Study on Image Steganography Techniques

C.Gayathri [#1], V.Kalpana[#2]
Computer Science & Engineering, School of Computing,
SASTRAUNIVERSITY, Tirumalaisamudram,
Thanjavur - 613401.Tamilnadu, India
[1] infotechgayathri@gmail.com
[2]kalpana@cse.sastra.edu

Abstract- **Steganography is a secret Communication to hide the secret Data. It is an invisible communication that hides data like text, image, and audio, video etc .The secret message is inserted into the image files. The image files can use stego-key to hide the data and the resultant image is called as stego-image. This is most important for the internet users to share their secret data in an efficient manner. Steganography plays an important role in defence. Various steganographic techniques are analyzed and its pros and cons are highlighted in this paper.**

Key Words: Data hiding, Security, Pay load capacity, Image Distortion.

I.INTRODUCTION

In this heterogeneous distributed computing world most of the applications Internet –based. So, there is a need for secret communication. Two techniques are used for secret communication. First method is cryptography. Cryptography is the process of encoding messages. Hackers cannot read it but authorized person can read. An authorized person is able to decode the messages. The second method is steganography. Steganography is the process of hiding the data.[1] Cryptography is visible communication and steganography is invisible communication in terms of message. The message is embedded in text files, audio, picture and video. The name Stego is from the Greek language. Cover is the meaning of stego so the image is called as cover image. Steganography is used in our day today life such as watermarking, ecommerce applications, and for data transfer. Watermarking is embedded in the images or files to show the ownership. It can be used for protecting copyright information of an authorized person. Currently, application transactions, mostly user's transactions are protected by a secret data. In biometric finger print person ID is integrated into the fingerprint images using steganography, to allow for the transaction verification for applications.

II.KINDS OF STEGANOGRAPHY

Steganography can be used for main categories of file formats like Text, images, audio/video and protocol.

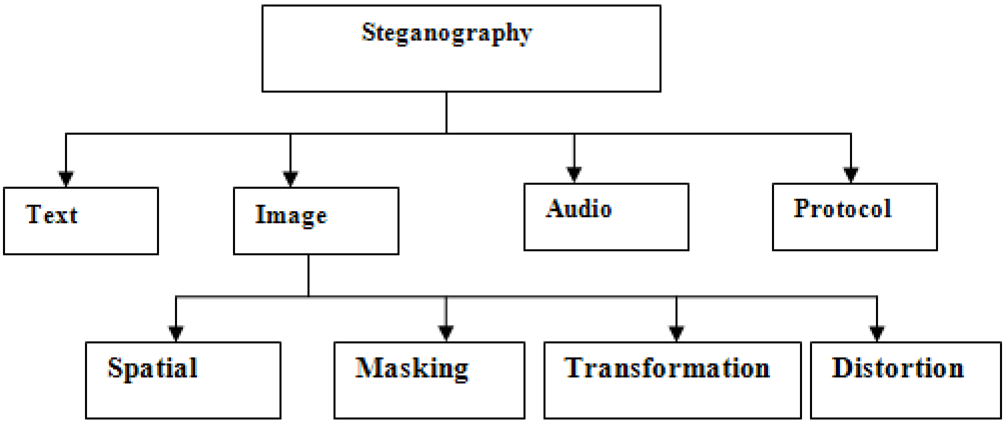

Figure 1: Classification of steganographic Techniques

A.Text Steganography:

Text as a cover medium is the oldest techniques used in early days. Secret message is detected by taking the 1st letter of every word present in the file. The process is continued by considering the various positions of the letters. The amount of message that is hidden in this type is very less and easily recoverable by frequency of letters. The following are the some of the methods used frequently by steganographers.

- Text hiding in mark-up languages (HTML)
- Text steganography in specific characters in words
- Line shifting method

- Word shifting
- Open spaces
- Semantic methods
- Character encoding

B.*Image Steganography*

Pictures are attractive to human rather than text Internet pages are very popular for its pleasant pictures. Human eye can not notice the changes in the LSB changes of the image. With this concept images are used to hide the secret information. Now a day's people are using various calculations. Randomly selecting the pixels in the image and replacing the ASCII values of the text are highly unbreakable algorithm cryptography and steganography shakes its hands together to make the image steganography robust.

C.*Audio Steganography*

Digital wave files are used to hide message. People are hearing the music in their day today life. Free music downloads from internet through PDA, mobile phones and pc makes the music files popular. Steganographers pay their attention in these audio files their secret message.

To embed data secretly onto digital audio there are few techniques introduced;

- LSB coding
- Phase coding
- Parity coding
- Spread spectrum

D. *Protocol Steganography*

A set of rules used to govern the communication is known as protocol. TCP, IP, UDP are the some of the protocols used for communication. Steganographers use this protocol for hiding their secret data. Some unused parts of the protocol like packet header are efficiently used for message hiding.[2]

III. TECHNIQUES OF IMAGE STEGANOGRAPHY

Image steganography focuses on many methods to apply on the images. Black and white, gray and color images are used to hide the message. According to the number of bits in a pixel the images are categorized. One bit per pixel images are monochrome images. Two bits per pixel can display gray scale images. Eight bits per pixel displays 256 colours of pictures. Twenty four bits per pixel is known as full colour or true colour system which displays millions of colours.

The following are the some of the techniques used in image steganography,

i) *Spatial Domain*

In spatial domain image steganography method pixel values are changed. Least Significant Bits are changed to hide the secret data. If the LSB bits are changed the image distortion won't be noticed by eye. Using the eye imperceptions LSB technique is widely used to hide the message. Pixels are selected either sequentially or randomly. Encryption of the data and hiding in the LSB makes Steganography stronger. MSB are also used to hide the data based on the intensity value. Key also embedded in the image itself so the intruder finds difficult to recover the text from the image

ii) *Masking and Filtering*

In this method MSB bits are used. Lossy compression images are used efficiently. Only gray scale images are used early.

iii*) Transform Domain Technique*

Transform domain uses the MSB to hide the data. This technique is widely used because of its independency over the image formats.[3] Transform domain is robust than LSB because it is focused on the image parts that are not altered by some image editing like cropping, resizing. Transform domain works well in both lossy and lossless compression images.

Steganography techniques with its pros and cons have been listed in the TABLE I with the brief description as follows.

TABLE I
Steganography Techniques

S. NO	Techniques	Advantages	Disadvantages
1	Spatial domain technique	i) Image quality is not changed for any algorithm that uses spatial method. ii) The large capacity of data can be stored.	i) Editing the image leads the image to lose its secret data. Less robust. ii) Secret data can be modified by the intruder during the communication.
2	Masking and Filtering	i) Stronger than the LSB method. Even though the image is compressed data is not affected . ii) The information hiding done in visible parts of the image.	These techniques can be applied only to gray Scale images and restricted to 24 bits.
3	Transform Domain Technique	i) To hide data in most significant areas of the cover-image, it makes them more robust from attack than LSB. ii) It can be applied changes for the whole image.	These method types are computationally complex.

IV.DATA HIDING MEDTHODS

Several methods are available in literature for hiding data, they are Least Significant bit(LSB),Pixel value differencing(PVD),Gray level Modification (GLM), Parity checker method(PCM),Diamond encoding method(DEM),Optimal pixel Adjustment process(OPAP),Exploiting modification direction(EMD),Adaptive pixel pair matching(APPM).

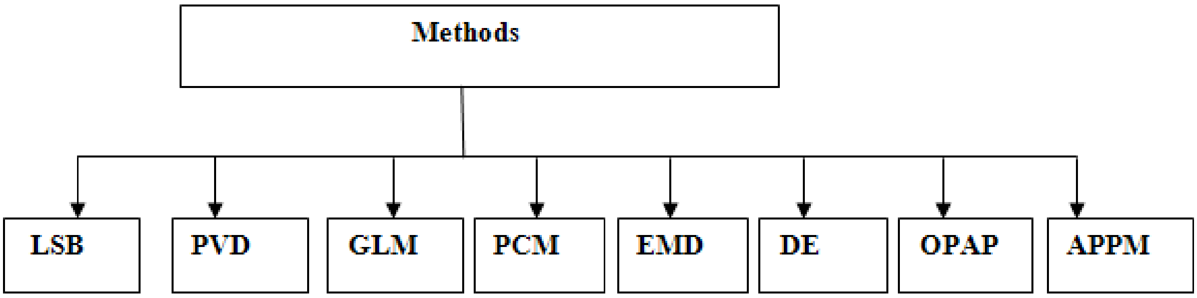

Figure 2: Various Steganography methods

A .*Least Significant Bit Method (LSB)*

This method replaces least bit significant bits with the message to be encoded. It is a frequent technique used so far when dealing with images [8]. It is simple, susceptible to lossy compression and image manipulation.

B. *Pixel value differencing Method (PVD)*

This method can successfully use both embedding and outstanding gradual of the stego-object [9]. The differencing method may be divided in to original image into acceptable blocks having two joining pixels and changes the pixel difference in every one block for data can be embedded.

C. *Gray level modification Method (GLM)*

This method is used to map data by changing grey level of the image pixel. GLM steganography is a technique of diagrammatic representation of the data by changing the gray level values of the image pixel. Gray level steganography uses the sum of 0's and 1's the value to map within an image. This is directly mapped between the binary values and the suitable pixels in an image. The set of image pixels are based on a mathematical function [10]. Grey level values of that pixel are determined based on the similarity with the bits stream that is to be mapped into the image. Starting with the suitable pixels, the bit 1 is made to 0 by modifying the gray level by one unit. At one time all the suitable pixels will have a 0, the gray level value similarity with the bits stream, it have been mapped. The first position of the bit in the stream is compared with first pixel. The 1st bit 0 means first pixel is not modified all the pixel will have 0.other than the bit is 1then the gray value of pixels is reduction by one unit to made its value 1,should represent an 1 bit map.

D. *Parity Checker Method (PCM)*

This method uses 0 and 1 parity mechanism. In a simplified manner this method even value can be inserted at a pixel position to identify pixel has 1(odd) parity bits. It can be identical odd value insert at a pixel; if the pixel should be 0 (even) parity [11]. If the close similarity parity do not exist at a pixel position for odd or even, then the pixel location can be added and subtracted such that the change in the image quality will not be Visible (to the human visual system).

E. *Exploiting modification direction method (EMD)*

This method uses only one pixel pair which is modified to one gray –scale unit message digits in a five-ary system for embedding. [12]. this is not efficient for high payload applications.

F. *Diamond encoding Method (DE)*

This method is contest position in pixel pair. It is improved by much more payload capacity, meanwhile able to accept stego image with excellence quality [12]. Still two problems need to be overcome such that the payload should be in a most suitable notational system. The arbiter value is not selected in a system.

G. *Optimal pixel adjustment process method (OPAP)*

This easily understood and effort pixel adjustment process makes minor distortion by the least significant bit replacement [12]. However distortion will be there by LSB replacement of adjusting pixel values.

H. *Adaptive pixel pair matching method (APPM)*

This method uses for pixel pair which competes each other. It is used to refer different elements and find element in the area surrounding a particular pixel pair position in corresponding message digit. This method has low distortion for different payload.

The steganography methods pros and cons have been listed in the TABLE II with the brief descriptions as follows:

TABLE II
Steganography Methods

S.No	Methods	Advantages	Disadvantages
1	LSB Method[8]	It is used for insertion of data. Implementation is very simple.	Easily recovered by unauthorized person.
2	PVD Method[9]	High capacity embedding and outstanding imperceptibility of the stego-image.	Each part of the cover image is divided into non overlapped blocks that has two connecting pixels and changes to different pixel in every one block (pair) for data Embedded. A larger difference in the original pixel values allows an extent modification.
3	GLM Method[10]	It has low computational complexity and high information hiding capacity	Contain Binary data. Allows one to one mapping Data loss occurs from image modification. Low embedding capacity.
4	Parity Checker Method [11]	Odd and even parity for insertion and retrieval of messages. Retrieval of message bits from all the locations are allowed.	Payload capacity is low.
5	Diamond encoding Method[12]	The diamond encoding technique Minimizes the distortion and helps in having better visual quality. Large notational system can be embedded in the digits that extent notational system.	It is a selected notational system. This system cannot be arbitrarily selected.
6	OPAP method[12]	Reduce the Distortion	Distortion is present.
7	EMD method[12]	Pixel pair is the only pixel to be modified .Grey scale unit data digits in 5th-array elements can be embedded to provide better stego image quality.	The maximum payload capacity of EMD is 1.161bpp
8	APPM Method[12]	It is used for any notational system. Embedding is appreciated to achieve better image quality.	Security is not applied.

V. STEGANALYSIS

Steganalysis is a process of recovering the data that is hidden in the images. Steganalyzer will use various attacks to find the secret data. Chi square method is widely used to detect the data using the statistical properties of the images. Passive attack is very hard to detect because the intruder capture the secret data without modifying the image. So it should be prevented. Active attacks can be traced because the intruder changes the data that is embedded in the image. Active attack should be detected to keep the secret data as confidential.

VI. CONCLUSION

Steganography is one of the oldest and robust techniques used in various applications involving the secret data sharing. Steganography becomes powerful when it is used along with cryptography. Different kinds of image steganography methods are discussed by highlighting its strong and weak points. Predicting a best method is not possible. The recent spatial domain techniques shows that message hiding can be done efficiently using only the LSB itself. Combining the MSB and LSB for hiding the secret data makes the algorithm very stronger. Steganography is an ongoing research area and the study in this paper the initial step to reach the milestone of the steganography.

REFERENCES

[1] Ramanpreet Kaur, Prof.Baljit Singh "Survey and Analysis Of Various Steganographic Techniques" international Journal Of Engineering Science & Advanced Technology Volume-2 , Issue-3, May-June 2012.

[2] Vijay kumar sharma, Vishal shrivastava "A steganography Algorithm for hiding image in image by improved lsb substitution by minimize detection" journal of theoretical and applied information technology 15th february 2012. vol. 36 no.1

[3] Dr. Ekta Walia a, Payal Jainb "An Analysis of LSB & DCT based Steganography",Global Journal of Computer Science and Technology, 4 Vol. 10 Issue 1 (Ver 1.0), April 2010,

[4] Nitin Jain, Sachin Meshram, Shikha Dubey "Image Steganography Using LSB and Edge – Detection Technique " ,International Journal of Soft Computing and Engineering (IJSCE) ISSN: 221-2307, Volume-2, Issue-3, July 2012

[5] Nagham Hamid , Abid Yahya, R. Badlishah Ahmad, Osamah M. Al-Qershi "Image Steganography Techniques: An Overview", International Journal of Computer Science and Security (IJCSS), Volume (6) : Issue (3) : 2012

[6] Saurabh Singh, Gaurav Agarwal "Use of Imageto secure text message with the help of LSB replacement", International ournal of Applied Engineering Research, Dindigul, Volume 1, No1, 2010, ISSN 09764259

[7] Pradeep Kumar Saraswat ,and Dr. R. K. Gupta "A Review of Digital Image Steganography" in Journal of Pure and Applied Science & Technology Copyright © 2011 NLSS, Vol. 2(1), Jan 2012

[8] Neil F Johnson, Sushil Jajodia, "Exploring Stenography: Seeing the Unseen", IEEE Computer, Feb 1998,

[9] D.C. Wu and W.H. Tsai. "A steganographic method for images by pixel value differencing". Pattern Recognition Letters, 24: 1613-1626, 2003

[10] Vidyasagar M. Potdar, Elizabeth Chang, "Grey Level Modification Stegnography for Secret Communication", 2nd IEEE International Conference on Industrial Informatics INDIN 2004 June 24th, 26th June, Berlin, Germany, Submitted Tuesday, May 25, 2004.

[11] Yadav, Rajkumar, Rishi, Rahul, Batra, Sudhir, "A new Steganography Method for Gray Level Images using Parity Checker", International Journal of Computer Applications(0975-8887) Volume 11-No. 11, December 2010.

[12] Wien Hong and Tung-Shou Chen "A Novel Data Embedding Method Using Adaptive Pixel Pair Matching" IEEE transactions on information forensics and security, vol. 7, no. 1, february 2012.