International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 3, March 2014)

Overview of Secure Data Transmission Using Steganography

Rucha Bahirat [1], Amit Kolhe [2]
Department of Electronics and Telecommunication, CSVTU University
RCET Bhilai INDIA

***Abstract*—In this paper we survey various steganography schemes for hiding the data. The main goal of steganography is to communicate securely in a completely invisible manner so that no one can detect the transmission of a hidden data. In this paper we discuss the concept behind the steganography by describing what is steganography and the terms that are related to steganography. This paper gives the steganography methods for image steganography, audio steganography, video steganography, and text steganography that are used to embed the information in digital media. The two most important aspects of stegnography system are the quality of stego object and the capacity of the cover media. By reviewing this paper, researchers can build up a better steganography approach to increase the PSNR value and to decrease the MSE.**

***Keyword*- Steganography, Cryptography, Image, Audio, Video.**

I. INTRODUCTION

This The need to send a message as securely and as safely as possible has been the point of discussion since long time. Information is the assets of any association. This makes security-issues main concern to an association dealing with secret information. Whatever is the process we select for the security point, the strong concern is the level of security. Steganography is the ability of covered or hidden writing [1]. The aim of steganography is hidden communication to cover a message from a third party.

The term Steganography is of created from Greek word and means enclosed or secrete writing. Information hiding is used in secrete communication, closed captioning, indexing, or watermarking. It is in distinguished to cryptography. Cryptography is the method of converting plain text or original data into a meaningless form (cipher text) so that it may be sent over communications or unsafe channel. The changing process is controlled by a key.

Cryptography and Steganography are famous and commonly used methods that control information in order to code or cover their existence respectively. Steganography is the ability and skill of communicating by a means which hides the existence of the message.

Cryptography mixed up a message so it cannot be understood; the Steganography hides the message so it cannot be observed. [3]. In the cryptography system, the transmitter encrypts the message on the basis of encryption algorithm and keys when it is sent into the network. When receiver receives the data is decrypt with the help of keys and get the original data. Steganography is not as same as cryptography. Mainly the idea of cryptography and Steganography are to give covert communication. Basically, cryptography proposed the capability of transmitting information among people in a way that avoids a third party from reading it. Even though both techniques offer security, a study is made to join both cryptography and Steganography techniques into one system for better confidentiality and security [4].

A few key properties must be taken into consideration when creating a digital data hiding system [5].

- *Imperceptibility:* Imperceptibility is the main goal of steganography. When a person views a cover object, then that person should be unable to distinguish the object with embedded information from an object without embedded information. The goal is that the before hiding and after hiding object should appear identical.
- *Embedding Capacity:* Embedding Capacity refers to the amount of message that can be embedded using a particular system. Capacity is repeatedly a matter in steganography; however, one may want to secretly transmit a long message, so the capacity of a steganographic algorithm may become a significant factor.
- *Robustness:* Robustness refers to the degree of difficulty required to tear down embedded information without destroying the cover object itself.
- *Undetectability:* Detectability refers to the ability to determine whether or not a cover medium contains embedded information using statistical or technological means. Undetectability is nearly as important a goal as imperceptibility in steganographic systems because steganography seeks to cover the fact that a message is being transmitted.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 3, March 2014)

II. STEGANOGRAPHY

Steganography is the way to provide the security when data is transferred in the network. It is an ability of hiding information in the system to prevent the detection of secret messages. In this approach we cover the information through some multimedia files. These multimedia files can be audio, image or video. The principle of Steganography is to secret communication to hide the secret information from illegal user or the third party. In this process if the element is visible, the point of attack is clear thus the goal here is always to give chances to the very existence of embedded data. The safety issues and top priority to a society dealing with secret data the scheme is used for security purpose as the burning concern is the degree of security. The basic form for steganography is shown in figure below

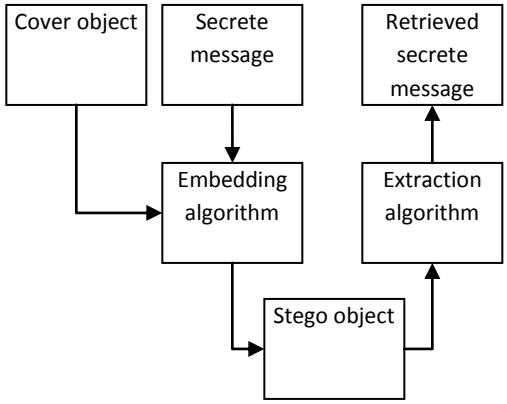

Fig.1. Basic steganography model

The basic model of steganography consists of cover object, message, embedding algorithm and Stego key. The model for steganography is shown in Figure 1. Cover object is also known as a carrier, which hides the message and serves to hide its presence. Digital images, videos, sound files, and other PC files that hold perceptually irrelevant or redundant information can be used as "covers" or carriers to hide secret data. After embedding a secret data into the cover-object, a so-called stego-object is obtained. At the receiver end, by applying an extraction algorithm we can retrieved the secrete message from stego object.

III. TECHINEQUES OF STEGANOGRAPHY

The majority of today's steganographic systems uses multimedia objects like video, image, audio etc. as cover object because people often send out digital pictures over email and other Internet communication [6]. In present approach, depending on the type of cover object, steganography can be separated into five types:

- Text Steganography
- Image Steganography
- Audio Steganography
- Video Steganography
- Protocol Steganograhy

Text Steganography:

In text Steganography the secrete message is hidden in the text and we use the different method to hide the message in text by changing the last bit of the message. Since everyone can read, encoding text in neutral sentences is doubtfully effective. But taking the first letter of each word of the previous sentence, we will see that it is possible and not very difficult. There are many different ways to hide information in plain text.

Image Steganography:

Taking the cover object as image in steganography is known as image steganography. Generally, in this technique pixel intensities are used to hide the information. To hide information, straight message insertion may encode every bit of information in the image or selectively embed the message in "noisy" areas that draw less attention—those areas where there is a great deal of natural color alteration. The data may also be spread randomly throughout the image

Audio Steganography:

In this technique, secret messages are embedding in digital sound. The secret data is embedded by slightly varying the binary sequence of a sound folder. Audio Steganography software can implant messages in WAV, MIDI and even MP3 sound files.

Video Steganography:

Video files are generally a group of images and sounds, so most of the existing techniques on images and audio can be applied to video files too.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 3, March 2014)

The big advantages of video are the huge size of data that can be hidden inside and the fact that it is a moving stream of images and sounds. Therefore, any small but otherwise perceptible distortions might go by unobserved by humans because of the continuous flow of information. Video steganography uses such as H.264, Mp4, MPEG, AVI or other video formats.

Protocol Steganography:

The term protocol steganography refers to the technique of embedding data within messages and network control protocols used in network transmission. In the layers of the OSI network model there exist hidden 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.

There are numerous approaches of categorizing steganographic system. One could classify them according to type of cover medium used for secrete communication. Another possibility is a classification according to cover modifications applied in the embedding process. Above we have is already discuss the first approach. According to 2nd approach steganographic scheme can be divided into following categories.

- **Substitution system** replace unneeded parts of a cover with a secrete data.
- **Transform domain techniques** embed secrete message in a transform space of the signal (e.g., in frequency domain).
- **Spread spectrum techniques** implement ideas from spread spectrum communication.
- **Statistical methods** encode data by changing several statistical properties of a cover and use assumption testing in the extraction process.
- **Distortion methods** accumulate data by signal alteration and measure the deviation from the original cover in the decoding step.
- **Cover generation schemes** encode data in the approach a cover for secrete communication is created.

IV. Related Work

Kousik Dasgupta et al. [7] suggested Hash based least significant bit technique for video steganography (HLSB). It is a spatial domain technique where the secret information is embedded in the LSB of the cover frames. Eight bits of the secret data is divided into 3, 3, 2 and implanted into the RGB pixel values of the cover frames respectively.

The position of insertion in LSB bits are selected by hash function. The proposed system is examined in terms of both Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE).

ShengDun Hu et al. [8] described a novel Video Steganography which can hide an uncompressed secret video stream in a cover video stream. Both video streams are of almost the same size. Each frame of the secret video will be divided into Non-uniform rectangles and the partitioned codes achieved can be an encrypted edition of the original frame. These partitioned codes will be concealed in the Least 4 Significant Bits of each frames of the cover video. Experimental results illustrate that this algorithm can hide a same-size video in the cover video without apparent distortion in the cover video.

N Sathisha et al. [9] proposed Chaos based Spatial Domain Steganography using MSB. Spatial Domain Steganography using 1-Bit Most Significant Bit (MSB) with chaotic manner has been proposed in this paper. The cover image is divided into blocks of 8*8 matrix of equal size. The first block of cover image is embedded with 8 bits of upper bound and lower bound values required for recovering payload at the end. The mean of median values and dissimilarity between consecutive pixels is determined to insert payload in 3bits of Least Significant Bit (LSB) and one bit of MSB in disordered manner. From the above technique it is observed that the capacity and security is improved compared to the existing methods with reasonable PSNR.

S.Changder et al. [10] proposed LCS based Text Steganography through Indian Languages. This paper presents some new techniques for steganography in Indian Languages. Considering the accessibility of more characters and flexible grammar sentences of Indian Languages this method hide the secret message in the cover text by creating meaningful sentences after discovering the longest common subsequence of two binary string among which one is the secret message and another may be any binary string. The collection of these created Indian sentences will be used as the cover media for this steganography approach. Similarly the system extract the original message from the cover file by applying the reverse method to the cover file that is after finding the longest common subsequence of sentences from the cover file and replacing the matched character by the bits of another binary string.

Suresh Babu et al., [11] have described an authentication of secret information in image steganography which can be used to confirm the reliability of the secret message from the stegoimage.

This can verify the consistency of the information being transmitted to the receiver, and verifies whether hacker tried to edit, delete or forge the secret message in the stegoimage.

M. Hassan Shirali-Shahreza and Mohammed Shirali-Shahreza, [12] proposed a synonyms text steganography, a method for steganography in English text by replacement of the word which have different terms in British English and American English. The method is used for printing text and printing the electronic document, so that the hidden data is not damaged.

Ding-Yu Fang et al. [13] proposed an effective data hiding approach that embeds data in digital video using the phase angle of the motion vector of the macroblock in the interframe. The method can be useful to either compressed or uncompressed videos. In this system we replace the original motion vector with another optimal motion vector to hide data in the motion vectors in the interframe. Local optimal motion vector saves lots of computational burdens. The embedded data can be removed directly without using the original video stream. The proposed method not only can embed large amount of data in video but also maintain good video value.

Pritish Bhautmage et al. [14] proposed a new technique for data embedding and extraction for high resolution AVI videos. In this scheme in place of changing the LSB of the cover media, the LSB and LSB+3 bits are changed in alternate bytes of the cover file. The secret message is encrypted by using a simple bit exchange method before the actual embedding process starts. A key can also be created for the secret information and the key is placed in a frame of the video itself. With the help of this key, we can easily remove the secret data, which can decrease the extraction time.

V. Conclusion

This paper gave an overview of different steganographic techniques its main types and categorization of steganography which have been proposed in the literature during last few years. By the reference of this paper, researchers can create a better steganography approach to enhance the PSNR value, embedding capacity and Imperceptibility. Many different techniques exist and continue to be developed, while the ways of detecting hidden messages also advance quickly. Since detection can never give a guarantee of finding all hidden information, it can be used together with methods of defeating steganography, to minimize the chances of hidden communication taking place.

Even then, perfect steganography, where the secret key will merely point out element of a cover source which form the message, will pass undetected, because the cover source contains no information about the secret data at all.

REFERENCES

[1] Johnson, N. F. and Jajodia, S. (1998). Exploring steganography: Seeing the unseen. Computer, 31(2):26–34.

[2] Daniela Stanescu, Mircea Stratulat, Voicu Groza, Joana Ghergulescu and Daniel Borca, "Steganography in YUV color space", IEEE International Workshop on Robotic and Sensors Environments (ROSE 2007), Ottawa- Canada, pp.1-4, October 2007.M.

[3] A.Joseph Raphael,Dr.V Sundaram, "Cryptography and Steganography – A Survey," Int. J. Comp. Tech. Appl., Vol 2 (3), 626-630.

[4] C. Jasmin, M. Baca, "Steganography and its implication on forensic investigation", INFOTEH Jahorina, B & H, 2010.

[5] B. Sharmila, R. Shanthakumari, " Efficient Adaptive Steganography for Color Images Based on LSBMR Algorithm," ICTACT JOURNAL ON IMAGE AND VIDEO PROCESSING, FEBRUARY 2012, VOLUME: 02, ISSUE: 03.

[6] Niels Provos, Peter Honeyman, Hide and Seek: Introduction to Steganography 2003.

[7] Niels Provos, Peter Honeyman, Hide and Seek: Introduction to Steganography 2003.

[8] ShengDun Hu, KinTak U, "A Novel Video Steganography based on Non-uniform Rectangular Partition," The 14th IEEE conference on computational science and engineering 2011.

[9] N Sathisha1, Madhusudan G N, Bharathesh S, K Suresh Babu, K B Raja, Venugopal K R, "Chaos based Spatial Domain Steganography using MSB," 2010 5th International Conference on Industrial and Information Systems, ICIIS 2010, Jul 29 - Aug 01, 2010.

[10] S.Changder, D. Ghosh and N. C. Debnath, "LCS based Text Steganography through Indian Languages," IEEE 2010.

[11] K. Suresh Babu, K. B. Raja, Kiran Kumar K., Manjula Devi T. H., Venugopal K. R. And L. M. Patnaik, "Authentication of Secret Information in Image Steganography," IEEE Conference on TENCON, pp. 1 – 6, November 2008.

[12] M. Hassan, Shirali-Shahreza, and Mohammad Shirali-Shahreza, "A New Synonym Text Steganography," International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 1524 – 1526, August 2008

[13] Ding-Yu Fang and Long-Wen Chang, "Data Hiding for Digital Video with Phase of Motion Vector," IEEE 2006.

[14] Pritish Bhautmage, Prof. Amutha Jeyakumar, and Ashish Dahatonde, "Advanced Video Steganography Algorithm," International Journal of Engineering Research and Applications pp.1641-1644, Vol. 3, Issue 1, January -February 2013.