A Review on Digital Image Steganography with its Techniques and Model

Divyanshu Triapthi[1], Yash Kumar Singh[2], Rohit Singh[3]
[1, 2, 3] Department of CSE
[1, 2, 3] ITM University, Gwalior, India

Abstract- *Steganography is one of the methods of secret communication that hides the existence of hidden message. It can be defined as the study of invisible communication that usually deals with the ways of hiding the existence of the communicated message. The hidden message may be text, image, audio, video, etc. The files can be a cover image after inserting the message into the cover image using a stego-key. It is reffered to as stego-image. Steganography is the art of hiding information through original files in such a manner that the existence of the message is unknown. The term steganography is coming from the Greek word Steganos, which means, "Covered Writing". The original files can be referred to as cover text, cover image, or cover audio. After inserting the secret message it is referred to as stego-medium. A stego-key is used for hiding process to restrict detection and/or recovery of the embedded data. While cryptography protects the content of messages, steganography hides the message so that intermediate persons cannot see the message. In this paper, we define survey on steganography , types on steganography, classification on steganography and techniques of steganography, etc.*

Keywords- Steganography, LSB, PVD, BPCP.

I. INTRODUCTION

Steganography is a technique to hide information in ways that prevent the detection of hidden messages. It uses digital media as carriers for secret communication. Cryptography and Steganography are not one and the same. While Cryptography scrambles a message so that it cannot be understood, Steganography hides the messages so that it cannot be seen. Un-detectability, Robustness and capacity of the hidden data are the main features that differentiate steganography from cryptography. A Steganogram is nothing but a steganographically modified carrier with hidden information. Secure steganographic algorithms hide confidential messages in carrier media to form steganograms so that an attacker will not able to find it [1].

II. STEGANOGRAPHY MODEL

Generally a steganographic system has a coverage file that is used to cover the original message and the steganography algorithm to carry out the required object as shown in Fig. 1. The result is a file called stego-file which has the message inside it, hidden. This stego file is then sent to the receiver where the receiver retrieves the message by applying the de-steganography. The goal of modern steganography is to keep the message undetectable [2].

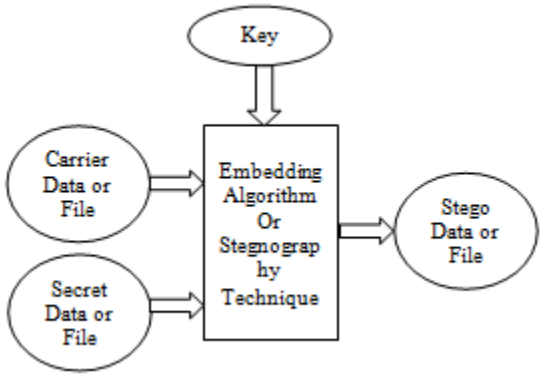

Fig.1: Basic Steganography Model [2]

III. STEGANOGRAPHY SYSTEM

Steganography is the art of hiding the information in some other host object. It has been used since ancient time by the people. In ancient time, secret information is hidden in the back of the wax, the scalp of the slaves, in rabbits, etc. With passage of time, the application of steganography and its area has become widened. With the introduction digitization era, digital steganography has emerged as the new tool to hide the information secretly. Text, digital image, digital audio and digital video have become the host object for data hiding. Below are some of the common term which is necessary to understand any steganography system [3].

Cover Media- It is the medium in which secret information is embedded in such a way that it is difficult to detect the presence of data

Stego-Media- It is medium obtained after embedding the secret information.

Secret data- The data or information to be hidden in cover media.

Steganalysis- The process of detecting, presence of secret data in cover media.

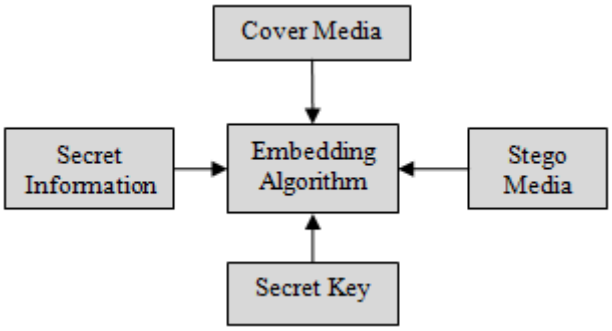

Fig.2: Steganography Process

IV. STEGANOGRAPHY TYPES

The various types of steganography include [4]:

a) Image Steganography

The image steganography is the process in which we hide the data within an image so that there will not be any perceivable change in the original image. The conventional image steganography algorithm is an LSB embedding algorithm.

b) Audio Steganography

The method of hiding secret information in an audio is known as audio steganography. There are various methods for hiding secret data in an audio such as LSB, Phase Coding etc.

c) Video Steganography

The method of hiding secret information in a video is known as video steganography. Video consist of images as well as audio. Hence, both images and audio steganography can be used for video steganography.

d) Text files Steganography

The method of hiding secret information in a text is known as text steganography. Text steganography requires less memory as it can only store text files. It provides quick communication or transfer of files from one computer to another. Text steganography is not commonly used as text files containing a large amount of redundant data.

V. STEGANOGRAPHY IN DIGITAL MEDIUMS

Depending on the type of the cover object there are many suitable steganographic techniques which are followed in order to obtain security. It can be shown in Figure 1.

i) Image Steganography:

Taking the cover object as an image in steganography is known as image steganography. Generally, in this technique pixel intensities are used to hide the information.

ii) Network Steganography:

When taking a cover object as network protocol, such as TCP, UDP, ICMP, IP *etc*, where protocol is used as carrier, is known as network protocol steganography. In the OSI network layer model, there exist covert channels where steganography can be achieved in unused header bits of TCP/IP fields.

iii) Video Steganography:

Video Steganography is a technique to hide any kind of files or information into a digital video format. Video (combination of pictures) is used as a carrier for hidden information. Generally discrete cosine transform (DCT) alter values (*e.g.*, 8.667 to 9) which is used to hide the information in each of the images in the video, which is not noticeable by the human eye. Video steganography uses, such as H.264, Mp4, MPEG, AVI or other video formats.

iv) Audio Steganography:

When taking audio as a carrier for information hiding it is called audio steganography. It has become a very significant medium due to voice over IP (VOIP) popularity. Audio steganography uses digital audio formats such as WAVE, MIDI, AVI, MPEG or *etc* for steganography.

v) Text Steganography:

General technique in text steganography, such as the number of tabs, white spaces, capital letters, just like Morse code [5] and *etc* is used to achieve information hiding.

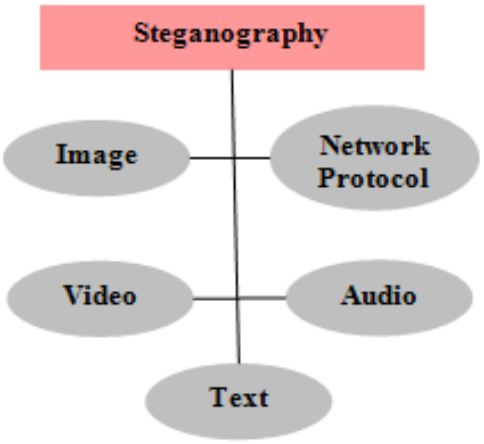

Figure-3. Digital Medium to Achieve Steganography

VI. STEGANOGRAPHY TECHNIQUES

1) Spatial Domain Methods:

In this method the secret data is embedded directly in the intensity of pixels. It means some pixel values of the

image are changed directly during hiding data. Spatial domain techniques are classified into following categories:

i) Least significant bit (LSB)
ii) Pixel value differencing (PVD)
iii) Edges based data embedding method (EBE)
iv) Random pixel embedding method (RPE)
v) Mapping pixel to is hidden data method
vi) Labelling or connectivity method
vii) Pixel intensity based.

i) LSB:

This method is most commonly used for hiding data. In this method the embedding is done by replacing the least significant bits of image pixels with the bits of secret data. The image obtained after embedding is almost similar to the original image because the change in the LSB of image pixel does not bring too much differences in the image.

ii) PVD:

In this method, two consecutive pixels are selected for embedding the data. The payload is determined by checking the difference between two consecutive pixels and it serves as a basis for identifying whether the two pixels belongs to an edge area or smooth area.

iii) BPCP:

In this segmentation of the image are used by measuring its complexity. Complexity is used to determine the noisy block. In this method noisy blocks of bit plan are replaced by the binary patterns mapped from a secret data.

2) Spread Spectrum Technique:

The concept of spread spectrum is used in this technique. In this method the secret data is spread over a wide frequency bandwidth. The ratio of signal to noise in every frequency band must be so small that it's become difficult to detect the presence of data. Even if parts of the data are removed from several bands, there would be still enough information is present in other bands to recover the data. Thus, it is difficult to remove the data completely without entirely destroying the cover .It is a very robust technique mostly used in military communication.

3) Statistical Technique:

In the technique message is embedded by changing several properties of the cover. It involves the splitting of cover into blocks and then embedding one message bit in each block. The cover block is modified only when the size of message bit is one, otherwise no modification is required.

4) Transform Domain Technique:

In this technique; the secret message is embedded in the transform or frequency domain of the cover. This is a more complex way of hiding messages in an image. Different algorithms and transformations are used on the image to hide message in it. Transform domain techniques are broadly classified such as

i) Discrete Fourier transform technique (DFT)
ii) Discrete cosine transformation technique (DCT)
iii) Discrete Wavelet transformation technique (DWT)
iv) Lossless or reversible method (DCT)
v) Embedding in coefficient bits

5) Distortion Techniques:

In this technique the secret message is stored by distorting the signal. A sequence of modification is applied to the cover by the encoder. The decoder measures the differences between the original cover and the distorted cover to detect the sequence of the modifications and consequently recover the secret message.

6) Masking and Filtering:

These techniques hide information by marking an image. Steganography only hides the information where as watermarks become a potion of the image. These techniques embed the information in the more significant areas rather than hiding it into the noise level. Watermarking techniques can be applied without the fear of image destruction due to lossy compression as they are more integrated into the image. This method is basically used for 24-bit and gray scale images [7].

VII. LITERATURE SURVEY

Hui Tian et.al (2015) Evaluate the proposed scheme with ITU-T G. 711 (Alaw) as the codec of the cover speech and compare it with previous methods. The experimental results demonstrate that the proposed scheme is really feasible in both theory and practice, and can provide consistently optimal embedding performance in any case [8].

Vidhya P.M, et.al (2015) a method of steganography is proposed with an Indian local language, Malayalam. The proposed method consists of custom Unicode based technique with embedding based on indexing, i.e. the original message is encoded in Malayalam text with custom UNICODE values

generated for the Malayalam text. The comparative study of the proposed method against an existing method revealed that, the proposed steganography methods is more precise in the encoding process and in the decoding process. The method achieved a precision rate of .95 and the decoding rate of .81 [9].

Milia Habib et.al (2015) a secure DCT steganography method is proposed. It allows hiding a secret image in another image randomly using Chaos. The chaotic generator Peace Wise Linear Chaotic Map PWLCM with perturbation was selected, it has good chaotic properties and an easy implementation. It was used to obtain the pseudo-random series of pixels in which the secret image will be embedded in their DCT coefficients. It enhances the LSB-DCT technique with threshold [10].

Yugeshwari Kakde et.al (2015) Working on audio-video steganography, which is the combination of Audio steganography and Image steganography, in this the author is using computer forensics technique for authentication purpose. In this paper our aim is to hide secret information behind audio and image of a video file. As we know that video is the combination of many still frames of images and audio[11].
Kamaldeep Joshi, et.al (2015) a new method of image steganography in spatial domain on gray images blend with cryptography is present. Steganography and cryptography are used to hide messages and its meaning respectively. By this method, the message is first encrypted using Vernam cipher algorithms and then the message (encrypted) is embedded inside an image using the new image steganography method i.e. LSB with Shifting (LSB-S) [12].

Sayantari Ghosh, et.al (2015) a Hilbert curve based technique to embed information in an image using the neuro psychological behavior of the human vision system which is robust to different attacks like cropping, scratching, additive noise etc [13].

Avinash Tyagi et.al (2015) a new image steganography technique has been proposed which is based on the pixel value differencing and the pixel value sum of two consecutive pixels of a cover image. The proposed algorithm hides the secret data in the cover image by manipulating the difference or sum of the non-overlapping blocks of two consecutive pixels. This technique is an improvement over the Wu and Tsai's PVD technique that is totally based on pixel value differencing [14].

In Soon-Nyean Cheong, et.al (2014) Validates the user perception and behavioral intention to use NFC ESGP smartphone access control system through an experiment and user evaluation survey. Results indicated that users weigh security as a dominant attribute for their behavioral intention to use NFC ESGP smartphone access control system. Author's findings offer a new insight for security scholars, mobile device service providers and expert systems to leverage on the two-factor authentication with the use of NFC-enabled smartphone [15].

In Ifra Bilal, et.al (2014) a survey on latest audio steganographic methods is carried out along with their strength and weakness. Also, comparison between various steganographic methods based on robustness is carried out. Another contribution of this paper is evaluation of performance of various reviewed steganography techniques [16].

Md. Rashedul Isla et.al (2014) The proposed technique has focused on Bitmap image as it is uncompressed and convenient than any other imageformat to implement LSB Steganography method. For better security AES cryptography technique has also been used in the proposed method. Before applying the Steganography technique, AES cryptography will change the secret message into cipher text to ensure two layer security of the message [17].

Prabakaran G et.al (2014) Secret image hides into two different domains like as IWT (Integer Wavelet Transform) and DWT (Discrete Wavelet Transform). The cover image and secret image co-efficient values are embedded by 512*512 using fusion process techniques. We applied various combinations of DWT and IWT on both images and obtained a good quality stego image [18].

Nadeem Akhtar,et.al (2014) An improvement in the plain LSB based image steganography is proposed and implemented. The paper proposes the use of bit inversion technique to improve the stego image quality. Two schemes of the bit inversion techniques are proposed and implemented. In these techniques, LSBs, of some pixels of cover image are inverted if they occur with a particular pattern of some bits of the pixels [19].

P. Thiyagarajan, et.al (2013) The proposed method is designed by considering issues related to transmission errors which could contaminate the medical images transmitted. The performance of the proposed method is compared to other information hiding methods against various parameters such as the robustness of stego-image against affine transformations, toughness of the dynamic key generated, detection of transmission error, embedding rate and reversibility [20].

Ratnakirti Roy, et.al (2013) This paper proposes an edge adaptive image steganography mechanism which combines the benefits of matrix encoding and LSBM to embed data and also uses a chaotic mapping scheme to provide enhanced security to the payload. Efforts have been given to ensure that the proposed mechanism conforms to high Imperceptibility and Fidelity, which are the essential quality requirements for any image steganography system [21].

Susmita Mahato, et.al (2013) a modified approach for text steganography based on HTML tags and attributes. As HTML is rich in tags and its attributes, easily communicated in the internet, and the source code is rarely checked by anybody it can be used intelligently to perform text steganography. By hiding the secret data inside the source code of HTML, text steganography can be easily achieved [22].

Jose Juan et.al (2013) a low complexity steganographic system for digital images is proposed. The core of the proposed system is an adaptation of the interpolation-error expansion technique. From experimental results the high perceptual and statistical transparency of the proposed scheme are shown. Moreover, the proposed system embedding rate is similar and some times outperforms the frequency transform-based embedding rate with lower computational complexity [23].

C.L. Philip Chen, et.al (2012) Builds up a pattern recognition system to detect anomalies in JPEG images, especially steganographic content. The work demonstrated in this paper is extensible and can be improved by integrating various new and current techniques [24].

D. Biswasa, et.al (2012) a new innovative technique for hiding and then retrieving a secret image. The technique consists of two processes viz. Encoding and decoding. The main focus in the encoding phase is to hide the secret RGB colour image in a cover image and get some shares which are to be transmitted to the receiver. In the decoding phase, the main focus is to get back the retrieved image back to the original image quality as much as possible from the shares in the received end [25].

Siddharth Singh et.al (2012) a robust image steganography technique based on redundant discrete wavelet transforms has been proposed. Steganography is the process of hiding one medium of communication like text, audio and image within another. The proposed steganography algorithm uses blind recovery approach. We have tested the proposed method on different cover and payload images[26].

Ribhu et.al (2012) an approach to steganography that is based on sparse representation of signals. The proposed method hides data within an audio clip or an image without compromising on their perceived qualities. It is also demonstrated in our experiments that the hidden data can be successfully separated out from the cover message. However, the proposed method is a fragile one in the sense that it is not robust to any sort of lossy processing like compression, cropping, etc [27].

VIII. COMPARISON OF STEGANOGRAPHY TECHNIQUE [28]

Image Steganography Techniques	**Description**	**Advantage**
Extension of LSB(Least significant bit)	Compression algorithm is used to maximize storage capacity.	Robust and efficient for hiding text and works efficiently for .bmp images.
Hash-LSB	Uses a hash function to generate a pattern for hiding data bits in LSB.	Hash-LSB with RSA increases the security of secret message
LSB and DCT(Discrete Cosine Transform)	Comparative Analysis of two techniques based on security, PSNR	Peak signal to noise ratio is improved using LSB but security wise DCT is best
Modified LSB	Hides the secret message based on searching about identical bits.	More efficient, simple, Appropriate and accurate.
Combinations of LSB	Hiding the data in LSB bit pairs of pixels and comparison between two bit pairs.	Less visible to human eye that is quality of image is better.
LSB with compression technique	Preprocess data is embedded into the LSBs of the pixels.	High image embedding capacity, sufficient payload and high security
IWT(Integer Wavelet Transform)	Hide multiple secret images and keys in cover image.	High quality of the stego image and having high PSNR values.
LSB replacement	Generate cross platform and use selected pixel value to represent character.	Increase message security and reduce the distortion rate.

Edge Detection	Edges hide the data without altering the quality of image	High embedding capacity and high quality of encoded image.

IX. CONCLUSION

Steganography and steganalysis are important topics in information hiding. Steganography refers to the technology of hiding data into digital media without drawing any suspicion, while steganalysis is the art of detecting the presence of steganography. In this paper, we survey different steganography techniques for encrypting the data. Steganography is a technique that allows the one to hide the data within an image while adding a few noticeable changes. This paper discusses the concept behind the steganography by exploring firstly what are the steganography and the terms that are related to steganography. This paper explores the steganography methods –image steganography, audio steganography, video steganography, text steganography that are used to embed the information in digital carriers.

REFERENCES

[1] Kalaivanan., Ananth. and Manikandan. "A Survey on Digital Image Steganography", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) 2015,

[2] Hemang A . Prajapati1, Dr. Nehal G. Chitaliya," Secured and Robust Dual Image Steganography: A Survey", International Journal of Innovative Research in Computer and Communication Engineering 2015,

[3] Kedar Nath Choudry, Aakash Wanjari, "A Survey Paper on Video Steganography", (IJCSIT) , 2015.

[4] Md. Khalid Imam Rahmani, Kamiya Arora and Naina Pal, "A Crypto-Steganography: A Survey", (IJACSA), 2014.

[5] Mehdi Hussain and Mureed Hussain, "A Survey of Image Steganography Techniques", International Journal of Advanced Science and Technology2013.

[6] Z. V. Patel and S. A. Gadhiya, "A Survey Paper on Steganography and Cryptography", RESEARCH HUB – International Multidisciplinary Research Journal (RHIMRJ), 2015.

[7] Hui Tian, Jie Qin, Yongfeng Huang, Yonghong Chen, Tian Wang, Jin Liu, Yiqiao Cai "Optimal matrix embedding for Voice-over-IP steganography" College of Computer Science and Technology, National Huaqiao University, Xiamen 361021, China

[8] Vidhya P.M,Varghese Paulb, "A Method for Text Steganography Using Malayalam Text" (ICICT 2014)

[9] Milia Habib, Bassem Bakhache, Dalia Battikh, Safwan El Assad "Enhancement using chaos of a Steganography method in DCT domain"

[10] Yugeshwari Kakde, Priyanka Gonnade, Prashant Dahiwale, "Audio-Video steganography" 2015 IEEE

[11] Kamaldeep Joshi, Rajkumar Yadav, "A New LSB-S Image Steganography Method Blend with Cryptography for Secret Communication" 2015 IEEE

[12] Sayantari Ghosh, Saumik Bhattacharya Amity University, Kolkata W.B., India "Hilbert Curve Based Steganographic Scheme for Large Data Hiding", 2015 IEEE

[13] Avinash Tyagi, Ratnakirti Roy, Suvamoy Changder, "High Capacity Image Steganography based on Pixel Value Differencing and Pixel Value Sum" 2015 IEEE

[14] Soon-Nyean Cheong, Huo-Chong Ling, Pei-Lee Teh , "Secure Encrypted Steganography Graphical Password scheme for Near Field Communication smartphone access control system" (2014)

[15] Ifra Bilal, Mahendra Singh Roj, Rajiv Kumar, P K Mishra, "Recent Advancement in Audio Steganography", 2014 IEEE

[16] Md. Rashedul Islam, Ayasha Siddiqa, Md. Palash Uddin, Ashis Kumar Mandal and Md. Delowar Hossain, "An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography" 2014 IEEE

[17] Prabakaran,Dr. Bhavani R , Sankaran S, "Dual Wavelet Transform in Color Image Steganography Method" 2014 International Conference on Electronics and Communication System (ICECS -2014)

[18] Nadeem Akhtar, Shahbaaz Khan, Pragati Johri "An Improved Inverted LSB Image Steganography", 2014 IEEE

[19] P. Thiyagarajan*, G. Aghila, "Reversible dynamic secure steganography for medical image using graph coloring" 2013

[20] Ratnakirti Roy, Anirban Sarkar, Suvamoy Changder, "Chaos based Edge Adaptive Image Steganography" 2013

[21] Susmita Mahato, Dilip Kumar Yadav, Danish Ali Khan, "A Modified Approach to Text Steganography using HyperText Markup Language" 2012 IEEE

[22] Jose Juan Garcia-Hernandez LTI-CINVESTAV "On a Low Complexity Steganographic System for Digital Images Based on Interpolation-Error Expansion" 2013 IEEE

[23] C.L. Philip Chen, Mei-Ching Chen, Sos Agaian, Yicong Zhou, Anuradha Roy, Benjamin M. Rodriguez, "A pattern recognition system for JPEG steganography detection" 2012

[24] D. Biswas, S. Biswas, A. Majumder, D. Sarkar, D. Sinha, A. Chowdhury, S. K. Dasa," Digital Image Steganography using Dithering Technique" 2012

[25] Siddharth Singh and Tanveer J. Siddiqui," Robust Image Steganography Technique Based on Redundant Discrete Wavelet Transform" 2012 IEEE

[26] Ribhu, D. Ghosh, "A Sparse Representation Based Approach for Steganography" 2012 IEEE

[27] Shivani Kundra and Nishi Madaan," A Comparative Study of Image Steganography Techniques", International Journal of Science and Research (IJSR), 2014.