Gunjan Chugh et al. International Journal of Recent Research Aspects ISSN: 2349-7688,
Vol. 5, Issue 1, March 2018, pp. 115-119

Review on Audio and Video Steganography Techniques

Gunjan Chugh[1], Priyanka Gaba[2]

Department of Information Technology, Northern India Engineering College, New Delhi, India

[1]chugh.gunjan8917@gmail.com

[2]priyanka.gaba2202@gmail.com

***Abstract* - Security of data that needs to be transmitted digitally is one of the major concern now-a-days. To maintain this, different methods of hiding data have been proposed. Steganography is one of the method in which secret data is hidden in some cover media. The cover media can be text, image, audio or video. Audio steganography deals with hiding the data in some audio file where as in video steganography secret data is hidden in a video in such a way that the original video does not loose its functionality. In this paper we review different techniques available for audio and video steganography.**

***Keywords* - Audio Steganography, Video Steganography, Cover media, Secret file, HAS.**

I. INTRODUCTION

With the rapid development of internet technologies, data needs to be transmitted digitally over the internet. But due to different attacks and unauthorized access, measures must be taken to protect the secret information. Information can be kept secret either by cryptography or by steganography. Earlier Cryptography was considered as sufficient technique that encrypts the data and keeps it safe. But now a days, it is not sufficient to keep only the contents of message secret, but it is also required to keep the existence of message secret. Thus, Steganography has emerged as a technique that hides and conceals the existence of message as well.

The word Steganography comes from the Greek origin, means "concealed (covered) writing". The word 'steganos' means "covered or protected" and 'graphie' means "writing" [1]. Steganography is thus, not only the art of information hiding, but also the art and science of hiding the fact that communication is even taking place [2]. Steganalysis, on the other hand, is to discover hidden information and to break the security of its carriers. Thus, the goal of steganography is to avoid drawing suspicion during the transmission of the secret message.

II. STEGANOGRAPHY CLASSIFICATION

The concept of "What You See Is What You get (WYSIWYG)" which we encounter sometimes while printing images or other materials, does not always hold true. Images can be more than what we see with our Human Visual System (HVS); hence they can convey more than merely 1000 words. For decades people strove to create methods for secret communication [1]. Figure1 shows classification of steganography:

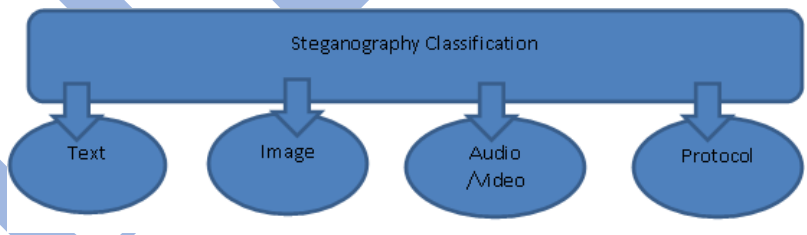

Figure 1: Steganography Classification

Different categories of steganography are discussed as follows:

A. Text Steganography

The most popular method was to hide a secret message in every nth letter of every word of a text message [1]. Since text files have very small amount of redundant data, therefore, this technique is not used widely.

B. Image Steganography

In Image Steganography, images are used as cover source for hiding the secret data. Since images contain a large amount of redundant bits therefore a large amount of secret data can be hidden in images.

C. Audio/Video Steganography

In audio/video steganography, audio/video files are used as cover source for hiding the secret data. This steganography uses the concept of masking, which exploits the properties of the human ear to hide information unnoticeably. A faint, but audible, sound becomes inaudible in the presence of another louder audible sound [3].

This property creates a channel in which information can be hidden. In this paper, we will have on overview of different audio and video steganography techniques

D. Protocol Steganography

In Protocol Steganography, message is embedded in network control protocol used in network transmission. In the OSI network model there exist covert channels where steganography can be used [4]. An example 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.

The basic model of steganography consists of Carrier (i.e. Image, Audio, and Video File), Secret Key and Secret Message as shown in Figure 2.

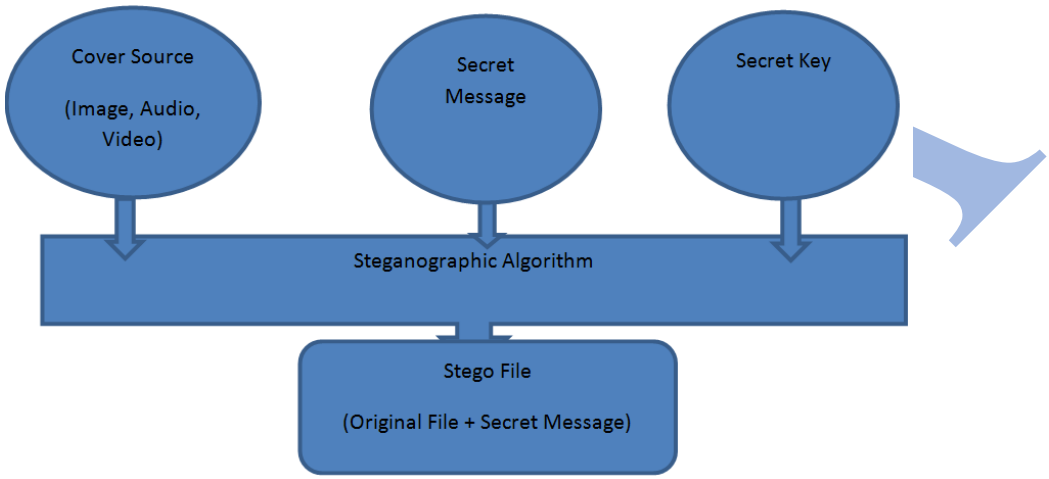

Figure 2: Steganography Model

III. AUDIO STEGANOGRAPHY

In audio steganography, audio file is used as cover file to hide the secret message. The steganography process can embed secret data in WAV, AU and MP3 files. In audio steganography we can embed information in sound files with the help of Human Auditory System (HAS). The HAS perceives the additive random noise and also the perturbations in a sound file can also be detected [5]. Hiding process consists of 2 steps: - Firstly, redundant bits in the audio file are identified. Secondly, Secret data is embedded by replacing these redundant bits with the message bits.

A. Audio Steganography Techniques

1.) Least Significant Bit(LSB) Coding

In this method, secret message bits replace LSB of binary sequences of each sample of digitized audio file. In LSB coding large amount of data can be encoded [6]. It is simple, fast and popular method for embedding information in audio file. But the drawback of this method is that it is vulnerable to attacks.

2.) Phase Coding

In this method, the reference phase that represents the secret data substitutes the phase of the initial audio segment i.e. audio signal is encrypted using Discrete Fourier Transform. The phase coding exploits the fact that Human Auditory System (HAS) can't recognize the phase change in audio signal as it recognizes noise [7]. Thus, in this technique message bits are encoded when phase shifts in the phase spectrum of a digital signal, achieving an inaudible encoding in terms of signal-to-perceived noise ratio (SPNR)[6]. As phase coding encodes secret data in first signal segment only, so the drawback of this method is that it provides low data transmission. Thus phase coding is used only when small amount of data need to be hidden like watermark [7].

3.) Echo Data Hiding

In this method, an echo is introduced into the original signal and secret data is embedded in the audio file. This method provides high data transmission rate and high robustness as compared to other methods. Three parameters of original signal are manipulated when the data is hidden using this method- initial amplitude, offset(delay) and decay rate so that echo is not audible[8]. This method is not so popular because of low data rate and security.

4.) Parity Coding

In this method, a signal is broken into separate samples and each bit of secret message is embedded from parity bit thus avoiding breaking a signal into individual samples. The secret bit to be encoded is compared with the parity bit of a selected region, if they does not match, the process inverts the LSB of one of the samples in the region. Thus, the sender has more choice in encoding the secret bit [9]. It is the robust technique of data hiding using audio steganography.

5.) Spread Spectrum

This method spread the secret information over the frequency spectrum of sound file using a code which is independent of actual signal. Thus the bandwidth of actual signal is more than what is actually required for transmission .The advantage of this method lies in the fact that it provides moderate data transmission rate and high level of robustness but it introduces noise in the sound file[9].

IV. VIDEO STEGANOGRAPHY

Videos are considered as good candidates for hiding the data as they have high degree of spatial and temporal redundancy in representation. Video Steganography is extension of image steganography. But as the video content is dynamic, lower chances of detection of the hidden data compared with images. The hiding capacity is much higher in case of video. Videos provide new dimensions for data hiding such as hiding messages in motion components. The audio components of the video file can also be utilized for data hiding [10].

A. Video Steganography Techniques

1.) Substitution Based Techniques

In these techniques, secret data is replaced with redundant data of the cover. Different types of substitution-based techniques are Least Significant Bit (LSB) technique, Bit Plane Complexity Segmentation (BPCS), Tri-way Pixel Value Differencing (TPVD) etc [10].

LSB is the oldest substitution-based techniques. It operates by replacing some LSB of pixels from the cover video with the secret message bits [10]. This method provides high embedding capacity but it is vulnerable to attacks.

BPCS (Bit Plane Complexity Segmentation) is used to decompose an image/frame into bit planes. From each binary digit, all bits of a specific significant position are taken and a bit plane is formed. The complexity of each region in the bit planes is measured after decomposing the image into bit planes. The noise-like regions are then replaced with the secret data so that degradation in quality is minimum [10].

TPVD (Tri-way Pixel Value Differencing method) provides more hiding capacity by embedding secret data in horizontal, vertical and diagonal edges. This is modified version of PVD (Pixel Value Differencing method) in that secret data is hidden in the difference value of two adjacent pixels. Difference values are classified in 3 categories- lower bound, upper bound and width. TPVD was used by Sherly et al. [11] to embed data in MPEG compressed videos [10].

2) Transform Domain Techniques

The main drawback of substitution-based techniques is that those techniques cannot tackle any change in cover source that includes compression, format change etc. and the embedded data can be easily destroyed by an attacker using these techniques. Transform domain techniques are thus introduced and they provides more robustness and perceptual transparency of the produced stego-objects. In these techniques, secret data is embedded in transformed coefficients and the modified coefficients are transformed back to the original form of the cover. Example include: Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). All these transforms are used in image and video compression methods. In wavelet transform a signal is decomposed into a set of basis functions which are called wavelets. DWT analyses the signal at different frequencies giving different resolutions and thus provides a multi-resolution analysis. The main advantage of DWT is temporal resolution. That is, it captures frequency as well as location information [10]. In DCT, secret message and the cover video frames are transformed using 8X8 block DCT. The secret message coefficients are quantized and then encoded using the multidimensional lattices, and finally embedded into the cover frame DCT coefficients [10].

3.) Adaptive Techniques

These techniques are also known as “Masking” or “Statistics-aware embedding”. It works on statistical features of the cover before modifying the secret data. This helps in identifying best regions called Regions-of Interest (ROI) where secret data can be hidden. Thus, in this method, cover is adaptively modified according to some criteria and then secret data is hidden in it. Multiple features in video streams can be used for developing adaptive techniques [10].

4.) Format Based Techniques

As the name indicates, these techniques are designed for specific video formats. One of the latest compression standards for video is H.264/AVC. It provides high compression efficiency and it is well adapted for network transmission [10]. A technique based on this format was proposed by Mozo et al. in [12]. In this, secret message is divided equally among the video tags of the entire file and it is added after each video tag in such a way that the actual video and audio tags are never modified or omitted. The drawback of this method is that it increases the cover size after embedding the secret message [10].

5.) Cover Generation Techniques

In these techniques, a cover video is generated by the use of secret key and secret message. The generation process uses a function X(A,D) where X is the function to generate the container file using the message, A is the number of samples required to hide the message and D is the message bits to be hidden. In this method, a database is required to collect the images necessary for the video generation [10]. The advantage of this technique is the difficulty to perform steganalysis and the drawback is that suspicion may arise if the selected sequence of images was irrelevant to each other.

B. Some Other Video Steganography Techniques

1.) Index Based Technique

Balaji and Naveen [13] in 2011 have proposed a method that is based on creating an index for secret information and using this index, frames containing secret information are located at the sender's end and at the receiver end. The advantages offered by this method are firstly, the probability of finding hidden information by an attacker is less and secondly, the time taken for extraction of hidden information is less.

2.) 2-Layer Encryption Technique

In this technique, Vipula & Suresh Kumar [14] have proposed a method that uses two layer encryption to provide high robustness and security. Using AES algorithm, secret data is encrypted and then SHA-1 algorithm is used to generate secret hash function or key. At sender's side, image frames and audio file are extracted from the video file. The unused or free bits in audio file are utilized for hiding secret data. The stego file thus obtained is again encrypted using AES algorithm. At receiver's side, stego file is decrypted and then secret data is obtained from the audio component of video file. Secret data is again decrypted to obtain the required secret data.

3.) Modified LSB Technique

In 2011, Ramalingam [15], has proposed a method to perform video steganography using modified LSB technique. In the proposed method, firstly the secret data is encrypted and then hidden in the video file using modified LSB technique. At the receiver's end, firstly secret data is retrieved from the stego(video) file and then decrypted to obtain the original message. Researchers have also made a GUI i.e. STEGOMACHINE to implement the proposed method. The proposed stegomachine (i.e. the GUI) is implemented in Java therefore provides interoperability over multiple platforms.

4.) Steganography with Encryption

In the proposed method [16], a secret video file is hidden in the cover video file. Secret video is broken into individual components and then converted into 8-bit binary values. After that encryption is performed by taking XOR of binary values with the secret key and the obtained encrypted frames are hidden in least significant bits of cover video using sequential encoding. Security is enhanced by storing secret frames in cover frames by following a pattern BGRRGBGR.

5.) Enhanced LSB based Video Steganographic System

Kapoor and Mirza [17], in 2015 proposed a secure and efficient data transmission method that is based on firstly dividing the host video into frames and then the secret file to be hidden is compressed using ZIP compressor and the bytes are generated. The extracted bytes are used to create chunks of bits which are then embedded in the video frames. Stego file is sent after combing text file with the video frames. The proposed method is designed for MPEG formats but by doing slight modification it also works for other formats like AVI, 3GP. Researchers have shown that the proposed method provides better results than the LSB method both in terms of PSNR (Peak Signal to Noise Ratio) and MSE (Mean Square Error).

V. CONCLUSION

The main goal of steganography is to hide confidential data in some cover media in such a way that the secret data is immune to external attacks as well as it does not convey any suspicion of communication taking place between two parties. Different types of cover source can be used such as text, image, audio, video and protocol. Thus, the main objective is to find different techniques that are robust and thus provides capacity enhancement with

minimum degradation in quality of stego file. This paper gives an overview of different types of steganography. A review on audio and video steganography is addressed in detail. Different techniques of audio and video steganography are also discussed.

REFERENCES

[1] Rajkumar Yadav "Study of Information Hiding Techniques and their Counterattacks: A Review Article", International Journal of Computer Science & Communication Networks, Vol 1(2), 142-164, Oct-Nov 2011
[2] Angela D. Orebaugh " Steganalysis: A Steganography Intrusion Detection System" , George Mason University
[3] Lisa M. Marvel "Image Steganography for Hidden Communication" A Dissertation submitted to the Faculty of the University of Delaware in partial fulfilment of the requirements for the degree of Doctor of Philosophy in Electrical Engineering, Springer 1999
[4] Abbas Cheddad "Strengthening Steganography in Digital Images", School of Computing and Intelligent Systems, Faculty of Engineering, University of Ulster, Magee
[5] Navneet Kaur, Sunny Behal "Audio Steganography Techniques-A Survey", International Journal of Engineering Research and Applications, Vol. 4, Issue 6(Version 5), June 2014, pp.94-100
[6] Palwinder Singh, "A Comparative Study of Audio Steganography Techniques", International Research Journal of Engineering and Technology (IRJET), Volume: 03 Issue: 04 | Apr-2016
[7] Gunjan Nehru , Puja Dhar "A Detailed look of Audio Steganography Techniques using LSB and Genetic Algorithm Approach", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, January 2012
[8] Fatiha Djebbar, Beghdad Ayad, Karim Abed Meraim, Habib Hamam "Comparative study of digital audio steganography techniques", EURASIP Journal on Audio, Speech, and Music Processing, 2012
[9] Jayaram P, Ranganatha H R , Anupama H S "Information Hiding using Audio Steganography: A Survey", The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011
[10] Mennatallah M. Sadek & Amal S. Khalifa & Mostafa G. M. Mostafa, "Video steganography: a comprehensive review", Springer Conference on Multimedia Tools and Appl., New York 2014
[11] Sherly AP, Amritha PP, "A Compressed Video Steganography using TPVD", International Journal of Database Management System, Volume 2, Issue 3, 2010
[12] Mozo AJ, Obien ME, Rigor CJ, Rayel DF, Chua K, Tangonan G, "Video steganography using flash video (FLV)", Conference on "Instrumentation and Measurement Technology", 2009 , pp 822–827
[13] R. Balaji and G. Naveen, "Secure data transmission using video Steganography", IEEE Conference, 15-17 May 2011, Mankato, MN, USA
[14] Vipula Madhukar Wajgade , Dr. Suresh Kumar, "Enhancing Data Security Using Video Steganography", International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 4, April 2013
[15] Mritha Ramalingam, "StegoMachine – Video Steganography using Modified LSB Algorithm",World Academy of Science, Engineering and Technology International Journal of Information and Communication Engineering Vol 5, No.2, 2011
[16] Pooja Yadav, Nishchol Mishra, Sanjeev Sharma, " A secure video steganography with encryption based on LSB technique", IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), 2013
[17] Vivek Kapoor and Akbar Mirza, "An Enhanced LSB based Video Steganographic System for Secure and Efficient Data Transmission", International Journal of Computer Applications, Volume 121 – No.10, July 2015

