A Survey on various types of Steganography and Analysis of Hiding Techniques

Navneet Kaur#1, Sunny Behal#2

[1]Research Scholar, Department of Computer science Engineering, SBSSTC, India

[2]Associate Professor, Department of Computer science Engineering, SBSSTC, India

***Abstract*—Digital Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio, and video files. Under this assumption, if the feature is visible, the point of attack is evident, thus the here goal is conceal to the existence of the embedded data .This is totally review paper, in which we provide the comparison of available steganography technology hiding text in an image file using Least Significant Bit (LSB) based Steganography, Discrete Cosine Transform (DCT) based Steganography and Discrete Wavelet Transform (DWT) based steganography. The LSB algorithm is implemented in spatial domain in which the payload bits are embedded into the least significant bits of cover image to derive the stego-image whereas DCT & DWT algorithm are implemented in frequency domain in which the stego -image is transformed from spatial domain to the frequency domain**.

***Keywords*—Steganography, Cryptography, Least Significant Bit (LSB); Discrete Cosine Transform (DCT); Discrete Wavelet Transform (DWT).**

I. INTRODUCTION

Steganography is the art and science of covered writing (hide in plain sight) and its techniques are in use from hundreds of years. Digital Steganography is the technique of securing digitized data by hiding it into another piece of data. Today, in digital age the easy access to any form of data such as audio, videos, images and text make it vulnerable to many threats [1]. The data can be copied for purpose of copyright violation, tampered with or illegally accessed without the knowledge of owner. Therefore, the need of hiding secret identification inside different types of digital data is required such that owner can prove copyright ownership; identify attempts to tamper with sensitive data and to embed annotations. The main task of the field of steganography is the storing, hiding, and embedding of secret data in all types of digital data. The main goal of steganography is to communicate securely in a completely undetectable manner [2] such that no one can suspect that it exist some secret information. Unlike cryptography, which secures data by transforming it into another unreadable format, steganography makes data invisible by hiding (or embedding) them in another piece of data [3]. Thus cryptography is science of overt secret writing while steganography as covert secret writing. The cover, host or the carrier is the target media in which information is hidden so that other person will not notice the presence of the information. The modified cover, including the hidden data, is referred to as a stego object which can be stored or transmitted as a message [4]. The secret information can be embedded in various types of covers. If information is embedded in a cover text (text file), the result is a stego-text object. Similarly, it is possible to have cover audio, video and image for embedding which result in stego-audio, stego-video and stego-image respectively. Nowadays, the combinations of steganography and cryptography methods are used to ensure data confidentiality [5] and to improve information security. Steganography is used in other grounds also like copy right, preventing e-document forging. Table 1 shows the comparison of various secret communication techniques used nowadays

TABLE I
COMPARISON OF SECRET COMMUNICATION TECHNIQUES

Secret Communication Techniques	**Confidentiality**	**Integrity**	**Un-removability**
Encryption	Yes	No	Yes
Digital Signatures	No	Yes/No	No
Steganography	Yes/No	Yes/No	Yes

The proposed paper provide a systematic survey of existing Steganography research by categorizing existing methods according to the certain features and analysing the advantages of these features. The motive of the paper is to provide researchers with in-depth study of subject. The proposed paper is organized in 4 sections. Section 2 deals with the classification of various types of steganography. The section 3 demonstrates the comparative study of existing steganography methods.

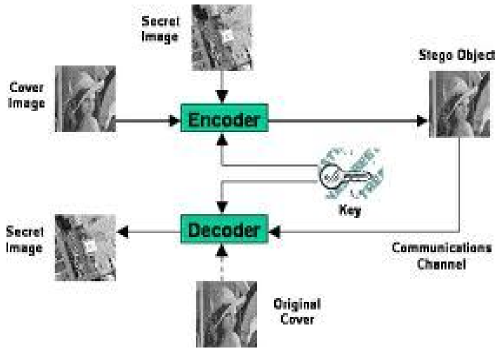

Fig1. Process of steganography

Figure 1 shows a simple representation of the generic embedding and decoding process in steganography. In this example, a secret image is being embedded inside a cover image to produce the stego image. The first step in embedding and hiding information is to pass both the secret message and the cover message into the encoder. Inside the encoder, one or several protocols will be implemented to embed the secret information into the cover message. The type of protocol will depend on what information you are trying to embed and what you are embedding it in. For example, you will use an image protocol to embed information inside images

II. CLASSIFICATIONS OF DIGITAL STEGANOGRAPHY

The steganography can be classified according to its importance and goals. So; various types of steganography are:

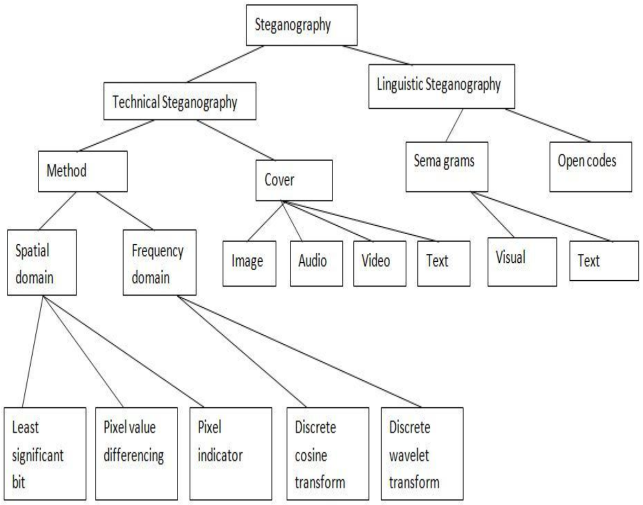

Fig2. Types of steganography

1) Linguistic Steganography:
Linguistic technique is used to hide the message within the cover text in non-obvious way such that the presence of message is imperceptible to an outsider [6]. It is divided into two types:

A) *Semagrams:* It uses only symbols and signs to hide the information. It is further categorized into two ways:

i) *Visual Semagrams***:** A visual semagrams uses physical objects used every day to convey a message. For example: the positioning of items on a particular website.

*ii)Text Semagrams***:** This type is used to hides a message by modify the appearance of the carrier text, or by changing font size and type, or by adding extra space between words and by using different flourished in letters or handwritten text.

B) *Open Code*: In this approach the message is embedded in legitimate paraphrases of cover text in the way such that it appears not obvious to an unsuspecting observer. It can be achieved by two ways viz., Jargon which is understood only by a group of peoples and Cipher which uses some concealed ciphers to hide a message openly in the carrier medium. A subset of jargon codes are cue codes, where certain pre-arranged phrases convey meaning.

2) *Technical Steganography*:
Technical steganography uses special tools, devices or scientific methods to hide a message. In this type one can use invisible ink, microdots, computer based methods or various hiding places to keep message secret

I) *Cover*: The cover message is the carrier of the message such as image, video, audio, text, or some other digital media [7]. The cover is divided into blocks and message bits which are hidden in each block. The information is encoded by changing various properties of cover image. The cover blocks remain unchanged if message block is zero [8].

A) Text Steganography: In this approach the cover text is produced by generating random character sequences, changing words within a text, using context-free grammers or by changing the formatting of an existing text to conceal the message. The cover text generated by this approach can qualify for linguistic steganography if text is linguistically-driven. Although these text- based methods has its own unique characteristics for cover text but suffers from various problems from both a linguistic and security stand point [9] [10].

B) Image Steganography:
This Steganography technique is more popular in recent year than other steganography possibly because of the flood of electronic image information available with the advent of digital cameras and high-speed internet distribution. It can involve hiding information in the naturally occurred noise within the image. Most kinds of information contain some kind of noise. Noise refers to the imperfections inherent in the process of rendering an analog picture as a digital image. In Image steganography we can hide message in pixels of an image. An image steganographic scheme is one kind of steganographic systems, where the secret message is hidden in a digital image with some hiding method [11]. Someone can then use a proper decoding procedure to recover the hidden message from the image. The original image is called a cover image in steganography, and the message-embedded image is called a stego image [12] [13]. Various methods of image steganography are:

i) Data Hiding Method: hiding the data, a username and password are required prior to use the system. Once the user has been login into the system, the user can use the information (data) together with the secret key to hide the data inside the chosen image. This method is used to hiding the existence of a message by hiding information into various carriers. This prevents the detection of hidden information [14].

ii) Data Embedding Method: For retrieving the data, a secret key is required to retrieving back the data that have been embedded inside the image. Without the secret key, the data cannot be retrieved from the image. This is to ensure the integrity and confidentiality of the data. The process of embedding the message inside the image, a secret key is needed for retrieving the message back from the image, the secret message that is extracted from the system is transfer into text file and then the text file is compressed into the zip file and zip text file is converting it into the binary codes [15].

iii) Data Extracting Method: It is used to retrieve an original message from the image; a secret key is needed for the verification. And for extracting method, a secret key is needed to check the key is correct with the decodes from the series of binary code. If key is matched, the process continues by forming the binary code to a zipped text file, the unzip the text file and transfer the secret message from the text file to retrieve the original secret message [15].

I) Features Of Image Steganography:

1) Transparency: The steganography should not affect the quality of the original image after steganography.

2) Robustness: Steganography could be removed intentionally or unintentionally by simple image processing operations like contrast or enhancement brightest gamma correction, steganography should be robust against variety of such attacks.

3) Data payload or capacity: This property describes how much data should be embedded as a steganography to successfully detect during extraction.

C) *Audio Steganography*:

Audio steganography, the hiding of messages in audio “noise” (and in frequencies which humans can’t hear), is another area of information hiding that relies on using an existing source as a space in which to hide information. Audio steganography can be problematic and can be useful for transmitting covert information in an innocuous cover audio signal [8] [16]

A) Types of Audio Steganography:

1) Echo Hiding
2) Phase Coding
3) Parity Coding
4) Spread Spectrum
5) Tone insertion

1) Echo Hiding: This method embeds data or text into audio signals by adding a small echo to the host signal. The Nature of the echo is a resonance added to the host audio. Then the data is invisible by varying three echo parameters: initial amplitude, decay rate, and offset. If only one echo is produced from the original signal, then only one bit of information could be encoded [17]

2) *Phase Coding:* One of the most effective coding methods in terms of the signal-to perceived noise ratio. In this phase components of sound are not as perceptible to the human ear as noise is. It can be done by substituting the phase of an initial audio segment with a reference phase that represents the data. It 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 subsequent segments is then adjusted store the relative phase between segments. Disadvantage: It is a complex method and has low data transmission rate [17] [18]

3) *Parity Coding*: This method breaks a signal down into different regions of samples and encodes each bit from the secret message in a sample region's parity bit. If the parity bit of selected region does not match the secret bit to be encoded, Disadvantage: This method like LSB coding is not robust in nature. Advantage: The sender has more of a choice in encoding the secret bit, and the signal can be changed in a more unobtrusive manner [17]

4) *Spread Spectrum:* This is analogous to a system using an implementation of the LSB coding that randomly spreads the message bits over the entire sound file. It is used to encode a category of information by spreading the encoded data across frequency spectrum. This allows the signal reception, even if there is interference on some frequencies. Disadvantage: It can introduce noise into a sound file [17] [18].

5) *Tone insertion:* In this inaudibility of lower power tones in the presence of significantly higher ones. Tone insertion method can resist to attacks such as low-pass filtering and bit truncation addition to low embedding capacity, embedded data could be maliciously extracted since inserted [19]

A) Uses of Audio Steganography:

1) Audio data hiding can be used anytime you want to hide data. There are many reasons to hide data but most important is to prevent unauthorized persons from becoming aware of the existence of a message.

2) Audio data hiding can also be used in the non commercial sector to hide information that someone wants to keep private.

3) It can also be used in forensic applications for inserting hidden data into audio files for the authentication of spoken words and other sounds

III) TECHNIQUES OF STEGANOGRAPHY:

1) Method: In spatial domain, images are represented by pixels. Simple watermarks could be embedded by modifying the pixel values or the least significant bit (LSB) values [20]. It directly loads the raw data into the image pixels. Some of its algorithms are LSB, SSM Modulation based technique.

A)Spatial Domain: In this technique only the least significant bits of the cover object is replaced without modifying the complete cover object. It is a simplest method for data hiding but it is very weak in resisting even simple attacks such as compression, transforms [23].

i) Least Significant Bit (LSB):

This is the most common, simple approach for embedding data in a cover image. The least significant bit (8th bit) of one or all of the bytes inside an image is changed to a bit of the secret message. When we use 24-bit image, three color bits components are used which are red, green, blue, each byte store 3 bits in every pixel. An 800 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data. For example a grid for 3 pixels of a 24-bit image can be as follows:

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

When the number 200, which binary representation is 11001000, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

(00101101 00011101 11011100)
(10100110 11000101 00001100)
(11010010 10101100 01100011)

The number was embedded into the first 8 bytes of the grid, only the 3 underlined bits needed to be changed according to the embedded message. On average, only half of the bits in an image will modified to hide a secret message using the maximum cover size. Since there are 256 possible intensities of each primary color, changing the LSB of a pixel results in small changes in the intensity of the colors. These changes cannot be visible by the human eye due to the message hidden. In these consecutive bytes of the image data – from the first byte to the end of the message – are used to embed the information. And easy to detect, more secure system for the sender and receiver to share a secret key that specifies only some pixels to be changed   In its simplest form, LSB makes use of BMP images, since they use lossless compression. It hide a secret message inside a BMP file, one would require a very large cover image. In BMP images of 800 × 600
Pixels are not often used on the Internet and might arouse suspicion. For this reason, LSB steganography has also been developed for use with other image file formats [4]. It is a simple method for embedding data in a cover image. This is the simplest algorithm in which information can be inserted into every bit of image information. Given an image with pixels, and each pixel being represented by an 8-bit sequence, the watermarks are embedded in the last (least significant bit) of selected pixels of the image proposed a simple data hiding technique by simple LSB substitution. In this technique last bit of host data is randomly changed and produce the watermarked data at output. The cover LSB media data are used to hide the message [21].

ii) Pixel Value Differencing:

It provides both high embed-ding capacity and outstanding imperceptibility for the stego-image; this segments the cover image into non overlapping [8] blocks containing two connecting pixels and it modifies the pixel difference in each pair for data embedding.

iii) *Pixel Indicator*:

This method gives the stego images of better quality than the traditional method while maintaining a high embedding capacity and it also uses concept of hiding the data using the difference between the pixel values [20]. It's more complex way of hiding information in an image. Transformations are used on the image to hide information in. Transform domain embedding can be termed as a domain of embedding techniques in frequency domain; image is represented in terms of its frequencies.

B) Frequency Domain:

i) Discrete Cosine Transformation:

These methods convert the uncompressed image into JPEG compressed type[22]*It is based on* data hiding used in the JPEG compression algorithm to transform successive 8x8-pixel blocks of the image from spatial domain to 64 DCT coefficients each in frequency domain. [23]The main advantage of this method is its ability to minimize the block like appearance resulting when boundaries between the 8x8 sub-images become visible (known as blocking artefact).

ii) Discrete Wavelet Transformation:

It gives the best result of image transformation .it splits the signal into set of basic functions .there are two types of wavelet transformation one is continuous and other is discrete [24] This is the new idea in the application of wavelets, in this the information is stored in the wavelet coefficients of an image, instead of changing bits of the actual pixels. It also performs local analysis and multi-resolution analysis. DWT transforms the object in wavelet domain and then processes the coefficients and performs inverse wavelet transform to show the original format of the stego object [25].

IV COMPARISON OF DIFFERENT STEGANOGRAPHIC TECHNIQUES

TABLE 2:

Steganography Techniques	Cover Media	Embedding Techniques	Advantages
Image Hiding	Image		
1.LSB(Least Significant Bit)		This method is used the least significant bit of every pixel in one image to hide the most significant bit of another	Simplest & easiest way of hiding information
2.DCT (Discrete Cosine Transform)		Embeds the information by altering the transformed DCT co-efficient	Hide data can be distributed more evenly over the whole image in such a way to make it robust
3.DWT (Discrete Wavelet transform)		This technique work by talking many wavelet to encode a whole image	Coefficient of wavelet are altered with the noise within tolerable level

III. CONCLUSION

In this paper provides literature review on digital steganography. As steganography becomes widely used in computing, there are issues that need to be resolved. There are a wide variety of different techniques with their own advantages and disadvantages. We surveyed various types of steganography. We studied the various techniques, Least Significant Bit (LSB), DCT (Direct Cosine Transform), DWT (Discrete Wavelet Transform)which helps to improve in security.

REFERENCES

[1] Artz, Donovan. "Digital steganography: hiding data within data." internet computing, IEEE 5.3 (2001): 75-80.

[2] Amin, Muhalim Mohamed, et al. "Information hiding using steganography." Telecommunication Technology, 2003. NCTT 2003 Proceedings. 4th National Conference on. IEEE, 2003.

[3] Shashikala Channalli, Ajay Jadhav, "Steganography An Art of Hiding Data" International Journal on Computer Science and Engineering Vol.1(3), 2009, 137-141

[4] Morkel, Tayana, Jan HP Eloff, and Martin S. Olivier. "An overview of image steganography." ISSA. 2005.

[5] Yuk Ying Chung, fang Fei Xu , "Development of video watermarking for MPEG2 video" City university of Hong Kong ,IEEE 2006.

[6] Singh, Nanhay, Bhoopesh Singh Bhati, and R. S. Raw. "Digital image Steganalysis for computer forensic investigation." Computer Science and Information Technology (CSIT) (2012): 161-168..

[7] AL-Shatnawi, Atallah M., and Bader M. AlFawwaz. "An Integrated Image Steganography System with Improved Image Quality." Applied Mathematical Sciences 7.71 (2013): 3545-3553.

[8] Bhattacharyya, Souvik and Gautam Sanyal. "A Robust Image Steganography using DWT Difference Modulation (DWTDM)." International Journal of Computer network & Information Security 4.7 (2012)..

[9] K. Bennett, "Linguistic Steganography: survey, analysis, and robustness concerns for hiding information in text" center for Education and Research in Information Assurance and Security,Purdue University 2004.

[10] Hitesh Singh, Pradeep Kumar Singh, Kriti saroha "A Survey on Text Based Steganography" Proceedings of the 3rd National Conference; INDIACom-2009 Computing For Nation Development, February 26 – 27, 2009 Bharati Vidyapeeth's Institute of Computer Applications and Management, Ne w Delhi.

[11] Hitesh Singh, Pradeep Kumar Singh, Kriti Saroha "A Survey on Text Based Steganography" Proceedings of the 3rd National Conference; INDIACom-2009 Computing For Nation Development, February 26 – 27, 2009 Bharati Vidyapeeth's Institute of Computer Applications and Management, Ne w Delhi

[12] Jain, Nitin, Sachin Mesh ram, and Shikha Dubey. "Image Steganography Using LSB and Edge–Detection Technique. " International Journal of Soft Computing and Engineering (IJSCE) ISSN (2012): 2231-2307.

[13] M. M. Amin, M. Salleh, S. Ibrahim, M.R. Katmin, M.Z.I. Shamsuddin, "Information Hiding using Steganography" Proceedings of 4th National Conference on Telecommunication Technology, Shah Alam , Malaysia, 2003.

[14] Amin, Mohamed "Muhalim and Ibrahim, Subariah and Salleh, Mazleena and Katmin, Mohd rozi (2003) Information hiding using steganography.

[15] Ibrahim, Rosziati, and Teoh suk Kuan. "Steganography Algorithm to hide secret message inside an Image." arXiv preprint arXiv: 1112.2809 (2011).

[16] Jenkins, Neil, and Jean Everson Martina "Steganography in audio." University of Cambridge CST Part II Dissertation (2009) ..

[17] Nosrati, Masoud, Ronak Karimi, and Mehdi Hariri. "Audio Steganography: A Survey on Recent Approaches." World Applied Programming 2.3 (2012): 202-205..

[18] Dutta, Poulami, Debnath Bhattacharyya, and Tai-hoon Kim. "Data hiding in audio signal: A review." International journal of database theory and application2.2 (2009): 1-8..

[19] H.B.kekre , Archana Athawale , "Information Hiding In Audio Signal".Intertional Journal of Computer Application volume 7-No.9 October 2010.

[20] Sohag, Saeed Ahmed, Md Kabirul Islam, and Md Baharul Islam. "A Novel Approach for Image Steganography Using Dynamic Substitution and Secret key. "

[21] Goel, Arun Rana, and Stuti Manpreet Kaur. "A Review of Comparison Techniques of Image Steganography. " Global Journal of Computer Science and Technology 13.4 (2013) .

[22] AL- Shatnawi, Atallah M., and Bader M. AlFawwaz. "An Integrated Image Steganography System with Improved Image Quality." Applied Mathematical Sciences 7.71 (2013): 3545-3553..

[23] Bhattacharyya, Souvik, and Gautam Sanyal. "A Robust Image Steganography using DWT Difference Modulation (DWTDM)." International Journal of Computer Network & Information Security 4.7 (2012) .

[24] Saddaf rubab and M Younus article: Improved Image Steganography Technique for Colored Images using Wavelet Transform. International Journal of Computer Applications 39(14):29-32, February 2012. Published by Foundation of Computer Science, New York, USA.

[25] Banik Bamali Gupta and Samir K Bandyopadhyay " A DWT Method for Image Steganography "International Journal 3.6(2013)