International Journal of Recent Research and Review, Vol. VII, Issue 1, March 2014

ISSN 2277 – 8322

Secure communication with Steganography- An Overview

Kazi Azizuddin Rafiuddin[1], Chetan Kumar[2]

M.Tech Student, Assistant Professor, Department of CSE, KITE, Jaipur, India

Email: ramkishan.bairwa@gmail.com

Abstract- **Steganography is the art and science of hiding information within other information in such a way that it is hard or even impossible to tell that it is there. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the internet. The carrier can then be sent to a receiver without anyone else knowing that it contains a hidden message. Now days, terrorists also using Steganography techniques to communicate with one another without anyone else's knowledge and cause harm to people as well as government. Here, objective is not to make it difficult to read the message or to prevent the message being read as cryptography does, it is to hide the existence of the message. For hiding secret information in images, there exists a large variety of Steganography techniques some are more complex than other and all of them have respective strong and weak points. Different applications have different requirements of the Steganography technique used. Software is readily available on the internet for any user to hide data inside images. These softwares are designed to fight illegal distribution of image documents by stamping some recognizable feature into the image.**

Keywords- Hiding information, Image, Image Steganography, Steganoanalyst.

I. INTRODUCTION

Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography. In modern terms, steganography is usually implemented computationally, where cover works such as text files, images, audio files, and video files are tweaked in such a way that a secret message can be embedded within them.

Watermarking and fingerprinting are closely related to Steganography [1]. In watermarking and fingerprinting the fact that information is hidden inside the files may be public knowledge so sometimes it may even be visible while in steganography the imperceptibility of the information is crucial. Steganography differs from cryptography in the sense that, where cryptography focuses on keeping the contents of a message secret, Steganography focuses on keeping the existence of a message secret [2]. Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated.

In steganography information can be hidden in carriers such as images, audio files, text files, and video and data transmissions. When message is hidden in the carrier a stego carrier is formed for example a stego-image. Hopefully it will be perceived to be as close as possible to the original carrier or cover image by the human senses.

Images are the most widespread carrier medium. The process of steganography work as follows: The message is firstly be encrypted. The sender embeds the secret message to be sent into a graphic file. This results in the production of what is called stego-image. Additional secret data may be needed in the hiding process e.g. a stegokey etc. This stego-image is then transmitted to the recipient. The recipient extractor extracts the message from the carrier image. The message can only be extracted if there is a shared secret between the sender and the

recipient. This could be the algorithm for extraction or a special parameter such as stegokey. A stegoanalyst or attacker may try to intercept the stego image.

II. OVERVIEW OF STEGANOGRAPHY

To provide an overview of steganography, terms and concepts should first be explained. An overview of the different kinds of steganography is given at a later stage.

Origins of Steganography

Steganography was around long before computers were invented. As long as people have desired to communicate in secret, steganography has been there, allowing them to at least attempt to do so. The term "steganography" dates back to 440 BC and derives from a Greek word meaning "covered or hidden writing." This word was used to refer to practices of leaders hiding messages sent to other leaders. One early such practice used by the Greeks was to scrape wax off of tablets, write on the wood underneath, and cover the message with the scraped off wax. In another early steganography example, a man's head was shaved, a message tattooed upon it, and the man sent to another leader to deliver the message after his hair had grown back and covered it so that others would not be aware he was carrying a message [3].

Steganography came to what is now the United States as early as the Revolutionary War, during which it took the form of secret message drops, code words, and invisible inks used for communications between General George Washington and a group of spies [4]. It continued in use through additional wars, including World War I and II. Following the tragedy of September 11, 2001, investigations revealed that Al'Queda terrorists may have transmitted images containing hidden messages via usenet. Evidence exists primarily in the form of Islamic extremist websites that provide information on how to embed data in images [4]. Though the use of steganography in planning 9/11 was not confirmed, the possibility of its use sparked new interest in steganography, and led to further research into its use and its prevention.

Steganography concepts

In this section, we will discuss how actually the steganography concept works. In our example shown below a secret image is being embedded inside a cover image to produce the stego image.

Firstly embedding and hiding information is to pass both the secret message and the cover message into the encoder. Inside the encoder, one or several protocols will be implemented to embed the secret information into the cover message. The type of protocol will depend on what information you are trying to embed and what you are embedding it in. For example, you will use an image protocol to embed information inside images.

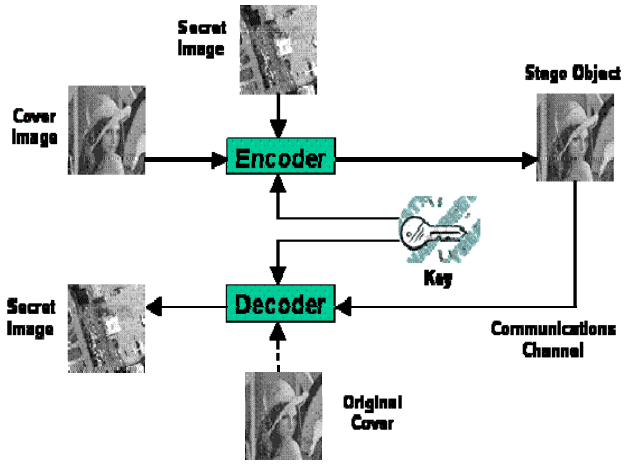
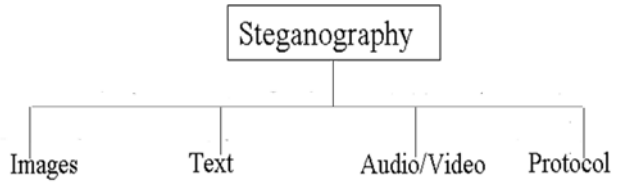


Fig.1 Image Protocol

A key is often needed in the embedding process. This can be in the form of a public or private key so you can encode the secret message with your private key and the recipient can decode it using your public key. In embedding the information this way, you can reduce the chance of a third party attacker getting hold of the stego object and decoding it to find out the secret information. Although Steganography is an ancient subject, the modern formulation of it is often given in terms of the *prisoner's problem* proposed by Simmons where two inmates wish to communicate in secret to hatch an escape plan. All of their communication passes through a warden who will throw them in solitary confinement should she suspect any covert communication [5].

Different Kinds of Steganography

All digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display. The redundant bits of an object are those bits that can be altered without the alteration being detected easily [6]. Image and audio files especially comply with this requirement, while research has also uncovered other file formats that can be used for information hiding.



Text - Hiding information in text is historically the most important method of steganography. An obvious method was to hide a secret message in every nth letter of every word of a text message. It is only since the beginning of the Internet and all the different digital file formats that is has decreased in importance [7]. Text steganography using digital files is not used very often since text files have a very small amount of redundant data.

Image - digital images are the most popular because of their frequency on the Internet. Also large amount of redundant bits present in the digital representation of an image, images are the most popular cover objects for steganography.

Audio- In audio steganography, secret message is embedded into digitized audio signal which result slight altering of binary sequence of the corresponding audio file. There are several methods are available for audio steganography. Some of them are LSB Coding, Phase Coding, Spread Spectrum, Echo Hiding etc.

Video - Although Image files BMP are perfect for steganographic use, they are able to carry only small files. So there is a problem, how to get much enough files to hide our message, and what to do to read them in a correct order? Good way out is to hide information in a video file, because as we know, AVI files are created out of bitmaps, combined into one piece, which are played in correct order and with appropriate time gap. Keeping that in mind all we have to do is to get out is file single frames and save them as BMP files. If we'll use algorithm for hiding data in digital pictures, we can hide our message in bitmap obtained in this way, and then save it into new AVI file.

Protocol - The term protocol steganography refers to the technique of embedding information within messages and network control protocols used in network transmission [8]. In the layers of the OSI network model there exist covert channels where steganography can be used. An example of where information can be hidden is in the header of a TCP/IP packet in some fields that are either optional or are never used. A paper by Ahsan and Kundur provides more information on this [8].

III. IMAGE STEGANOGRAPHY

Millions of images moving on the internet each year it is safe to say that digital image steganography is of real concern to many in the IT security field. Digital images could be used for a number of different types of security threats. In the corporate world the sending of a harmless looking bitmap file could actually conceal the latest company secrets. JPEGS could be used in the government to conceal the latest military secrets. It is believed that the terrorists that died in the 9-11 crash in New York had aircraft configuration plans sent to them hidden inside of a digital image. It is felt that the use of steganography has allowed the terrorists cells to communicate without the fear of being caught [9].

The use of digital images for steganography makes use of the weaknesses in the human visual system, which has a low sensitivity in random pattern changes and luminance. [10] The human eye is incapable of discerning small changes in color or patterns and because of this weakness text or graphic files can be inserted into the carrier image without being detected. Each graphic image is made up of what is called pixel elements (pixels). Each elements color is determined by the numerical value that it is assigned, ranging from 0 to 255.

Image steganography techniques-

a) LSB method: The popular and oldest method for hiding the message in a digital image is the LSB method. In LSB method hide the message in the least significant bits (LSB's) of pixel values of an image. In this method binary equivalent of the secret message is distributed among the LSBs of each pixel [11].
b) Parity Checker Method: According to this method, 0 can be inserted at a pixel location if that pixel has odd parity i.e. the number of 1's in the binary value of the pixel should be odd. Similarly, 1 can be inserted at a pixel location if that pixel has even parity i.e. the number of 1's in the binary value of pixel should be even. If the corresponding parity does not exist at a pixel location either for 0 or 1, then make corresponding parity at that pixel location (odd parity for 0 and even parity for 1) by adding or subtracting 1 to the pixel location such that the change in the image quality should not be visible to the human visual system (HVS) [12].
c) PVD Method: The pixel value differencing (PVD) method proposed by Wu and Tsai can successfully provide both high embedding capacity and outstanding imperceptibility for the stego- image. The pixel value differencing (PVD) method segments the cover image into non overlapping blocks containing two connecting pixels and modifies the pixel difference in each block (pair) for data embedding. A larger difference in the original pixel values allows a greater modification [13].
d) Tri-way PVD Method: This method is an improvement of the PVD method in terms of hiding capacity. In PVD method, only one direction is referenced whereas in these method three directional edges i.e. horizontal, vertical and diagonal edges are taken into consideration in order to hide the secret data bits [14].
e) Pixel Indicator Technique: The pixel indicator technique uses the least two significant bits of one channel from the Red, Green and Blue channel as an indicator for existence of data in other two channels. The indicator channels are chosen in sequence with Red being the first. Table 3.2 shows the relation between the indicator bits and amount of hidden data stored in the other [15].
f) Local Pixel Adjustment Technique: Local Pixel adjustment process improves the image quality of the stego-image. Local pixel adjustment process only considers the last three significant bits and the fourth bit but not all bits. The local pixel adjustment method is not optimal. As the local Pixel Adjustment process modifies the LSBs, the technique cannot be applied to data hiding schemes based on simple LSB substitution [16].
g) Optimal Pixel Adjustment Technique: This is the technique given by Chan et. al in 2003. This is a data hiding scheme which uses simple LSB substitution with an optimal pixel adjustment process. This method provides less change in image quality as compared to the LSB Method and local pixel adjustment process (LPAP). The image quality of the stego-image is improved by using this method [17].
h) 6^{th}, $7t^{h}$ and 8^{th} Bit Method: in these method 6^{th}, 7^{th} and 8^{th} bits of the image pixels are used to hide the message. Since this method involves 8th bit for hiding the message, intruder can easily change 8th bit of all image pixels and this may result in the loss of message. To avoid this, time factor has been introduced, i.e. at some time t1, sender sends the cover object with message and at some other time t2 sender sends the cover object without message. Sender and recipient agree on this time factor initially before starting any communication. The advantage of introducing time factor (slot) is that if least significant bits of all pixels are changed by the intruder even then the message can be retrieved by comparing the two cover objects, i.e. one containing the message and the other not containing the message [18].

IV. CONCLUSION

In this paper we discussed about Steganography concept with basic workflow, its origin and different types. Also we discussed image steganography in details with various techniques. Although only some of the main image steganographic techniques were discussed in this paper, one can see that there exists a large selection of approaches to hiding information in

images. All the major image file formats have different methods of hiding messages, with different strong and weak points respectively.

V. REFERENCES

[1] Shahana T, "An Enhanced Security Technique for Steganography Using DCT and RSA", International Journal of Advanced Research in Computer Science and Software Engineering, July-2013.

[2] Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, 47:10, October 2004.

[3] http://en.wikipedia.org/wiki/Steganography, Wikipedia page on steganography, includes links to many other sources.

[4] Kipper, Gregory. Investigator's Guide to Steganography. Auerbach Publications: Boca Raton, 2005.

[5] Chandramouli, Kharrazi & Memon "Image steganography and steganalysis: Concepts & Practice", Proceedings of the 2nd Internationa Workshop on Digital Watermarking, October 2003.

[6] Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", IEEE Journal of selected Areas in Communications, May 1998.

[7] Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science,

[8] Ahsan, K. & Kundur, D., "Practical Data hiding in TCP/IP", Proceedings of the Workshop on Multimedia Security at ACM Multimedia, 2002.

[9] Fixmar, Robert, "Terrorists and steganography", Zdnet News, 09/23/2001, http://zdnet.com.com/2100-1107-530751.html

[10] W. Bender, D. Grhul, N Morimoto, and A. Lu, "Techniques for Data Hiding", IBM Systems Journal, Vol 35,Nos.3-4,February1996.

[11] N. Johnson and S. Jajodia, "Exploring steganography: seeing the unseen," IEEEComputer, pp. 26-34, February 1998.

[12] 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.

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

[14] Ko-Chin Chang, Chien-Ping Chang, Ping S. Huang, and Te-Ming Tu," A Novel Image steganographic Method Using Tri-way Pixel-Value Differencing", Journal of Multimedia, Vol. 3, No. 2, June 2008.

[15] Adnan Abdul-Aziz Gutub," Pixel Indicator Technique for RGB Image Steganography", Journal of Emerging Technologies in Web Intelligence, VOL. 2, NO. 1, February 2010

[16] Chi-Kwong Chan, L.M. Cheng," Improved hiding data in images by simple LSB substitution", Pattern Reorganization, Elsevier,37(2004)469-474

[17] Chi-Kwong Chan, L.M. Cheng," Improved hiding data in images by optimal moderately significant bit replacement", IEEE Electron. Lett. 37(16)(2001)1017-1018.

[18] Sudhir Batra, Rahul Rishi and Raj Kumar, "Insertion of Message in 6th, 7th and 8th bit of pixel values and its retrievals in case intruder changes the least significant bits of image pixels", International Journal of Security and its application, Vol. 4, No. 3, July 2010.