Modern Steganographic technique: A survey

Pratap Chandra Mandal
Asst. Prof., Department of Computer Application
B.P.Poddar Institute of Management & Technology
Kolkata, West Bengal, India
pcmandal9@gmail.com

***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 stego-key. It is reffered to as stego-image. Steganography is now more important due to the exponential growth and secret communication of potential computer users on the internet. In this paper I have analyzed various steganographic techniques. It also given an overview of steganography, different methods of steganography, its applications, how it is different from cryptography.**

Keywords – Steganography, LSB, spatial, frequency, masking, filtering, distortion.

I. INTRODUCTION

Now a day, a lot of applications are Internet-based and in some cases it is desired that the communication be made secret. There are two techniques are available to achieve this goal. One is cryptography, where the sender uses an encryption key to encrypt the message, this encrypted message is transmitted through the insecure public channel, and decryption algorithm is used to decrypt the message. The reconstruction of the original message is possible only if the receiver has the decryption key. The second method is steganography, where the secret message is inserted in another medium.

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 comes from 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.

Steganography differs from cryptography. The purpose of cryptography is to secure communications by changing the data into a form that can not be understand. Steganography techniques, on the other hand, hide the existence of the message itself, which makes it difficult for a third person to find out where the message is. Sometimes sending encrypted information may draw attention, while invisible information will not. Accordingly, cryptography is not the good solution for secure communication; it is only part of the solution. Both techniques can be used together to better protect information. In this case, even if steganography fails, the message cannot be recovered because a cryptography technique is used as well. The cracking of steganographic messages is called steganalysis. The purpose of steganalysis is to identify the information and determining that whether or not they have hidden messages encoded into them and if possible, extract the hidden information [1].

Watermarking and fingerprinting related to steganography are basically used for intellectual property protection. A digital watermark is a signal which is permanently embedded into digital data that can be detected or extracted afterwards to confirm the authenticity of the data. The watermark may be hidden in the host data. The embedded information in a watermarked object is a signature refers the ownership of the data in order to ensure copyright protection. In fingerprinting, different and specific marks are embedded in the copies of the work that different customers are supposed to get. In this case, it becomes easy for the property owner to find out such customers who give themselves the right to violate their licensing agreement when they illegally transmit the property to other groups.

II. DIFFERENT KINDS OF STEGANOGRAPHY

The four main categories of file formats that can be used for steganography are:

I. Text
II. Images
III. Audio
IV. Protocol

I. Text steganography: Hiding information in text is the most important method of steganography.The method was to hide a secret message in every n^{th} letter of every word of a text message. After booming of Internet and different type of digital file formats it has decreased in importance. Text stenography using digital files is not used very often because the text files have a very small amount of redundant data.

II. Image steganography: Images are used as the popular cover objects for steganography. A message is embedded in a digital image through an embedding algorithm, using the secret key. The resulting stego image is send to the receiver.On the other side, it is processed by the extraction algorithm using the same key. During the transmission of stego image unauthenticated persons can only notice the transmission of an image but can't guess the existence of the hidden message.

III. Audio steganography: Audio stenography is masking, which exploits the properties of the human ear to hide information unnoticeably. An audible, sound can be inaudible in the presence of another louder audible sound .This property allows to select the channel in which to hide information.[2]

IV. Protocol steganography: The term protocol steganography is to embedding information within network protocols such as TCP/IP. We hide information in the header of a TCP/IP packet in some fields that can be either optional or are never used.

III. STEGANOGRAPHIC TECHNIQUES

This paper introduced various stegnography techniques for hiding data in images. The images are represented with numerical values of each pixel where the value represents the color and intensity of the pixel. Images are mainly of two types: 8-bit images, 24-bit images

8-bit images: In 8-bit images maximum numbers of colors that can be present are only 256 colors.

24-bit images: Each pixel in these images have 24 bit value in which each 8 bit value refers to three colors red, blue and green.

There are several Steganographic techniques for image file format which are as follows:

I. Spatial domain technique

II. Masking and filtering

III. Transform techniques

IV. Distortion Techniques

I. Spatial Domain Technique: There are many versions of spatial steganography, all directly change some bits in the image pixel values in hiding data. Least significant bit (LSB)-based steganography is one of the simplest techniques that hides a secret message in the LSBs of pixel values without introducing many perceptible distortions. To our human eye, changes in the value of the LSB are imperceptible. Embedding of message bits can be done either sequentially or randomly. Least Significant Bit (LSB) replacement, LSB matching, Matrix embedding and Pixel value, differencing are some of the spatial domain techniques.

Advantages of spatial domain LSB technique are:

1. There is less chance for degradation of the original image.
2. Hiding capacity is more i.e. more information can be stored in an image.

Disadvantages of LSB technique are:

1. Less robust, the hidden data can be lost with image manipulation.
2. Hidden data can be easily destroyed by simple attacks

II. 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. Watermarking techniques can be applied without the fear of image destruction due to lossy compression as they are more integrated into the image.

Advantages of Masking and filtering Techniques: This method is much more robust than LSB replacement with respect to compression since the information is hidden in the visible parts of the image.

Disadvantages: Techniques can be applied only to gray scale images and restricted to 24 bits.

III. Transform Domain Technique This is a more complex way of hiding information in an image. Various algorithms and transformations are used on the image to hide information in it. Transform domain embedding can be termed as a domain of embedding techniques for which a number of algorithms have been suggested [3]. The process of embedding data in the frequency domain of a signal is much stronger than embedding principles that operate in the time domain. Most of the strong steganographic systems today operate within the transform domain Transform domain techniques have an advantage over LSB techniques as they hide information in areas of the image that are less exposed to compression, cropping, and image processing. Some transform domain techniques do not seem dependent on the image format and they may outrun lossless and lossy format conversions. Transform domain techniques are broadly classified into :

1. Discrete Fourier transformation technique (DFT).

2. Discrete cosine transformation technique (DCT).

3. Discrete Wavelet transformation technique (DWT).

IV. Distortion Techniques: 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. The encoder adds a sequence of changes to the cover image. So, information is described as being stored by signal distortion [4].Using this technique, a stego-object is created by applying a sequence of modifications to the cover image. This sequence of modifications is use to match the secret message required to transmit [5].The message is encoded at pseudo-randomly chosen pixels. 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.However, the need for sending the cover image limits the benefits of this technique. In any steganographic technique, the cover image should never be used more than once. If an attacker tampers with the stego-image by cropping, scaling or rotating, the receiver can easily detect it.In some cases, if the message is encoded with error correcting information, the change can even be reversed and the original message can be recovered [6].

A. Least Significant Bit (LSB): LSB is the lowest bit in a series of numbers in binary. e.g. in the binary number: 10110101, the least significant bit is far right 1.The LSB based steganography is one of the steganographic methods which is used to embed the secret data in to the least significant bits of the pixel values in a cover image. e.g. 210 can be hidden in the first eight bytes of three pixels in a 24 bit image.

PIXELS: (00100110 11100001 11101000) (01100111 11001010 11101101) (11011001 10100111 11101000)

210 : 11001010

RESULT: (00100111 11100001 11101000) (01100110 11001011 11101100) (11011001 10100110 11101000) Here number 210 is embedded into first eight bytes of the grid and only 5 bits are changed.

IV. LITERATURE SURVEY

A lot of Research has been carried out on Steganography:

Rajkumar Yadav et al. [7] proposed a new image steganography technique for embedding messages into gray level Images. This new technique distributes the message uniformly throughout the cover image. The image is divided into blocks of equal sizes and the message is then inserted into the central pixel of the block using cyclic combination of 6^{th}, 7^{th} & 8^{th} bit. The blocks of the cover image are chosen randomly using the pseudo random generator seeded with a secret key. Cyclic combination of last three bits of pixel value provides 100% chances of message insertion at the pixel value and division of image into blocks distribute the message uniformly throughout the image. This method also provides minimum degradation in image quality that cannot be perceived by human eye. This method also shows greater immunity to various types of noises. This method shows minimal change at a pixel value i.e. of +1 or -1 and does not gives any clue to the intruder to identify difference between original image and stego image. This method also provides strong degree of temper resistance. If the intruder tries to tamper with the stego image then it becomes visible at the receiver.

Dr. Ekta Walia et al. [8] provides analysis of Least Significant Bit (LSB) based steganography and Discrete Cosine Transform (DCT) based steganography. LSB based steganography insets the text message in lsb of digital data. Converting an image from a format like BMP or GIF which reconstructs the original message exactly to a JPEG which does not and then back could destroy the information hidden in the LSBs. DCT based steganography embed the text message in lsb bits of the discrete cosine (DC) coefficient of digital picture. When information is hidden inside video, the program hiding the information usually performs the DCT. DCT slightly changes each of the images in the video. An implementation of both these methods and their performance analysis has been done for LSB based and DCT based stego images using PSNR ratio shows that PSNR ratio of DCT based steganography scheme is high as compared to LSB based steganography scheme for all types of images. DCT based steganography scheme works perfectly with minimal distortion of the image quality as compared to LSB based. But DCT based steganography scheme is recommended because of the minimum distortion of image quality.[9]

Rajkumar Yadav [10] proposed a new method for the most LSB for hiding data in digital image. Another technique for hiding data in digital image is GLM technique [6]. Main drawback of above methods is that if the intruder changes least significant bit (LSB) of all image pixels then hidden message can be destroyed. In this case the change in image quality is in the range of +1 to -1 at each pixel position that. Second drawback is that LSB bit may be corrupted by hardware imperfections or quantization noise due to which message can be distorted. In GLM method if lsb bit changes due to above two problems then pixel value become from even to odd or odd to even due to which message can be destroyed. In their method, they have used 5^{th}, 6^{th} and 7^{th} bit for embedding and retrieval of message. Their method removes both drawbacks associated with LSB and GLM technique and provide us better results.According to their approach if decimal value of 5^{th} , 6^{th} and 7^{th} bits are 0, 2, 4 or 6 then insert 0 at these locations if decimal value of 5^{th} , 6^{th} and 7^{th} bit are not 0, 2, 4 or 6 then add or subtract 1 at that location for making decimal value of 5^{th} , 6^{th} and 7^{th} bit 0, 2, 4 or 6 for insertion of 0.

Similarly, we can insert 1 at a pixel location if decimal value of 5^{th} , 6^{th} and 7^{th} bit at that location is 1, 3, 5 or 7. If decimal value of 5^{th} , 6^{th} and 7^{th} bit at that location is not 1, 3, 5 or 7 then add or subtract 1 at that location for making decimal value of 5^{th} , 6^{th} and 7^{th} bit 1, 3, 5 or 7 for insertion of 1. For retrieval of message, they again check decimal value of 5^{th}, 6^{th} and 7^{th} bit. If the decimal value of 5^{th}, 6^{th} and 7^{th} bit at the selected location is 0, 2, 4 or 6, then 0 is the message bit else message bit is 1[5].

M.Sivaram et al.[11] in their proposed system they have choosen a random pixel in a cover image and in that they took last two bits for encrypting the data. So, the data length of the secret message can be extended. In the proposed technique they have embedded a character with the help of only 2 pixels instead of using the 3 pixels. So we can insert more characters in a single image by using this technique. In old technique the main disadvantages of using LSB technique requires a fairly large cover image to create a usable amount of hiding space. Even nowadays uncompressed images of 800 x 600 pixels are not often used on the Internet, so using these might raise suspicion. But in their proposed system it can overcome the problem by inserting a character in last two bits of the byte.This shows the efficiency over the other existing systems.

Nitin Jain et al.[12] they have shown how the edges of the images can be used to hide text message in steganography. It gives the depth view of image steganography and edge detection filter techniques. The method calculates binary value of each character of text message and then tried to find dark places of gray image (black) by converting the original image to binary image. Then these images have been converted to RGB image in order to find dark places.In this way each sequence of gray color turns into RGB color and dark level of grey image is found by this way. In the final stage each 8 pixels of dark places has been considered as a byte and binary value of each character has been put in low bit of each byte that was created manually by dark places pixels for increasing security of the main way of lsb bit steganography. Steganalysis then used to evaluate the hiding process to ensure the data can be hidden in best possible way. This approach hides the text in selected dark places but the data is not put directly in those pixels and put in low bits of each eight bit pixel.

V. USES OF STEGANOGRAPHY

Steganography can be used for digital watermarking, ecommerce, and the transport of sensitive data [13]. Digital watermarking involves embedding hidden image or file to show ownership.This is useful for protecting copyright of the owner. In current e-commerce transactions, most users are protected by a username and password.But there is no real method of verifying that the user is the actual card holder. Biometric finger print scanning which is combined with unique session IDs embedded into the fingerprint images via steganography, allow for a very secure option to open e-commerce transaction verification.

VI. IMAGE BASED STEGANALYSIS

Steganalysis is the science of detecting hidden information [14]. The main objective of steganalysis is to break steganography and the detection of stego image is the goal of steganalysis. Almost all steganalysis algorithms rely on steganographic algorithms introducing statistical differences between cover and stego image. Steganalysis deals with three important categories:

1. Visual attacks: it reveal the presence of hidden information, which helps to separate the image into bit planes for further more analysis

2. Statistical attacks: These types of attacks are more powerful and successful, because they reveal the smallest alterations in an images statistical behavior. Statistical attacks may be passive or active. Passive attacks involves with identifying presence or absence of a covert message or embedding algorithm used.Active attacks is used to investigate embedded message length or hidden message location or secret key used in embedding.

3. Structural attacks: The format of the data files changes as the data to be hidden is embedded,identifying this characteristic structure changes can help us to find the presence of image.

VII. STEGANALYTIC TOOLS

There are several steganalytic tools available in market like PhotoTitle, 2Mosaic and StirMark Benchmark etc. These three steganalytic tools can remove steganographic content from any image. This is achieved by destroying secret message by two techniques: break apart and resample. StegDetect, StegBreak, StegSpy identify the information embedded via the following tools - Jsteg-shell, JPhide, and Outguess 0.13b, Invisible Secrets, F5, appendX, Camouflage, Hiderman, JPHIde and Seek, Masker, JPegX, Steganography Analyzer Real-Time Scanner is the best available steganalysis software in the market at the moment, which can analyze all the network traffic to look for traces of steganographic communication.

VIII. CONCLUSION

In this paper I have reviewed different methods of steganography. Each method has a procedure of embedding for itself. Each method have some advantages, and also disadvantages in comparison with other methods of steganography. So it is not possible to say that a specified method is the best and best off all. It is impossible to determine the worst one. We can just compare them form different aspects, which results in determining a suitable method for a specific usage. I have also explained the way algorithms works. It can help the reader proportionally to understand why an algorithm is better than another in a specific situation. Thus it may be concluded that steganographic algorithms developed for one cover media may not be effective for

another media. The research to device strong steganographic technique is a continuous process and still going on.

REFERENCES

[1] Ramanpreet Kaur,Prof.Baljit Singh "SURVEY AND ANALYSIS OF VARIOUS STEGANOGRAPHIC ECHNIQUES " INTERNATIONAL JOURNAL OF ENGINEERING SCIENCE & ADVANCED TECHNOLOGY Volume-2 , Issue-3, 561 – 566, 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, p1-8

[3] N. F. Johnson, S. Katzenbeisser. " A Survey of steganographic techniques. " in Information Hiding Techniques for Steganography and Digital Watermarking,S.Katzenbeisser and F.Petitcolas, Ed. London: Artech House, 2000, pp. 43-78.

[4] H.S. Majunatha Reddy and K.B. Raja. (2009)."High capacity and security steganography using discrete wavelet transform. " International Journal of Computer Science and Security. pp. 462-472.

[5] S.C. Katzenbeisser. "Principles of Steganography ." in Information Hiding Techniques for Steganography and Digital Watermarking, S. Katzenbeisser and F. Petitcolas, Ed. London: Artech House, 2000, pp. 43-78

[6] P. Kruus, C. Scace,M. Heyman, and M. Mundy. (2003), "A survey of steganography techniques for image files ." Advanced Security Research Journal. [On line], 5(1), pp. 41-52.

[7] Rajkumar Yadav, Ravi Saini and Kamaldeep "CYCLIC COMBINATION METHOD FOR DIGITAL IMAGE STEGANOGRAPHY WITH UNIFORM DISTRIBUTION OF MESSAGE ", Advanced Computing: An International Journal (ACIJ), Vol.2, No.6, November 2011, p29-43

[8] 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, p4-8

[9] S. Nithya Devi, P.Laura Juliet "SURVEY ON IMAGE STEGANOGRAPHY ALGORITHM "International Journal of Communications and Engineering Volume 04– No.4, Issue: 02 March2012.

[10] Rajkumar Yadav, Ravi Saini and Kamaldeep "A New Image Steganography Approach for Information Security Using Gray Level Images in Spatial Domain", Vol. 3 No. 7 July 2011, ISSN: 0975-3397, p2679-2690

[11] M.Sivaram ,B.DurgaDevi J.Anne Steffi " STEGANOGRAPHY OF TWO LSB BITS" International Journal of Communications and Engineering Volume 01– No.1, Issue: 01 March2012, p82-87
Nitin Jain, Sachin Meshram, Shikha Dubey "Image Steganography Using LSB and Edge – Detection Technique " , International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 2012 ,p217-222

[12] 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,p168-187

[13] József LENTI "STEGANOGRAPHIC METHODS" in PERIODICA POLYTECHNICA SER. EL. ENG. VOL. 44, NO. 3– 4, PP. 249–258 (2000).

[14] Vipul Singhal, Dhananjay Yadav, Devesh Kumar Bandil," Steganography and Steganalysis: A Review" International Journal of Electronics and Computer Science Engineering ,pp399-404.

[15] Bhavana.S and K.L.Sudha "TEXT STEGANOGRAPHY USING LSB INSERTION METHOD ALONG WITH CHAOS THEORY" International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol.2, No.2, April 2012, p145-149

[16] M.Sivaram, B.DurgaDevi, J.Anne Steffi "STEGANOGRAPHY OF TWO LSB BITS" International Journal of Communications and Engineering Volume 01– No.1, Issue: 01 March2012,p82-p87

[17] Saurabh Singh, Gaurav Agarwal "Use of Imageto secure text message with the help of LSB replacement", INTERNATIONAL JOURNAL OF APPLIED ENGINEERING RESEARCH, DINDIGUL, Volume 1, No1, 2010, ISSN 09764259, p200-205

[18] R. Radhakrishnan, K. Shanmugasundaram, and N. Memon. " Data masking: a secure-covert channel paradigm." in IEEE Workshop on Multimedia Signal Processing, 2002. pp. 339-342.

[19] Souvik Bhattacharyya, Indradip Banerjee and Gautam Sanyal " A Survey of Steganography and Steganalysis Technique in Image, Text, Audio and Video as Cover Carrier" in Journal of Global Research in Computer Science, Volume 2, No. 4, April 2011,pp1-16

[20] 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, pp. 98-106

[21] Jinsuk Baek, Cheonshik, Kim, Paul S. Fisherl, and Hongyang Chao, "(N-1) Secret Sharing Approach Based on Steganography with Gray Digital Images", IEEE, 2010, 978-14244-5849-3/10.

[22] Xinge You, Liang Du, Yiu-ming Cheung, Quuhui Chen, "A Blind Watermarking Scheme using New Nontensor Product Wavelet Filter Banks", IEEE Transactions on image processing, IEEE, December, 2010, Vol. 19, No. 12.