International Journal of Modern Computer Science (IJMCS)
Volume 5, Issue 4, August, 2017

ISSN: 2320-7868 (Online)

# Secure Data Transmission by using Image Steganography: A Study

Bharti Sharma
Research Scholar (Computer Science & Engineering Department)
Vivekananda Global University
Jaipur, India
E-mail: bhartisharmavit@gmail.com

Sachin Sharma, Asst. Prof.
Asst. Prof. (Computer Science & Engineering Department)
Vivekananda Global University
Jaipur, India
E-mail: sachin_sharma@vgu.ac.in

**Abstract:** Internet is a public network that is used to transfer secret data from one place to another place. Data security is a basic need of people who communicate through the internet. Data security means providing security to sensitive data from unauthorized access and intruders. Today lots of technique has been developed to provide secrecy to secret data like cryptography, watermarking, and steganography. Cryptography provides security to secret information by converting plain text into cipher text but it doesn't hide the existence of secret data so intruders can easily detect the secret information. Steganography is an art and science of technology that is used to provide security. Steganography provides more security to the data by hides the existence of secret data so that human eyes can't able to see the hidden information. In steganography technology data is hidden into the cover media like text, image, and audio/video. In this paper, we are giving some views in the development of image steganography. The image steganography technique is selected because it provides good capability for securing information without easily discovering by human visual system.

**Keywords:** Steganography, Cover Media, Image Steganography, Steganography Techniques, Steganography Algorithms.

## I. Introduction

Most of the communication is done over the internet and there are lots of hackers to steal the secret information because information Shas transferred through the public networks. So many applications are running over the internet that affects our everyday lives like Google, Facebook, and Instagram etc. Security of information is a measure concern in the field of information security and communication. Cryptography and Steganography provides security to secret data but cryptography alone was not capable enough for providing secure communication over the internet. To overcome the weakness of cryptography, Steganography technology is widely used to provide secure communication channel. The word steganography is derived from Greek words "Stegos" meaning "Cover" and "graphia" meaning "writing" [1]. Steganography is the science and art of hiding secret data in an appropriate multimedia career like image, audio, and video. The media without hidden information is called cover media and the media with hidden information is called stego-media [2]. In digital steganography images are widely used as a cover media for protecting secret information.

Cover Image
+
Secret Message
=
Stego-Image

**Figure1.** Steganography at Sender side

Stego-Image
=
Cover Image
+
secret Message

**Figure2.** Steganography at Receiver side

The main objective of this paper is to provide an overview about the steganography technique. Section-I briefs about the steganography, cryptography and other data hiding technique. Section-II comprises of how and when steganography came into existence for the first time. Section-3 briefs about the applications of the steganography which shows its increasing importance in today's digital world. Section-4 is all about steganography basic terminology and its types. Section-5 comes with the detailed description of Image steganography for our readers. On the other hand, Section-6 explains the detailed criteria for evaluating the performance of a steganography algorithm. In section 7, the detailed description of the image steganography techniques is given. Finally, Section 8 comes with the conclusion.

## II. Beginning Phase of Steganography Technique

Steganography is used to hide secret data in cover media to provide security from intruders and unauthorized people. The first technique of steganography was developed in ancient Greece around 440 B.C. People used invisible ink to write down the message, and then hide them with wax as a cover media. During the Roman Empire, the secret message was written on slave head. Histiaeus shaved the head of his most trusted slave then write down the message on his shaved head. Wait until the hair grew. The messenger was sent with secret message on his scalp, when he reached to the receiver end his head was shaved again for retrieving the secret message. During the American Revolution, invisible inks were used. Which will glow over the flame, both Americans and British were used this technique for secret communication. Microdots were used in World War II to communicate secretly [3]. All the techniques that are used in ancient times called physical steganography. Today's digital cover media is used to hide secret data.

## III. Applications of Steganography

### A. Secret Communication

The main objective of steganography is to provide secret communication to the person who wants to keep their information secret. Secret communication mean when two people are communicating then third person is unable to view the secret information. In steganography cover media is used to provide secret communication so that unauthorized person should not be able to distinguish between cover media and stego media. The media without secret data is called cover media and the media with secret information is called stego-media [1]. Thus in steganography aims to hide the existence of secret message rather than hiding the communicating parties while cryptography just change the secret message by converting it into cipher text. In cryptography, third party is aware of secret communication taking place between sender and receiver [3]. We can evaluate the efficiency of various steganography techniques by three main criteria: Capacity, Peak-Signal to Noise Ratio (PSNR), Mean Square Rate (MSR) [4]. Now-a-days secret communication is used for both legal and illegal activities. The legal activities aim to keep secret information confidential. The illegal activities shows the secret communication which aim to harm the country. Nowadays steganography is used on computer with internet connection to share secret data over the internet. Various types of steganography are used to hide the secret communication.

### B. Related to Copyright Protection

The term copyright protection refers to Monopoly granted to authors under the 1996 act. Permission is not granted to use those things which are protected by copyright protection. Copyright protection means protecting digital data from being copied [5]. To achieve authenticity and integrity of data several mechanism are used. Data hiding is a technique in which secret information is hidden inside the cover media to provide security. To maintain the original view of the digital image, a watermarking technique can be used to provide copyright protection [6]. ISO and ICE are using digital watermarks embedding technique for copyright protection. The DVD and CD, the web content, the computer forensic department used copyright protection to protect their data from copying [3]. Thus steganography provides confidentiality, and integrity that no other security mechanism may ensure.

## IV. Steganography and Its Types

### A. Steganography

Steganography technique is used to hide secret data inside the carrier object. This technique is in used from ancient time. The term steganography comes from Greece words "Stegos" meaning "covered" and "Grafia" meaning "writing" [1]. Steganography technology provides secrecy of text or image data to prevent them from unauthorized access. Cryptography provides secrecy by converting secret message into cipher but it does not hide the existence of the secret message so that an intruder is able to detect the secret communication. On the other hand steganography hides the existence of secret message by hiding the secret message into the cover media (text, image, and audio/video) so that an attacker and intended hacker are unable to view the existence of secret message. This technology includes a vast array of secret communications methods that conceal the secret information along with the existence. These methods include invisible inks, microdots, character arrangement, digital signatures, covert channels, and spread spectrum [2]. Steganography process is performed by using:

**Cover media**: In which the secret message is hidden.

**Secret message:** This is to be hidden inside the cover media.

**Stego-key:** It is used to hide secret message inside the cover media.

**Stego-media:** The media with the secret information.

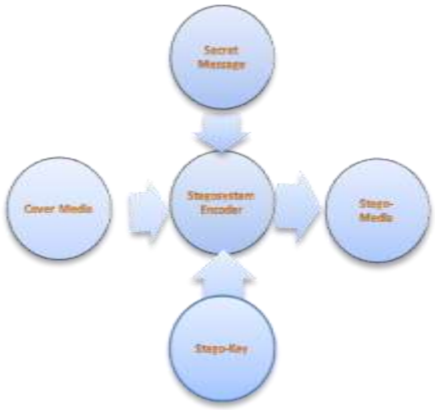

**Figure3.** Inserting the Secret Message into the Cover Media

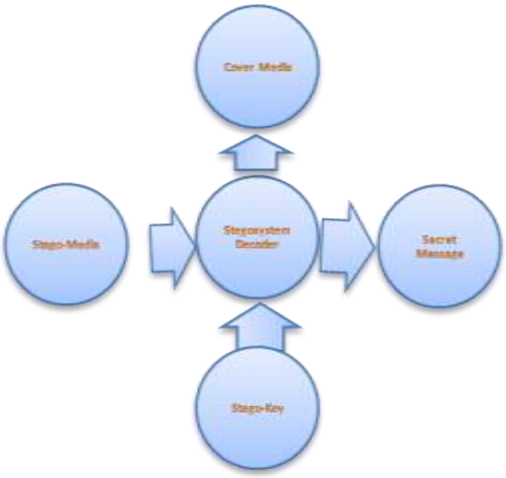

**Figure4.** Extracting the Secret Information from Stego-Media

### B. Types of Steganography

The steganography can be classified into five categories [3, 7]:

1. Text Steganography

In this technique text cover is used as a media to hide secret message behind every nth letter of every word of secret message in text files. The cover text is produces by changing words within a text, generating random character sequences, by changing the formatting of existing text or using context-free Grammar  to hide secret message. But this technique is not good for providing security to sensitive information.

2. *Image Steganography*

In this steganography technique an image is used as a cover media to hide secret message inside the image. This is the most popular steganography technique nowadays, because it provides more secrecy to data. In image steganography method, the secret message is hidden inside the more redundant binary bits of an image. The message embedded image is known as stego-image.

3. *Audio steganography*

In audio steganography technique, an audio is used as a cover media for hiding secret message. It can be performed by using any of the method: Echo Hiding, Phase Coding, Parity Coding, Spread Spectrum, Tone insertion. The secret information is hidden inside the audio files are like: MP3, AU, WAV etc.

4. *Video steganography*

In video steganography technique, the video is used as a cover media for hiding the secret information. A video is considered as a combination of pictures. It can hide any type of message file in a video formats like: MPEG, AVI, MP$, and H264.

5. *Protocol Steganography*

In network or protocol steganography technique, protocols are used as a cover media to provide security to data. The protocols are used like: IP, TCP, ICMP, UDP etc.

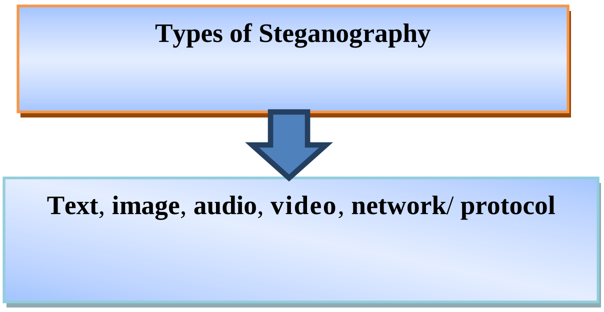

**Figure5.** Types of Steganography

## V. Image Steganography

Image steganography is a technique in which images are used as a cover media to hide secret information within the images so that an attacker and hacker unable to view the secret information by the naked eye. Various techniques can be used to perform image steganography.

### A. Definition of Digital Images

An image is a collection of different light intensities that has been created or copied and stored in electronic form. It can be described in term of raster graphics or vector graphics. There are various image formats used on the internet like .png, .bmp, .jpg, .tiff, .gif. The .bmp images are stored in raster form. The image can be represented in the form of pixels. The smallest item of information is the picture element or pixel that is represented by series of rows and columns [12]. Greyscale images are able to display 256 different shades of grey. Digital images have a number of digital values called pixels. A colored image has three channels: Red, Green, and Blue but the greyscale image has only one channel.

### B. Image Compression

Image compression is a technique that is used to reduce the cost for storage and transmission rate. The compression technique is classified into two categories: lossy compression and lossless compression. Compression algorithms are used to compress the digital images. In lossless image compression technique, the information does not change by compressing an image because only redundant information is removed for increasing the storage capacity while in lossy compression the information is stored in law resolution of an image rather than in actual image [9].

### C. Stego Analytic Threats

The image steganography method is the best method among all the other steganography methods. The humans are unable to view stego image by naked eye but they usually leave behind some type of fingerprint or statistical hint that they have been modified [3]. The attacks are explained as follow [3, 10]:

File only: In this type of attack, an attacker has access to file and easily detect if there is any message hidden inside.

File an original copy: In this type of attack, an attacker has two copies of file. First is the original copy and second is the encoded copy in which the message hidden inside. The attacker will replace the encoded file with original file to destroy the hidden message.

Reformat attack: In this type of attack, an attacker can destroy the hidden message by changing the format of the file. This can be happened because every file format has different ways to store data.

Visual attack: This type of attack is also known as stego-only-attack. In this attack, an attacker can detect the hidden message by displaying the least significant bit of an object.

Statistical attacks: Statistical attacks may be passive or active. Passive attacks mean identifying presence or absence of sensitive information or hiding/embedding algorithm used. On the other hand, active attacks are used to investigate secret message length that is to be hidden or hidden message location or secret key used in embedding.

## VI. Evalution Criteria for Image Steganography

Advantage and disadvantage of technique depends on various features of algorithm, which is used to perform image steganography. But it is not possible that the steganography algorithm fulfill all the specified criteria [3, 11].

### A. Imperceptibility

Perceptual transparency is known as imperceptibility. Data hiding in the cover image leads to some noise distortion. It is important that the hiding the secret information is done without the loss of perceptual quality of the cover image. The stego-image (image with secret message) should be similar to cover-image (image without secret message) that is no visible artifacts on the stego-object. Imperceptibility should be as high as possible.

### B. Robustness

The information that is hidden inside the cover image should be stay intact. For extracting the embedding information, a statistical test will perform on the stego-image by steganalyst. But the steganography algorithm must show robustness against statistical attacks so that an intruder can't able to detect hidden information.

### C. Security

Security means the hidden information should be stay intact after embedding it into the cover image by using steganography algorithms. It has an ability to survive from transformations like adding some noise in transmission, cropping, filtering, signal manipulation, and scaling.

### D. Payload Capacity

Payload capacity refers to the amount of data that can be hidden inside the stego-image. The payload capacity can be represented as a number of bits per pixel. A large amount of information hiding capacity inside the small size cover image decreases the need of large bandwidth for transmitting the stego-image.

### E. Invisibility

A steganography algorithm should provide invisibility feature i.e. an intruder should not be able to view the secret information hidden inside the cover-image.

### F. Computational Complexity

Computational complexity refers to the expenses for embedding and extracting the hidden information.

## VII. TECHNIQUES USED IN IMAGE STEGANOGTAPHY

An image steganography technique can be broadly classifies into two categories:

### A. Spatial Domain Technique

The secret message is directly embedded on the pixel value of the cover image is called spatial domain method. In this method the secret message is embedded inside the cover image in such way that an intruder can't able to view the secret message or we can say that it provides an invisibility feature [3, 13]. The common techniques used in spatial domain are:

1. *Least Significant Technique*

The most technique used today in image steganography is least significant bit insertion technique. The secret message is directly embedded behind the least significant bit of the cover image. This kind of embedding leads to an addition of a noise of 0:5p on average in the pixels of the image where p is the embedding rate in bits/pixel [14]. The secret information is hidden inside the cover image such that it cannot be seen by the human visual system (HVS). An algorithm to embed secret message into cover image using LSB technique is [15]:

- In the first step, read the cover image and secret message that is to be hidden inside the cover image.
- Convert the secret message into binary representation.
- Then calculate least significant bit (LSB) of each pixels of the cover-image.
- Embed each bit of the secret message on least significant bits of the cover image one by one.
- Write stego-image.

2. *Pixel Value Differencing Technique*

Pixel value differencing method is used to provide high embedding capacity and outstanding imperceptibility to the stego-image [7]. It is assume that our human visual system is more sensitive to slight change in the smooth region while can tolerate more severe changes in the edge region so that the PVD technique hides the secret message inside the cover image in such way that the human cannot able to see the hidden information [13]. In PVD technique, the difference between pixel and its neighbor shows the number of embedded bits. When both PVD and LSB technique having same embedding capacity than the PVD technique is more imperceptible than LSB technique [3].

3. *Edge Based Technique*

In the edge detection technique, the secret message is hidden into the three least significant bits (LSBs) of those pixels that make up the extracted edges of the carrier image [3, 13]. Using the edge based technique; any type of information can be hidden inside the cover image, but not in every pixel.

4. *Random Pixel Selection*

Random pixel selection method hides the secret data inside some randomly selected pixel. Random pixels can be generated by using Fibonacci series, pseudo-random generator, and prime-sequence generator [3, 13].

5. *Pixel mapping Method*

PMM method is used to hide secret data within the spatial domain of an image. Embedding pixels are selected based on some mathematical function which depends on the pixel intensity value of the seed pixel and its 8 neighbors are selected in counter clockwise direction. The selected embedding pixels or its neighbors should be between the boundaries of the image. Data embedding are done by mapping each two or four bits of the secret message in each of the neighbor pixel based on some features of that pixel [16].

6. *Pixel Intensity or GLV*

This technique is used to map data within an image not to embed or hide. It is used the concept of even and odd numbers for one to one mapping between binary and pixels (selected by some mathematical function) in an image by modifying the grey level values of these pixels [3, 13].

7. *Histogram Based Technique*

In this technique the data is embedded into the image histogram. Pairs of peak points and zero points are used to achieve low embedding distortion with respect to providing low data hiding capacity [12, 13].

### B. Transform Domain Technique

In transform domain method the secret message does not embed directly into an image. An image is transformed from spatial domain to frequency domain using any of these methods:

DCT (Discrete Cosine Transform)

DFT (Discrete Fourier Transform)
DWT (Discrete Fourier Transform)
IWT (Integer Wavelet Transform)
DCVT (Discrete Curvelet Transform)

1. *DCT (Discrete Cosine Transform)*

The DCT transforms an image from spatial domain to frequency domain. This method uses JPEG compression algorithm to convert 8X8-pixel blocks in special domain to 64 DCT coefficients. Discrete cosine transform technique allows image to be broken into frequency bands: High band, Middle band, Low band. The main advantage of this technique is that it provides an invisibility feature. And main disadvantage is that it works only on JPEG files [17].

2. *DFT (Discrete Fourier Transform)*

In DFT technique, Fourier transformation is used to transfer an image from spatial domain to frequency domain instead of cosine transform. This technique is complex and provide low invisibility feature.

3. *DWT (Discrete Wavelet Transform)*

In discrete wavelet transform technique, analysis filter is used to obtain DWT of an image. Wavelets are used to transform an image from spatial domain to frequency domain. DWT is a computationally efficient technique in computer science. It is used to perform local analysis and multi resolution analysis (analyze a signal at different frequencies and different resolution). Discrete wavelet transform technique is applied on image to obtain 4-sub bands: LL (low-low frequency band), LH (low-high frequency band), HL (high-low frequency band), and HH (high-high frequency band). Inverse wavelet transform is performed to obtain the original format of stego-image [18].

4. *IWT (Integer Wavelet Transform)*

IWT (Integer wavelet transform) is used to hide keys because using the key secret message can be extracted. To protect secret message from unauthorized access IWT is used [19]. Discrete wavelet transform allows independent processing of the resulting signals. Wavelet filters have floating point coefficients, thus when an input image consist of sequence of integer, the resulting filtered output no longer consist of integer. In this case the resulting image is not similar to the original image. Integer wavelet transform is used to provide perfect reconstruction of an original image. In this technique the resulting output completely characterized with integer. In the case of IWT, the LL sub band appears to be a close copy to the original image. While in DWT the LL sub band is distorted.

5. *DCTV (Discrete Curvelet Transform)*

Discrete wavelet transform represents edges better then wavelet. This technique is used to overcome the problems associated with the DCT (discrete cosines transform) and wavelets.

## VIII. Conclusion

This paper gives an overview about steganography techniques from the basic system to recent approaches. Also gives evaluation criteria by which we can decide which steganography technique is best to hide secret data. Different technique to embed secret information into the cover image has also been explained to the reader. Image steganography technique is best from the all other technique to hide data because it has a high invisibility factor. The analysis shows that the transform domain techniques are best for the attack resilient system with relatively lower data capacity and higher complexity while the spatial domain is best for limited complexity systems and also provides greater options for techniques selection for the systems with limited computational power.

## REFERENCES

[1] Rig Das, Thamrichon Tuithung, "A Novel steganography Method for Image Based on Huffman Encoding", IEEE, 978-1-4577-0748-3, 2012.

[2] Nadeem Akhtar, Pragati Johri, Shahbaaz Khan, "Enhancing the Security and Quality of LSB based Image Steganography", 5th International Conference on Computational Intelligence and Communication Networks IEEE, 978-0-7695-5069-5, 2013.

[3] Rupali Jain, Jaishree Boaddh, "Advances in Digital Image Steganography", 1st International Conference on Innovation and Challenges in Cyber Security, IEEE, 978-1-5090-2084-3, 2016.

[4] Hamad A. Al-Korbi, Ali Al-Ataby, Majid A. Al-Taee, Waleed Al-Nuaimy, "High-Capacity Image Steganography Based on Haar DWT for Hiding Miscellaneous Data", IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies, 978-1-4799-7431 3, 2013.

[5] https://en.wikipedia.org/wiki/Copyright_protection.

[6] Sanchit Mahajan, "Improved Copyright Image Protection using Steganography Technique", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 4, Issue 2, February 2016.

[7] Navneet Kaur, Sunny Behal,"A Survey on various types of Steganography and Analysis of Hiding Techniques", International Journal of Engineering Trends and Technology, Volume 11 Number 8 - May 2014.

[8] Kshetrimayum Jenita Devi of Department of Computer Science and Engineering National Institute of Technology-Rourkela Odisha, "A Secure Image Steganography Using LSB Technique and Pseudo Random Encoding Technique", 2013, pg. No. 6-7.

[9] https://en.wikipedia.org/wiki/Image_compression.

[10] Nikhil Patel, Shweta Meena, "LSB based Image Steganography using Dynamic Key Cryptography".

[11] S.Nandakishor, Dr.G.N.Kodanda Ramaiah, Dr.S.A.K.Jilani, "A REVIEW ON STEGANOGRAPHY THROUGH MULTIMEDIA", IEEE, International Conference on Research Advances in Integrated Navigation System, 2016.

[12] Yildiray Yalman, Feyzi Akar, Ismail Erturk, "Contemporary Approaches to the Histogram Modification Based Data Hiding Techniques" in 2012.

[13] Anjali Tiwari, Seema Rani Yadav, N.K. Mittal, "A Review on Different Image Steganography Techniques", International Journal of Engineering and Innovative Technology (IJEIT), ISSN: 2277-3754, ISO 9001:2008 Certified, Volume 3, Issue 7, January 2014.

[14] G.S.Sravanthi, B.Sunitha Devi, S.M.Riyazoddin & M.Janga Reddy, "A Spatial Domain Image Steganography Technique Based on Plane Bit Substitution Method", Global Journal of Computer

Science and Technology Graphics & Vision, ISSN: 0975-4172, Volume 12 Issue 15 Version 1.0 Year 2012.

[15] K.Thangadurai and G.Sudha Devi, "An analysis of LSB Based Image Steganography Techniques", IEEE, International Conference on Computer Communication and Informatics (ICCCI), 978-1-4799-2352, 2014.

[16] Souvik Bhattacharyya, Gautam Sanyal, "Study and analysis of quality of service in different image based steganography using Pixel Mapping Method (PMM)", International Journal of Applied Information Systems (IJAIS) – ISSN: 2249-0868, Volume 2– No.7, May 2012.

[17] Nadiya P v, B Mohammed lmran, "Image Steganography in DWT Domain using Double staging with RSA Encryption", IEEE International Conference on Signal Processing, Image Processing and Pattern Recognition [icsiprj], 978-1-4673-4862-1, 2013.

[18] Martin Baroda, Vladimir Hajduk, and Dusan Levicky, "Image Steganography Based on Combination of $_{\text{YCBCR}}$ Color Model and DWT", 56th International Symposium ELMAR, 28-30 September 2015.

[19] Hemalatha S., U Dinesh Acharya, Renuka A., and Priya R. Kamath, "An Integer Wavelet Transform Based Steganography Technique for Color Images", International Journal of Information & Computation Technology. ISSN 0974-2239 Volume 3, Number 1, pp. 13 24, 2013.

## BIOGRAPHY

**Bharti Sharma** was born in Jaipur, India, in 1992. She received her B.Tech degree in computer science engineering from the Vivekananda institute of technology, Jaipur, India, in 2014. Now she is a research scholar in the department of computer science & engineering at Vivekananda global university, Jaipur, India. Her 2017 paper, "Combined Technique of Cryptography and Steganography to provide Double Security", published in the Imperial Journal of Interdisciplinary Research (IJIR).

**Sachin Sharma** was born in Jaipur, India, in 1987. He received his B.E degree in computer science engineering from the Rajasthan University, Jaipur, India, in 2007 and the M.Tech degree in computer science engineering from Jagannath University, Jaipur, India, in 2014.
In 2016, he joined the department of computer science & engineering at Vivekananda global university as assistant professor and also works as Cyber Security researcher at free lancing. He has published 4 research papers in international journal and 12 research papers in national journal.