e-ISSN : 2349-9745
p-ISSN : 2393-8161
Scientific Journal Impact Factor (SJIF): 1.711
International Journal of Modern Trends in Engineering and Research
www.ijmter.com

Steganography : A Brief Survey

Khusbu J. Panchal[1], Falguni N. Patel[2]
[1]*M.E Student ,Computer Engineering(IT System and Network Security),Sardar Vallabhbhai Patel Institute of Technology,vasad*
[2]*Assistant Professor,Computer Engineering,Sardar Vallabhbhai Patel Institute of Technology,vasad*

Abstract - Steganography is going to gain its importance due to the exponential growth computer users and for secret communication over the internet. It is defined as hiding a message in such a way that no one apart from receipt knows the existence of data. In this paper we have first explained concept. We have also discussed different methods of steganography.In addition, we discuss steganography techniques and try to mention advantages and disadvantages of them.
Keyword - Steganography, Data hiding, LSB, DCT,PSNR

I. INTRODUCTION

In today's world the communication is the basic necessary of every growing area. Everyone wants their communication secure. Secret communication is required for business and military purposes. The word steganography comes from greek word steganos which means covered or secret and the graphy means writing or drawing[7]. Generally steganography is the art of hiding a message or data in cover. Cryptography provides confidentiality and steganography hide the message. Steganography do not alter the message but hide message inside cover object. It is the science that involves communicating secret data in an appropriate multimedia carrier e.g., image, audio, video files.

II. TYPES OF STEGANOGRAPHY

Depend on type of cover object there are many steganographic type which are follow:

A. Image Steganography:

Image are the most suitable carrier type for steganography. In image steganography pixel intensities are used to hide data.

B. Text Steganography:

It consists of hiding information inside the text files. The method was to hide a secret messagein every nth letter of every word of a text message.

C. Audio Steganography:

In this hide information in an audio file. This method hide data in AU, WAV and MP3 file.

D. Video Steganography:

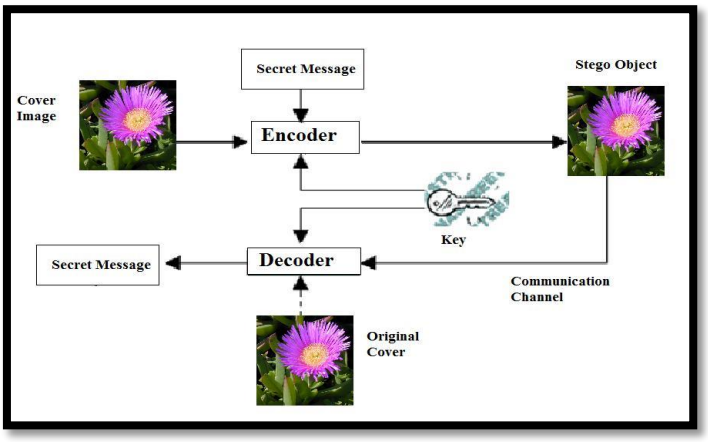
It hides any kind of file into digital video format. The use of the video steganography can be more eligible than other multimedia files.

E. Protocol Steganography:

It involves hiding information by taking the network protocol such as TCP, UDP, IP etc. In the OSI network layer model there exist covert channels where steganography can be achieved in unused header bits of TCP/IP fields[1].

III. BASIC TERMINOLOGIES

Message: Information which is used to hide. It is plain text or other image.
Cover-Object: It refers to the object used as a carrier to embed message into.
Stego-object: Object which carrying a hidden message.
Stego-key: A key refers to a password used to hide and later retrieval of message.
Embedding algorithm: An algorithm used to hide the message.
Extracting algorithm: An algorithm used to unhide/uncover the message.



"Fig 1. Work Flow of Steganography"

Information is hiding into cover-image and generates a stego-image. This stego-image then sent to the other party. After receiving stego-image hidden message can simply be extracted with or without stego-key by the receiving end[3].

IV. IMAGE STEGANOGRAPHY TECHNIQUES

A. Spatial Domain Technique:

It directly change some bits in image pixel value. Least Significant Bit(LSB) based steganography is one of the simplest technique that hides a secret data in the LSB of pixel values without any distortion. To human eye, changes in the value of the LSB are imperceptible. Least Significant Bit (LSB) replacement, LSB matching, Matrix embedding and Pixel value differencing are some of the spatial domain technique[6]. This method embeds the fixed-length secret bits in the same fixed length LSBs of pixels[2].

Advantages of LSB technique:

1) Less chance for degradation of original image.
2) More information can be stored in image.

Disadvantages of LSB technique:

1) Less robust.
2) Hidden data can be easily destroyed by simple attacks.

B. Transform Domain Technique

It is more complex way of hiding information in image. Various algorithms and transformation are used on image to hide information. Most of the strong steganographic system today operate within transform domain.

It is classified into:

- Discrete Fourier transformation technique (DFT).
- Discrete cosine transformation technique (DCT).
- Discrete Wavelet transformation technique (DWT).

Advantages of Transform Domain technique:

1) They hide information in areas of the image that are less exposed to cropping and image processing.

C. Distortion Technique

Distortion techniques need knowledge of the original cover image during the decoding process where the decoder functions to check for differences between the original cover image and the distorted cover image in order to restore the secret message. Using this technique, a stego object is created by applying a sequence of modifications to the cover image. If the stego-image is different from the cover image at the given message pixel, the message bit is a "1." otherwise, the message bit is a "0." The encoder can modify the "1" value pixels in such a manner that the statistical properties of the image are not affected.

D. Masking and Filtering

These techniques hide information by marking an image, in the same way as to paper watermarks. These techniques embed the information in the more significant areas than just hiding it into the noise level. The hidden message is more integral to the cover image.

Advantages of Masking and Filtering technique:

1) More Robust.

Disadvantages of Masking and Filtering technique:

1) It applied only gray scale image and restricted to 24 bits.

V. APPLICATION OF STEGANOGRAPHY

- In the business world audio data hiding, video data hiding and text data hiding can be used as a secret chemical formula or plans for a new invention. Audio data hiding can also be used in corporate world. Terrorists can also use audio data hiding to keep their communications secret and to co-ordinate attacks.
- Data hiding in video and audio is of interest for the protection of copyrighted digital media and to the government for information system security and for covert communication.
- It can also be used in forensic application for inserting hidden data in to audio files for the authentication of spoken words and other sounds and in the music business for the monitoring of the songs over broadcast radio.
- For contracting firms, sending an authentic bedding letter with authorization signature and date, hand-written.
- In the stock market, to authorize the buying or selling of stocks.

VI. CONCLUSION

This paper gave an overview of different steganographic technique its type an advantage and disadvantages. The main goal of steganography is to communicate securely in completelu undetectable manner and to avoid drawing suspicion to the transmission of a hidden data.

Spatial-domain least significant bit(LSB) substitution is one of the classic image steganography approaches. The LSB steganographic method is the simplest one and is widely used in the field of information security due to its high hiding capacity and quality.

REFERENCES

[1]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

[2]Sara Natanj and Seyed Reza Taghizadeh ”Current Steganography Approaches: A survey” International Journal of Advanced research in computer science and software engineering, ISSN:2277-128X Volume-1, Issue-1, December 2011

[3]Mehdi Hussain and Mureed Hussain “A Survey of Image Steganography Techniques” International Journal of Advanced Science and Technology Volume-54, May 2013

[4]Falesh M. Shelke, Ashwini A. Dongre and Pravin D. Soni “Comparison of Different Techniques for steganography in images” International journal of Application or Innovation in engineering & management, ISSN:2319-4847, Volume-3, Issue-2, February 2014

[5]M. Pavani, S. Naganjaneyulu and C.Nagaraju“A Survey on LSB Based Steganography Methods” International Journal Of Engineering And Computer Science, ISSN:2319-7242 Volume-2 Issue -8 August, 2013

[6]Chandra Prakash Shukla and Ramneet S. Chadha “A Survey of Steganography Technique, Attacks and Applications” International Journal of Advanced research in computer science and software engineering, ISSN:2277-128X Volume-4, Issue-2, February 2014

[7]Mukesh Garg and A.P.Gurudev Jangra “An Overview of Different Type of Data Hiding Scheme in Image using Steganographic Techniques” International Journal of Advanced research in computer science and software engineering, ISSN:2277-128X Volume-4, Issue-1, January 2014

[8]Amit Asthana and Sherish Johri “An Adaptive Steganography Technique for Gray and Colored Images” International Journal of Advanced research in computer science and software engineering, ISSN:2277-128X Volume-2, Issue-5, May 2012

[9]Prabhsimran Singh and Nitish Salwan "A Brief Study of Steganography on Different Cover Media's Using LSB Substitution Method" International Journal of Advanced research in computer science and software engineering, ISSN:2277-128X Volume-4, Issue-5, May 2014
[10]Mrs. Kavitha, Kavita Kadam, Ashwini Koshti and Priya Dunghav "Steganography Using Least Signicant Bit Algorithm" International Journal of Engineering and Applications, ISSN:2248-9622 Volume-2, Issue-3, May-June 2012
[11]Shang-kuan chen "A Module-based LSB Substitute Method with lossless secret data compression" ScienceDirect, January 2011
[12] S. M. Masud Karim, Md. Saifur Rahman, and Md. Ismail Hossain "A New Approach for LSB Based Image Steganography using Secret Key" International Conference on Computer and Information Technology (ICCIT 2011) 22-24 December, 2011

[13]Manu Devi and Nidhi Sharma "Improved Detection of Least Significant Bit Steganography Algorithms in Color and Gray Scale Images"IEEE March 2014

[14]Alina-Felicia Dragan "Another Steganographic LSB-based Function" IEEE 2012

[15]Rajib Biswas, Sayantan Mukherjee and Sayantan Mukherjee "DCT Domain Encryption in LSB Steganography" International Conference on Computational Intelligence and Communication Networks,IEEE 2013

[16] Prabakaran G, Dr. Bhavani R and Sankaran S "Dual Wavelet Transform Used in Color Image Steganography Method" International Conference on Intelligent Computing Applications,IEEE 2014
[17] NehaGupta and Ms. Nidhi Sharma "Dwt and Lsb Based Audio Steganography" International Conference on Reliability, Optimization and Information Technology -ICROIT 2014

