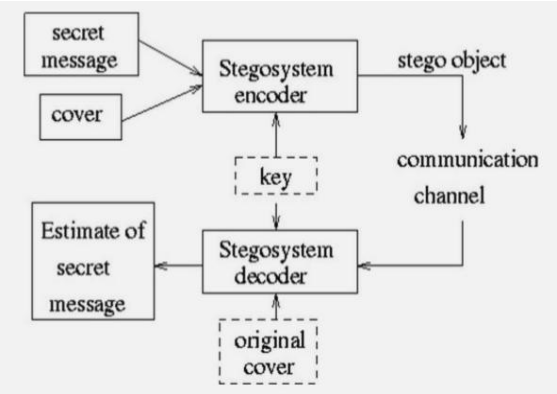
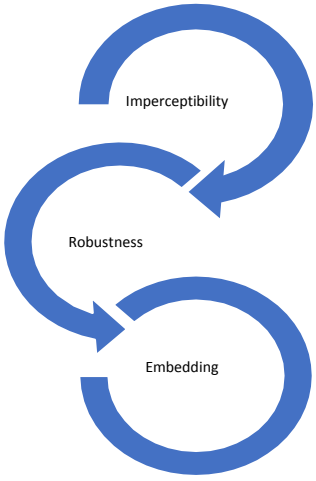


Fig.1 Simple Steganographic Model

While cryptography focuses on keeping the contents of a communication secret using various encryption techniques, steganography focuses on keeping the existence of a message hidden [4], as we shall describe later. Steganography and cryptography are two methods for keeping information safe from unapproved access, but neither is flawless and may be intercepted [4]



Imperceptibility, Robustness and Embedding Techniques are the three very important factor for any successful steganographic systems.

•The safety of steganography technologies that hide the secret message in the embedded video is directly connected to imperceptibility. Because of the great

imperceptibility, the embedded video has a low modification rate and good visual quality.

•The second prerequisite, robustness, assesses the steganography method's resistance to assaults in steganography. The need of resilience is due to the fact that the embedded message might be damaged by a variety of purposeful and inadvertent assaults, such as network transmission, packet loss, video cutting, and scaling processes.

•The third prerequisite need is embedding capacity, which is defined as the total number of hidden messages that may be inserted into a digital movie. The more hidden messages that can be inserted, the better the embedding capacity.

2. HISTORICAL BACKGROUND

Throughout the history, there are many instances when different techniques were used to hide a secret message and one of the most popular of such cases is that of Histiaeus, a Greek ruler who used the steganography technique by shaving the head of one of his slaves and writing the secret message on it and had waited for the hairs to regrow so that he can send the concealed data.

3. RELATED WORKS

With extensive research works and study in the field, hereby is a list of some important researches mentioning the name of their authors, topic of study, advantages and limitations to give a brief explanation of trends that follows in the previous research works and the topics of special significance that allows to explore and understand more about this ever popular way of concealing important messages.

Citations	le of the paper	Methodology	Advantages	Disadvantages	Evaluation
[12]	An overview of Image Steganography	Different steganographic techniques and spatial and transform domain methods, steganalysis prevention and detection,	Proposed techniques to keep in check image steganography methods according to Imperceptibiliy rules Security of LSB steganographic technique is slightly improved.	Robustness against statistical attacks and image manipulation needs to be in check. More sensitivity for steganalysis tools and providing unsuspicious files	The paper gave a brief overview of how image steganography can change the whole hidden communication scenario and proposed several techniques with their rules to follow.
[13]	Video Steganography :A review	The review methodology of this work contains data hiding ,visual quality, methods and techniques, embedding and capacity	Briefly defines the techniques used in the concealment of data in a video. Other methods and their importance in the field were introduced	N/A	The first task is to develop a video steganography system that achieves a fair trade-off between visual quality, embedding capacity, and resilience against a variety of unanticipated assaults.
[14]	Digital audio steganography: Systematic review, classification, and analysis of the current state of the art	Data gathering, technique analysis, major behaviour construction, and similarity- based categorization are all part of the review approach for this project.	Usefulness and importance of different techniques and their harms were briefly explained and highlighted through various research journals.	A comparison of the performance of the studied approaches, The discrepancy in assessment methodologies and embedding environments in the evaluated approaches allows for this comparison.	Understanding with statistical data of previous papers and present findings is beneficial and important.
[2]	)ata Security by Steganography	Securing data and information through different steganographic methods.	LSB algorithms in variations were proposed which optimized the quality of stego-image through bit invert techniqueImplementation of steganography, and future applications were explored.	No importance were given to other steganographic methods such as video audio, or text and only image steganography was explored.	Steganography is very useful in the field of data security and protection if correctly implemented. Secret information may be utilised to validate vital business transactions and user authentication via steganography.

4. CRYPTOGRAPHY, STEGANOGRAPHY AND STEGANALYSIS

4.1 Cryptography and Steganography

Cryptography is also the method or techniques of hiding messages, but unlike Steganography the messages are hidden using a set of complex codes that can only be decoded by the the one for whom the crypted data was made for. A special key is used for the decoding or deciphering of the code and it can be passed through one on one communication between sender and receiver[6][7].One camouflages a message in a file/image/video or audio whereas other uses encoding methods to conceal it[8].

4.2 Steganography and Steganalysis

While cryptography and steganography were very much similar to each other, on the other hand steganalysis is the compliment of steganography. In simpler words if we look into it from an opponent's point of view, Steganalysis[9] is the practice of preventing stealthy and concealed communications, which is the main role of steganography to provide with messages stealthily. Its primary goal is to check whether a secret is hidden in a message or package, or not and identifying the secret message induced files.

5. CATEGORIES AND CLASSIFICATION

Digital files or data, such as picture, video, text, music, network protocol, and DNA, are commonly used as communication mediums/carriers. Secret information is embedded in many digital mediums using their unique qualities. Text steganography, for example, employs line/word shifting encoding [8], and emoticons were recently used in textual chat to accomplish hidden Communication. For incorporating hidden information in audio steganography, phase coding, spread spectrum, and low-bit encoding are commonly used.

Hidden message can also be placed in packet payloads, packet headers inside another medium, and even retransmission steganography, which uses the behaviour of acknowledgement and retransmission of packets. The features of randomness in DNA may be used to incorporate the hidden data in DNA-based steganography, i.e., A approach that uses a numerical mapping table to map the DNA sequence for encoding secret data was recently published. Image and audio steganography are frequently combined in video steganography.

Among all the other steganographic methods the, most widely and popularly used technique is image steganography since images are the one that are most broadly used on the internet.

5.1 IMAGE STEGNOGRAPHY

An Image Steganographic method is generally assessed by the following major goals: Firstly, what is the maximum embedding payload that can be achieved? Secondly, how similar is the stego-image to its cover picture in terms of visual image quality? Thirdly, in terms of security, how can a stego-image withstand various steganalysis recognition attacks? As a result, the optimal steganographic approach must concurrently achieve the above goals of strong ability, acceptable visual picture quality, and undetectability. However, high-payload steganographic techniques frequently create distortion errors in stego-images, making them sensitive to steganalysis.

To create hidden data embedding, several ways have been developed, the majority of which involve a unique methodology. They may be further classified into numerous categories depending on their implementation if we classify them according to model / approach based techniques. We put them into several groups despite the fact that it is hard to classify them all exactly. We usually divide them according to their embedding domain which are of two types, Spatial Domain and Transform Domain.

5.1(A) SPATIAL DOMAIN

Also known as image domain, it embeds a message in the intensity of the image pixels directly, Bit-wise approaches that employ bit insertion and noise modification are referred to as "simple systems" in image domain techniques. Lossless image formats are best for image domain steganography, and the approaches are usually determined by the picture format. Following are the most often utilised spatial domain techniques:

1) Least Significant Bit, popularly known as LSB.

2) Pixel Value Difference, or PVD.

3) Exploiting Modification Direction (EMD) based methods.

4) Edge based Methods

LEAST SIGNIFICANT BIT(LSB)

Least significant bit (LSB) Steganography is a basic and well-known method for concealing bigger amounts of secret information in a cover image with little visual alterations. It operates by substituting secret message bits for the LSBs of (randomly chosen) selected pixels in the cover picture. A stego- key can determine the order of embedding or the selection of pixels.

It is a general, and easier approach for embedding information in a The Least Significant Bit (LSB) is a straightforward steganography approach. It embeds the data into the cover, like all steganographic techniques, so

that it cannot be noticed by a casual viewer[10]. The approach replaces some of the information in a pixel with data from the picture. Normally, the most-right bits of a cover file's bytes are replaced by an LSB algorithm. If a portion of the cover picture C(i,j) is missing, C(i, j) is unaltered if the bit of SM or the secret message to be embedded is equal to it, else C(i, j) is set to a bit of SM which is also known as secret message. Secret Message (SM). The letter 'C,' for example, has an ASCII code of 67 in decimal, which corresponds to 01000011 in binary and before concealing (embedding) a hidden message, bits of the picture pixels are:

Pixel 1: 11111000 11001001 00000011

Pixel 2: 11111000 11001001 00000011

Pixel 3: 11111000 11001001 00000011

The LSB (Least Significant Bit) algorithm embeds or conceals the 01000001 bits of the letter 'A' into the picture pixels to produce:

Pixel 1: 11111000 11001001 00000010

Pixel 2: 11111000 11001000 00000010

Pixel 3: 11111001 11001001 00000011

PIXEL VALUE DIFFERENCE(PVD)

The pixel-value differencing (PVD) method determines how many secret bits should be inserted by comparing the values of two successive pixels in a block. It calculates the payload by the difference value between two consecutive pixels by selecting two successive pixels and building a quantization range table which gives great imperceptibility to the stego picture. Furthermore, it has the benefit of transporting a high number of payloads while yet retaining visual integrity after data embedding.

EXPLOITING MODIFICATION DIRECTION(EMD) BASED METHODS

EMD (exploiting modification direction) has been a very well- known embedding approach for maintaining steganographic image integrity. During the embedding process in the EMD, the secret digit is generally changed using the (2n + 1)-ary system, where n is the number of cover pixels. The distortion range's maximum pixel value is just (1). To put it another way, the EMD uses a certain base to identify the local fluctuation of pixel intensity in a picture, allowing pixels in high texture areas to encode the more hidden information. In comparison to the LSB and PVD processes, the EMD may produce high visual quality. The highest capacity of the EMD approach, on the other hand, is up to 1.16 bpp for a number of (n = 2) two pixels.

As the number of chosen pixels is increased, the embedding payload reduces dramatically. As a result, many EMD-based strategies for improving embedding capacity have been developed.

EDGE BASED METHODS

The edge adaptive encoding approach is a popular embedding strategy in the spatial domain. When pixels in a smooth area of an image are directly modified in the spatial domain, the result is a visual distortion. Edge adaptive embedding schemes have thus evolved to keep visual distortion to a minimum.

Fig. 3 : Canny Edge Image

5.1(B) TRANSFORM DOMAIN TECHNIQUES

Instead of manipulating the picture itself, transformation or Image domain techniques modify the image's orthogonal transform.

The frequency content of a picture can be processed using Image domain methods. The frequency domain image enhancement approach works by computing a 2-D discrete unitary transform of the picture, such as the 2-D DFT, then modifying the transform coefficients using an operator M, after which the inverse transform is applied. The image's orthogonal transform contains two components: magnitude and phase. The frequency content of the picture makes up the magnitude. The phase is used to restore the spatial domain of the picture. Because the typical transform domain allows action on the image's frequency content, high frequency features such as edges and other subtle information may be easily increased. Steganography with JPEG pictures was considered to be impossible at first because they employ lossy compression, which causes sections of the image data to be changed. The JPEG compression process is split into two stages: lossy and lossless. The lossy stage includes the DCT and quantization phases, whereas the lossless stage includes the Huffman encoding used to further compress the data. Between these two processes, steganography can take place.

Discrete Wavelet Transform(DWT)

The DWT transform is described as a wavelet transformation that uses translations that obey established rules and a discrete collection of wavelet scales. When converting a spatial domain to a frequency domain, the wavelet transform is utilized. On a pixel-by-

pixel level, the wavelet transform distinguishes high frequency and low frequency information, which makes it useful in picture stenographic models. Because images at low frequency at various levels can give equivalent resolution, Discrete Wavelet Transform (DWT) is chosen over Discrete Cosine Transforms (DCT).

Discrete Cosine Transform (DCT)

This approach uses a sum of cosine functions to represent a static sequence of data information that may vary in frequency. These are significant in a variety of engineering and scientific applications, including lossy audio compression, such as MP3 files, and pictures, such as JPEG files, where little high-frequency components are discarded. For every image pixel which is a coloured component, The discrete cosine transformation is used by the JPEG image format to transform successive 8 × 8 pixel blocks of the image into 64 DCT coefficients each. The DCT coefficients F(u, v) of an 8 × 8 block of image pixels f(x, y) are given by

Below is the table to highlight the difference between algorithms of DCT and DWT techniques.

$$F(u,v) = \frac{1}{4}C(u)C(v)\left[\sum_{x=0}^{7}\sum_{y=0}^{7} f(x,y) * \cos\frac{(2x+1)u\pi}{16}\cos\frac{(2y+1)v\pi}{16}\right],$$

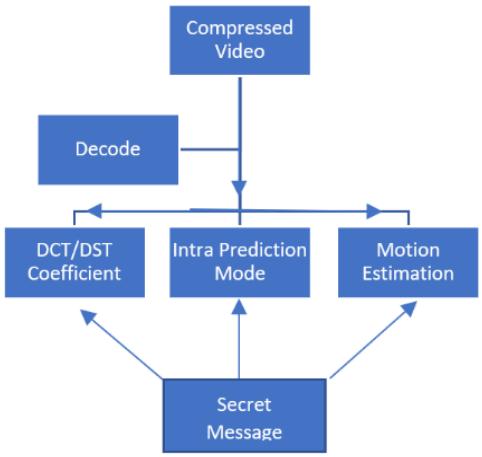
Below is the table to highlight the difference between algorithms of DCT and DWT techniques.

Algorithm for generating Stego-image through DWT	Algorithm for generating Stego-Image through DCT
Step 1: Examine the cover image and the secret text message that will be hidden within it. Step 2: Transform the secret text message into binary. 2D-Haar transform perform on the cover image. Step 3: Find filtering coefficients of the cover image in horizontal and vertical direction. Cover image is attached with data bits for DWT coefficients. Step 4: Get the stego image. Step 5: Determine the MSE or Mean Square Error, the PSNR or Peak Signal to Noise Ratio of the stego-image.	Step 1: Study cover image. Step 2: Study secret message and transform the message in binary form. Step 3: The cover image is divide into 8x8 blocks of pixels. Step 4: Operating from left to right and top to bottom for subtract 128 in each block of pixel. Step 5: DCT is perform to each block of pixel. Step 6: Each block is compressed by using quantization table. Step 7: Compute LSB of each DC coefficient and swap with each bit of secret message. Step 8: Create stego image. Step 9: Evaluate the PSNR or the Peak Signal to Noise Ratio.

5.2VIDEO STEGANOGRAPHY

Data hiding is a branch of video steganography, which is a method that embeds messages into cover contents and is utilized in a variety of domains including medical systems, law enforcement, copyright protection, and access control, among others . Because the human visual system is less sensitive to subtle changes in digital material, particularly digital video, video steganography is a technique for hiding messages and concealing the fact of transmission. It has lately gained in popularity for two key reasons: With the rapid expansion of computer applications, the information security problem is becoming increasingly important.[13] Types :

5.2(A) BASED ON INTRA EMBEDDING



Intra-embedding merges the video coding embedding process with syntactic features like intra- prediction, motion estimation, and DCT coefficients: As illustrated in the above figure, the sender embeds a hidden message into the video process. The common video coding formats H.26X and MPEG-X have a high compression ratio, and following compression coding, most of the video data redundancy is eliminated, making it more difficult to insert more data into the compressed video stream.

5.2(B) BASED ON PRE EMBEDDING

The transmitter embeds the cryptic message in the non-compressed video stream before compressing it, and the receiver decodes the compressed video received and extracts the secret message from the original video. Pre-embedded video steganography treats the video sequence as a collection of frames. Spatial and transform domain approaches are used in pre-embedding video steganography.

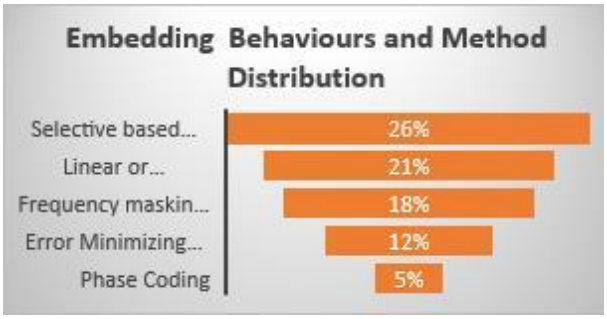
5.2(C) BASED ON POST EMBEDDING

The transmitter directly embeds secret messages into compressed bitstream, while the receiver extracts secret messages directly from the received embedded compressed video bit stream in the post- embedding video steganography process. Because of format compliance and computational complexity, it is not possible to include the entire bit stream.

5.3 AUDIO STEGANOGRAPHY

This is a technique for concealing information in audio signals. The signal is modified when data is encoded in it. This change should be undetectable to the human ear.[14] Audio steganography is more stunning than image steganography due to the properties of the Human Auditory System (HAS) such as big power, powerful range of hearing, and high range of audible frequency.

The chart below briefly explains the usage of different techniques, and embedding behaviors with method distributions, where it can be easily derived that the most popular technique is Selective based embedding with overall 26% usage spectrum over other methods of Audio Steganography. Secondly, we have sequential or linear embedding with 21% of overall audio data hiding methods.



Similarly, other constitutes rest 53% of the overall techniques includes error minimizing based embedding(12%), frequency masking and amplitude thresholding(18%), Pattern matching based embedding(7%), Phase Encoding(5%), etc.

6. STEGANALYSIS:DETECTING STEGANOGRAPHY

Analysis of a cover message of any kind to detect any hidden secret code is steganalysis. Just like steganography, steganalysis also uses several different techniques to detect and check for any concealed information in the given message.

Some of the techniques are briefly discussed below: Image, Audio and Video Steganalysis: As we know that image steganography has been very popular, the reverse technique, i.e., Image steganalysis has also caught millions of attention and interests.

Audio signals are data streams with a large capacity. Echo and phase over audio signals, there are several steganalysis techniques for concealment. The phase steganalysis method investigates the fact that phase coding is used inappropriately in each audio segment, causing changes in phase difference. Statistical techniques can also aid in the detection of hidden audio signals, where lineament selection and classifier construction are critical.

3. CONCLUSIONS

This paper gives a brief overview of steganography and its origins, from ancient times to modern days and the future that it awaits for. An extensive research work has been done to systematically review the possibilities in the world of steganography and getting more familiar with the techniques and methods that are in popular use and the methods that can be applied in action to overcome the previously used techniques(steganalysis).LSB, PVD, EDM, DWT, DCT, and other useful methods were implied and derived in order to get a better understanding of the field, it can be concluded that steganography has a great potential despite the challenges with other data hiding techniques.

REFERENCES

[1] Kirti Chopra, Ishpreet Singh Virk "Image Steganography Using Edge Detection Technique." International Journal of Computer Sciences and Engineering 6.12 (2018): 222-227.

[2] S.Bansal, Data Security by Steganography, International Journal of Scientific Research in Network Security and Communication, Vol.7, Issue.1, pp.10-12, 2019.

[3] Das, R.; Tuithung, T.,"A novel steganography method for image based on Huffman Encoding," Emerging Trends and Applications in Computer Science (NCETACS), 2012 3rd National Conferenceon ,vol., no., pp.14,18, 30-31 March2012

[4] Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM,47:10, October 2004.

[5] Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", IEEE Journal of selected Areas in Communications, May 1998.

[6] Joseph, A., and V. Sundaram. "Cryptography and steganography–A survey." (2011).

[7] Manoj I.VenkataSai, and B. Tech. "Cryptography and steganography. "International Journal of Computer Applications 1.12 (2010):63-68.

[8] Sangale, Adinath, et al. "secure messaging using cryptography, steganography and qr code."

[9] Li, Bin, et al. "A survey on image steganography and steganalysis." J. Inf. Hiding Multim. Signal Process. 2.2 (2011): 142-172.

[10] Saleh, Mohammed A. "Image steganography techniques-a review paper." International Journal of Advanced Researching Computer and Communication Engineering, ISSN (2018):2278- 1021.

[11] More, Nitesh Kumar and Sipi Dubey. "JPEG Picture Compression Using Discrete Cosine Transform." (2012).

[12] Morkel, Tayana & Eloff, Jan & Olivier, Martin. (2005). An overview of image steganography. 1-11.

[13] Yunxia Liu , Shuyang Liu , Yonghao Wang, Hongguo Zhao, Si Liu , Video Steganography: A Review, Neurocomputing (2018),

[14] Digital audio steganography: Systematic review, classification, and analysis of the current state of the art.

[15] Juned Ahmed Mazumder, K. Hemachandran, 2012, Review Of Different Techniques Used In Recent Steganography Researches, international journal of engineering research & technology (ijert) Volume 01, Issue 08 (October 2012)