INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

Review on Various Image Steganographic Techniques

Amrit Preet Kaur[1], Gagandeep Singh[2]

[1]M.Tech Scholar, Chandigarh Engineering College,
Department of CSE, Landran, India,
kaur.amritpreet13@gmail
[2]Assistant Professor, Chandigarh Engineering College,
Department of CSE, Landran, India

Abstract: *Detection of hidden data in cover images by means of steganography is termed as image steganalysis. All steganalytic methods can be classified as blind or targeted. The objective of a targeted steganalytic method is to detect stego images that are created by a specific steganographic algorithm, where as in case of a blind steganalytic method the detection is independent of the steganographic algorithm used and is usually based on a machine learning classifier trained with high-dimensional features. In order to improve security and processing speed, more and more new image steganographic algorithms become content-adaptive. Advanced content-adaptive steganographic methods pose great challenge to steganalyzers, especially to the feature-based blind steganalyzers. In this paper various steganographic techniques are reviewed.*

Keywords: *Steganography, Steganalysis, Image, Terminology, cryptography, Stego-image.*

1. INTRODUCTION

Nowadays people are becoming more and more concerned about the security of private information transmitted over the Internet. Protecting the private information from being attacked is regarded as one of the major problems in the field of information security. In today's world, the communication is the basic necessity of every growing area [1].

Everyone wants the secrecy and safety of their communicating data. In our daily life, we use many secure pathways like internet or telephone for transferring and sharing information, but it's not safe at a certain level. In order to share the information in a concealed manner two techniques could be used. These mechanisms are cryptography and steganography. In cryptography, the message is modified in an encrypted form with the help of encryption key which is known to sender and receiver only [3]. The message cannot be accessed by anyone without using the encryption key. However, the transmission of encrypted message may easily arouse attacker's suspicion, and the encrypted message may thus be intercepted, attacked or decrypted violently. In order to overcome the shortcomings of cryptographic techniques, steganography techniques have been developed.

Steganography is a Greek word which means concealed writing. The word "stegano" means "covered "and "graphical"means "writing" [7]. Apart from encryption, digital steganography has been one of the solutions to protecting data transmission over the network. Steganography is the science of covert communications that conceal the existence of secret information embedded in cover media over an insecure network. A broad definition of steganography includes all endeavors to communicate in such a way that the existence of the message cannot be detected.

The medium used to carry the message is called the cover. Stego media should look natural, but carries secret messages innocuously. Thus, stego media should be indistinguishable from the plain cover media having no secret message. Image steganalysis is the art of detecting data hidden in cover images by means of steganography.

The general block diagram of steganography is given below in the figure. 1.

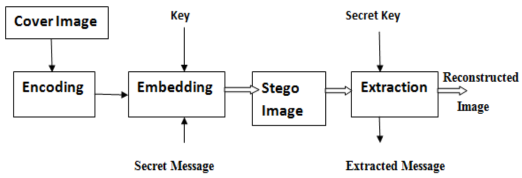

Figure 1: General block diagram of steganography.

2. STEGANOGRAHY HISTORY

Information hiding is a science which dates back to 1499, and it has long history. It has been used in various forms for 2500 years. It has found use in military, diplomatic, personal, spies, ruler, governments etc. Steganography has been widely used, including in recent historical times and the present day [4]. Some known examples include:

2.1 Past

Early steganography was messy. Before phones, before mail, before horses, messages were sent on foot. If you wanted to hide a message, you had two choices: have the messenger memorize it, or hide it on the messenger. While information hiding techniques have received a tremendous attention recently, its application goes back to Greek times [4]. According to Greek historian Herodotus, the famous Greek tyrant Histiaeus, while in prison, used unusual method to send message to his sonin- law. He shaved the head of a slave to tattoo a message on his scalp. Histiaeus then waited until the hair grew back on slave's head prior to sending him off to his son-in-law. Herodotus provides the first records of steganography in Greece.

- To communicate Greeks would etch the message they wished to send into the wax.
- Coating of a wooden tablet. The tablet would then be transported to the recipient who would read the message, then re-melt the wax to etch their reply. In order to communicate in secret, the army would remove the wax

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

completely, carve the secret message into the wood, and re-coat the tablet with wax.
- Messages were also written on envelopes in the area covered by postage stamps to avoid the possible detection of the message.

2.2 Present
In today's generation, as most of the people often transmit images, audio over the internet, so most of the Steganographic system's uses multimedia objects like image, audio and video as cover sources to hide the confidential data[4]. So, on the basis of this, steganography is divided into four categories:
1. Text Steganography
2. Image Steganography
3. Audio/Video Steganography
4. Protocol Steganography

2.3 Future
Steganalysis can be defined as process to crack the cover object in order to get the hidden data. In general terms, it is known as hacking i.e. unauthorized access of data during transmission. Future perspective of steganography lies on combining steganography with cryptography to achieve a higher level of security such that even if intruder detects the hidden message, he/she will not be able to decode it.

3. TYPES OF STEGANOGRAPHY
The types of steganography are shown below in the fig 2.

3.1. Text Steganography: It consists of hiding information inside the text files. In this method, the secret data is hidden behind every nth letter of every words of text message. Numbers of methods are available for hiding data in text file. These methods are i) Format Based Method; ii) Random and Statistical Method; iii) Linguistics Method [3], [5].

3.2. Image Steganography: Hiding the data by taking the cover object as image is referred as image steganography. In image steganography pixel intensities are used to hide the data. In digital steganography, images are widely used cover source because there are number of bits presents in digital representation of an image.

3.3. Audio Steganography: It involves hiding data in audio files. This method hides the data in WAV, AU and MP3 sound files. There are different methods of audio steganography. These methods are i) Low Bit Encoding ii) Phase Coding iii) Spread Spectrum.

3.4. Video Steganography: It is a technique of hiding any kind of files or data into digital video format. In this case video (combination of pictures) is used as carrier for hiding the data. Generally discrete cosine transform (DCT) alter the values (e.g., 8.667 to 9) which is used to hide the data in each of the images in the video, which is unnoticeable by the human eye. H.264, Mp4, MPEG, AVI are the formats used by video steganography.

3.5. Network or Protocol Steganography: It involves hiding the information by taking the network protocol such as TCP, UDP, ICMP, IP etc, as cover object. . In the OSI layer network model there exist covert channels where steganography can be used.

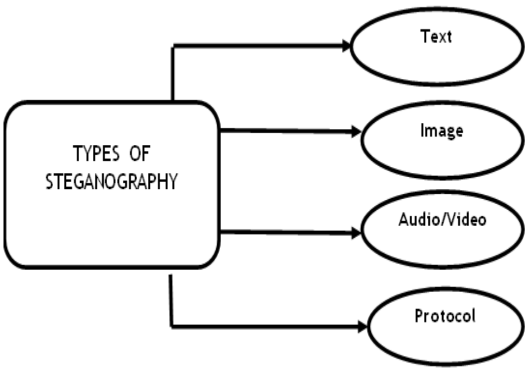

Figure 2: Stegnography types

4. STEGANOGRAPHY TERMINOLOGY
Steganography consists of two terms that is message and cover image. Message is the secret data that needs to hide and cover image is the carrier that hides the message in it. The stegnography diagram is given below in the figure.3.

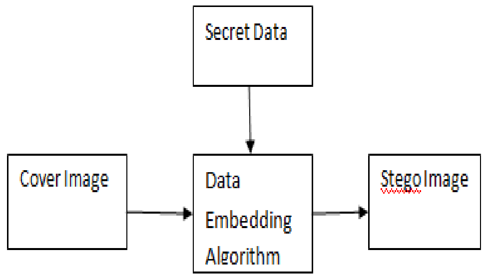

Figure 3: Steganography diagram.

5. METHODS OF CONCEALING DETAIN DIGITAL IMAGE
Steganography is used for covert communication. The secret image which is communicated to the destination is embedded into the cover image to derive the stego image. In this section evaluation parameters and proposed embedding and retrieval techniques are discussed [8].

a) Least significant bit substitution technique (LSB): In LSB steganography, the least significant bits of the cover media's digital data are used to conceal the message. The simplest of the LSB steganography techniques is LSB replacement. LSB replacement steganography flips the last bit of each of the data values to reflect the message that needs to be hidden. Consider an 8-bitgrayscale bitmap image where each pixel is stored as a byte representing a gray scale value [8].

Algorithm to embed text message:-
Step 1: Read the cover image and text message which is to be hidden in the cover image.

Step 2: Convert text message in binary.
Step 3: Calculate LSB of each pixels of cover image.
Step 4: Replace LSB of cover image with each bit of secret message one by one.
Step 5: Write stego image.
Step 6: Calculate the Mean square Error (MSE), Peak signal to noise ratio (PSNR) of the stego mage.

Algorithm to retrieve text message:-
Step 1: Read the stego image.
Step 2: Calculate LSB of each pixels of stego image.
Step 3: Retrieve bits and convert each 8 bit into character.

Advantages of LSB
1. Less suspicious to human eyes.
2. Simple to implement and many techniques uses this method.
3. High perceptual transparency [2].

Disadvantages of LSB
1. Three weakness- Robustness, Tamper and Resistance.
2. Extremely sensitive to any kind of filtering.
3. Scaling, Rotation, Cropping, adding extra noise lead to destroy the secret message [2].

b) Discrete Cosine Transform Technique (DCT): DCT coefficients are used for JPEG compression. It separates the image into parts of differing importance. It transforms a signal or image from the spatial domain to the frequency domain. It can separate the image into high, middle and low frequency components [8].

Algorithm to embed text message:-
Step 1: Read cover image.
Step 2: Read secret message and convert it in binary.
Step 3: The cover image is broken into 8×8 block of pixels.
Step 4: Working from left to right, top to bottom subtract 128 in each block of pixels.
Step 5: DCT is applied to each block.
Step 6: Each block is compressed through quantization table.
Step 7: Calculate LSB of each DC coefficient and replace with each bit of secret message.
Step 8: Write stego image.
Step 9: Calculate the Mean square Error (MSE), Peak signal to noise ratio (PSNR) of the stego image.

Algorithm to retrieve text message:-
Step 1: Read stego image.
Step 2: Stego image is broken into 8×8 block of pixels.
Step 3: Working from left to right, top to bottom subtract 128 in each block of pixels.
Step 4: DCT is applied to each block.
Step 5: Each block is compressed through quantization table.
Step 6: Calculate LSB of each DC coefficient.
Step 7: Retrieve and convert each 8 bit into character.

c) Discrete Wavelet Transform Technique (DWT)
The frequency domain transform we applied in this research is Haar-DWT, the simplest DWT. A 2-dimensional Haar-DWT consists of two operations: One is the horizontal operation and the other is the vertical one[8].

Algorithm to embed text message:-
Step 1: Read the cover image and text message which is to be hidden in the cover image.
Step 2: Convert the text message into binary. Apply 2DHaar transform on the cover image.
Step 3: Obtain the horizontal and vertical filtering coefficients of the cover image. Cover image is Added with data bits for DWT coefficients.
Step 4: Obtain stego image.
Step 5: Calculate the Mean square Error (MSE), Peak signal to noise ratio (PSNR) of the stego image.

Algorithm to retrieve text message:-
Step 1: Read the stego image.
Step 2: Obtain the horizontal and vertical filtering coefficients of the cover image. Extract the message bit by bit and recomposing the cover image.
Step 3: Convert the data into message vector. Compare it with original message.

6. FACTORS AFFECTING A STEGANOGRAPHIC METHOD

The effectiveness of any steganographic method can be determined by comparing stego-image with the cover Image [3]. There are some factors that determine the efficiency of a technique. These factors are:

1) Robustness: Robustness refers to the ability of embedded data to remain intact if the stego- image undergoes transformations, such as linear and non-linear filtering, sharpening or blurring, addition of random noise, rotations and scaling, cropping or decimation, lossy compression.

2) Imperceptibility: The imperceptibility means invisibility of a steganographic algorithm. Because it is the first and foremost requirement, since the strength of steganography lies in its ability to be unnoticed by the human eye [6].

3) Payload Capacity: It refers to the amount of secret information that can be hidden in the cover source. Watermarking usually embed only a small amount of copyright information, whereas, steganography focus at hidden communication and therefore have sufficient embedding capacity.

4) PSNR (Peak Signal to Noise Ratio): It is defined as the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. This ratio measures the quality between the original and a compressed image. The higher value of PSNR represents the better quality of the compressed image.
5) MSE (Mean Square Error): It is defined as the average squared difference between a reference image and a distorted image. The smaller the MSE, the more efficient the image steganography technique. MSE is computed pixel-by-pixel by adding up the squared differences of all the pixels and dividing by the total pixel count.

6) SNR (Signal to Noise Ratio): It is the ratio between the signal power and the noise power. It compares the level of a desired signal to the level of background noise.

7. APPLICATIONS OF STEGANOGRAPHY

There are various applications in steganography; it varies among the user requirements such as copyright control, covert communication, smart ID's, printers etc [2], [5].

Copyright Control: Inside an image, secret copyright information is embedded. This is achieved by Water marking which a complex structure is so that the intruder cannot identify the copyright information. There are various methods available to find the watermarking. It is achieved by statistical, correlation, similarity check. Watermarking is used to protect the copyright information.

Covert Communication: In general covert channel passes information by non-standard methods. Communication is obscured that is unnoticed. The aim of the covert communication is to hide the fact that the communication is being occurred. Covert communication ensures privacy. Steganography is one of the best techniques of covert communication [5]

Smart Id's: In smart ID's the information about the person is embedded into their image for confidential information. For an organization, the authentication of the resources is accessed by the people. So identifying the theft related to prevention of crimes.

Printers: Steganography make use of some modern printers like HP printer etc. In those printers, very small yellow dots are inserted into all pages. Information is hidden inside the yellow dots like serial number, date and time stamp. Property is available in laser printer for watermarking the confidential information [5].

Digital Watermark: A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal.

Use by terrorists: Steganography on a large scale used by terrorists, who hide their secret messages in innocent, cover sources to spread terrorism across the country. It come in concern that terrorists using steganography when the two articles titled "Terrorist instructions hidden online" and "Terror groups hide behind Web encryption" were published in newspaper.

Feature Tagging: Captions, annotations, time stamps, and other descriptive elements can be embedded inside an image, such as the names of individuals in a photo or locations in a map. Copying the stego-image also copies all of the embedded features and only parties who possess the decoding stego-key will be able to extract and view the features.

Secret Communications: In many situations, transmitting a cryptographic message draws unwanted attention. The use of cryptographic technology may be restricted or forbidden by law. However, the use of stenography does not advertise covert communication and therefore avoids scrutiny of the sender, message, and recipient. A trade secret, blueprint, or other sensitive I formation can be transmitted without alerting potential attackers or eavesdroppers.

8. STEGANALYSIS TOOLS

Various tools are available for steganalysis.

Digital invisible tool kit: It is a java based steganography tool capable of hiding information in a 24 bit color image. This tool also performs statistical analysis.

Steganography analyzer signature scanning (StegAlyzerSS): This tool efficiently scans the existence of hexadecimal byte patterns in a Stego File

.

Steganography analyzer artifact scanner (StegAlyzerAS): StegAlyzerAS scans a file system as a whole or a single file system on a Stego file for the existence of the embedded information in the Stego File.

Invisible Secret tool: This tool is not only encrypt the message but also used for secure transformation over the internet. Using Invisible Secret tool not evens the hackers or intruders came to know the embedded information in the Stego File. In this paper Invisible Secret tool is analyzed:
Step1: Select Action
Step2: Select Carrier File
Step3: Select Source File
Step4: Encryption Settings
Step5: Target File Settings
Step6: Encryption or Hiding

9. CONCLUSION

This paper reviewed the main steganographic techniques. Each of these techniques tries to satisfy the three most important factors of steganographic design (imperceptibility or undetectability, capacity, and robustness). LSB techniques in a spatial domain have a high payload capacity, but they often fail to prevent statistical attacks and are thus easily detected. The Paper gives the review of Steganography, its history and basic working of Image Steganography along with various insertion techniques used in Image Steganography, such as Spatial Domain Methods, Transform Domain Technique, Distortion Technique Masking and Filtering.

FUTURE SCOPE

From the above literature survey, it can be concluded that there are many challenges regarding in designing a steganalytic system like processing time, complexity and security. Various kinds so security model can be designed in accordance with type of data to be encrypted. Also, one of the major issues to be considered is the computational speed of the steganographic model. Existing techniques are not as susceptible to cropping, compression, etc. But, they also increase the total cost of the system because computational time of the algorithms have a major impact on the determining the cost effectiveness and efficiency of the system. So, authors need a better technique which must provide high level security, cost effective, lesser computational time, higher computational speed and high efficiency. Also, the text which will be ciphered by this method must not be broken.

Acknowledgement

The authors would like to thanks to the earlier work regarding different Steganography methods that contribute the work made in this paper. All work done in this paper will surely help to the researchers for future work on Steganography methods.

REFERENCES

[1] Shikha Sharda & Sumit Budhiraja "Image Steganography: A Review" International Journal of Emerging Technology and Advanced Engineering. Volume 3, Issue 1, January 2013) pp 707-710.

[2] R.Poornima and R.J.Iswarya "AN OVERVIEW OF DIGITAL IMAGE STEGANOGRAPHY" International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.1,February 2013.pp 23-31.

[3] Jasleen Kour and Deepankar Verma "Steganography Techniques –A Review Paper" International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-3, Issue-5)May 2014. Pp.132-135.

[4] Gunjan CHUGH "Image Stegnography Techniques: A Review Article" ACTA TECHNICA CORVINIESIS-Bulletin of engineering Tome VI July-September 2013.ISSN 2067-3809.pp 97-104.

[5] Rashi Singh and Gaurav Chawla "A Review on Image Steganography". International Journal of Advanced Research in Computer Science and Software Engineering.Volume 4, Issue 5, May 2014 ISSN: 2277 128X.pp 686-689.

[6] Babloo Saha and Shuchi Sharma "Steganographic Techniques of Data Hiding using Digital Images" Defence Science Journal, Vol. 62, No. 1, January 2012, pp. 11-18, DOI: 10.14429/dsj.62.1436 2012, DESIDOC.

[7] Rakhi and Suresh Gawande "A REVIEW ON STEGANOGRAPHY METHODS". International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (An ISO 3297: 2007 Certified Organization) Vol. 2, Issue 10, October 2013.pp 4635-4638.

[8] Stuti Goel, Arun Rana & Manpreet Kaur. "A Review of Comparison Techniques of Image Steganography". Global Journal of Computer Science and Technology Graphics & Vision Volume 13 Issue 4 Version 1.0 Year 2013