International Journal of Research (IJR) Vol-1, Issue-9, October 2014 **ISSN 2348-6848**

Survey paper - Audio-Video Steganography Using Anti Forensics Technique

Ms. V.Sarangpure[1]; Mrs. R. B. Talmale[2];Ms. M. Domke[3]

[1]Final Year M. Tech (CSE), Tulsiramji Gaikwad Patil College of Engineering & Technology Nagpur

[2]Assistant Professor M.Tech (CSE) Tulsiramji Gaikwad Patil College of Engineering & Technology Nagpur
[3]Assistant Professor M.Tech (CSE) Tulsiramji Gaikwad Patil College of Engineering & Technology Nagpur

Email:vaishali.vps@gmail.com, roshanikambe@rediffmail.com, minal.domke@gmail.com

ABSTRACT

Information hiding technique is a new kind of secretes communication technology. Data transmission in public communication system is not secure. To protect information from unauthorized access or to secure communication various methods like cryptography, steganography, hashing, and authentication are available. Today's steganography is one of the popular methods of information hiding. In Steganography hiding one medium of information of data in another medium. In this paper we will survey on audio-video steganography and different method available for audio-video steganography that mean how to hide secrete data in audio or video file using some anti forensic technique. Anti-forensics makes investigations on digital media

Keywords:
Information hiding; secure communication; steganography; cryptography; anti forensics

1. INTRODUCTION

Steganography the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" that means "covered writing". Steganography prevents an unintended recipient or unauthorized user from suspecting that the data exists. In modern steganography used electronic media rather than physical object for hiding the data. There are different approaches and methods of steganogphy [1, 2] and these approaches provide different facilitates.

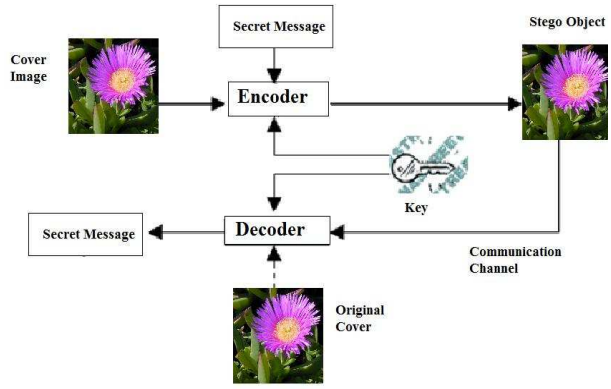

Fig: Steganography working

2. DATA HIDING

There are various technique of data hiding or sending a secret information sender to receiver like cryptography, watermarking, steganography etc [3, 4]. Generally secrete data can be hide behind other text data, image or any electronic media like audio or video. Audio and video is an electronic media. Electronic data often includes redundant, unnecessary and unnoticed data spaces which can be manipulated in order to hide messages.

3. LITERATURE SURVEY

3.1 Audio Steganography

Audio steganography is a process of hiding secret information in an innocent cover audio file. In audio steganography sound file is modified in a a way they contain a hidden information [5]. This modification done in such a way that secrete data must be secure and without destroying the original signal. Embed a data in an audio file use the properties of the Human Auditory System (HAS). The HAS perceives the random noise and also the perturbations in a sound file can also be detected. There are different format of audio file like WAV, AIFF,AU or MP3.

Audio steganography can be performed in time domain as well as frequency domain. When data hide behind the audio file it create “stego audio file” and then this “stego” audio file send to the receiver. Receiver can recover the data from “stego” audio file by using different algorithm or technique [6].

There are following technique and algorithms are available for hiding a data in audio file.

Phase Coding

Phase coding is one of the important techniques of audio steganography [8] . In phase coding Message [10]

bits are encoded as phase shifts in the phase spectrum of a digital signal.

The following steps must follow:

1) In first step of phase coding original sound is divided into smaller segments whose lengths equal the size of the message to be encoded.

2) After that Discrete Fourier Transform (DFT) applied to each segment and create a matrix of the phases and Fourier transform magnitudes.

3) In next step Phase differences between adjacent segments are calculated.

4) With the new phase matrix and original magnitude matrix, the sound signal is reconstructed by applying the

inverse DFT and then concatenating the sound segments back together.

If receiver want to extract secrete message they must to know length of segment. The receiver use the DFT to get the phases and extract the information

Least Significant Bit Encoding (LSB)

Generally any data byte consist of Least significant bit and Most significant bit .In LSB algorithm data is hide with replacing least significant bit in any byte of cover file or audio file with the byte of secrete data [7,8]. In LSB we hide every byte of secret data in every eight byte of cover file. In LSB coding, the ideal data transmission rate is 1 kbps per 1 KHz. By using LSB large amount of data can be encoded. If the receiver has to extract a secret message from an LSB encoded sound file, he needs access to the sequence of sample indices used in the embedding process.

Echo Hiding

In echo hiding secrete data is embedded into a sound file by using an echo into a discrete signal. There are three important parameter of echo amplitude, decay rate, Video is an electronic medium for the recording, copying and broadcasting of moving visual images. Video is nothing but a set of images. In video steganography secrete data hide in video file [9]. Video file is the collection of frame there are difference type of video files like MPEG, AVI, MOV etc. In this technique first select a frame and position to hide an image pixel.
In videos the number of still pictures per unit of time of video the ranges from six or eight frames per second (frame/s).The quality of picture can be measured with

and offset. To hide a data using this technique the parameter of echo are varied: amplitude, decay rate, and offset (delay time) from the original signal. All these three parameter are set below the human hearing threshold hence echo is not easily resolved. In one echo produced from the original signal, bit by bit information could be encoded [13].

Spread Spectrum

In spread spectrum method secrete message spread across the audio signal's frequency spectrum as much as possible. In this technique secrete message is spread using is spread spectrum.[15] In this technique text is modulated as a result, the final signal occupies a bandwidth in excess of what is actually required for transmission by pseudorandom noise sequence a code which is independent of the actual signal In some area this technique is better than LSB coding and phase coding [16].

The main disadvantages of this system are it can introduce noise into a sound file.

3.2 Video Steganography

formal metrics like PSNR that is Pick Signal Noise Ratio.

There are various technique of Video Steganography. The best technique is that hide
Secret message without affecting the quality of video, structure and content of the video file.
After hiding a secrete data in video create “stego” video file which send to the receiver side [10].

There are following techniques available for video steganography.

Non uniform rectangular partition

This algorithm is used steganography on uncompressed video. In this method we can hide an uncompressed secret video stream in a host video stream with almost the same size. Each frame of both videos as the images and apply the image steganography for each frame with some necessary mechanism. These codes will be hidden in the Least 4 Significant Bits of each frames of the host video.

Compressed Video Steganography

This is the new compressed video steganography method In this method data hiding operations are executed entirely in the compressed formed data are embedded in the macro blocks of I frame with maximum scene change and in block of P and B frames with maximum magnitude of motion vectors. Data can be also hide in compressed video using some secrete key [11].
For video compression H.264/advanced video coding (AVC) is the latest method for video compression with high compression efficiency

Least Significant Bit Encoding (LSB)
When used 24 bit color image it's consist each pixel consist of three bit of Red, Green and blue.
Supposed we want to hide **A** which binary equals 10000001.
This inserted into following grid

(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)

4. CONCLUSION

Here we need to change only three bit to insert the character. So only half of the bit in an image will need to be modified to hide a secret message using the maximal cover size[12]. Change made in least significant bit is too small to be recognized by the human eye, so the message is Effectively hidden [10].

Masking and filtering

Masking and filtering technique generally used with 24 bit or grey scale images, take a different approach to hiding the message. These methods are similar to watermarking, creating markings in an image [10]. Masking does change the visible Properties of an image; it can be done in such a way that the human eye will not notice the anomalies. it is more robust than LSB modification with respect to compression, cropping and different kinds of image processing.

3.4 ANTI FORENSICS TECHNIQUE

Anti-forensics makes investigations on digital media. There are some steps summarized as "Identification," "Acquisition," "Analysis" and "Reporting,". Computer anti forensics is as investigator worst nightmare. There are some that a make it hard or impossible to retrieve information during an investigation. There are many sub category of anti forensics technique. Steganography is a technique where information or files are hidden within another file. Using steganography and anti forensics technique communication between sender and receiver can be more secure.
Information security using data hiding audio video steganography provide better

hiding capacity and security. Hiding image and text behind video or audio file and extracted from a file using various techniques. We can hide encrypted data using steganography and cryptography behind selected frame of video and selected segment of audio. Not only text data but also images can also be hiding behind audio or video. Hench we can share a secrete data between sender and receiver using an electronic media like audio or video.

5. REFERENCES

[1] Shaveta Mahajan, Arpinder Singh, " A Review of Methods and Approach for Secure Stegnography", IJARCSS***E*** International Journal of Advanced Research in Computer Science and Software Engineering,vol 2,issu 10,oct 2012, ISSN: 2277 128X

[2] Budda Lavanya, 2 Yangala Smruthi, 3 Srinivasa Rao Elisala," Data hiding in audio by using image steganography technique", IJETTCS International Journal of Emerging Trends & Technology in Computer Science Volume 2, Issue 6, November – December 2013

[3] Dr.K.Sathiyasekar, S.Karthick Swathy Krishna K S," a research review on different Data hiding techniques" ,IJECS International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 3 Issue 1, Jan 2014 Page No. 3655-3659

[4] Komal Patel1, Sumit Utareja2, Hitesh Gupta3," Information Hiding Techniques", IJETAE International Journal of Emerging Technology and Advanced Engineering Volume 3, Issue 1, January 2013

[5] Nagaseshu.K, Srinivasa Rao.V , Hima Deepthi.V," A Novel Approach for Embedding Text in Audio to Ensure Secrecy", IJCSIT International Journal of Computer Science and Information Technologies, Vol. 2 (4) , 2011, 1592-1594

[6] Kamalpreet Kaur DeepankarVerma," Multi-Level Steganographic Algorithm for Audio Steganography using LSB, Parity Coding and Phase Coding Technique", IJARCSSE International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 1, January 2014

[7] Ashwini Mane.*Gajanan ,Galshetwar.**Amutha Jeyakumar" ,Data Hiding Technique: Audio Steganography using Lsb Technique", IJERA International Journal of Engineering Research and Applications, Vol. 2, Issue 3, May-Jun 2012, pp.1123-1125.

[8] Kriti Saroha Pradeep Kumar Singh, "A Variant of LSB Steganography for Hiding Images in Audio ", IJCA,International Journal of Computer Applications Vol1– No.6, December 2010

[9] Xuejun Zhang, Xiang Xie," Data Hiding System Based On New Multiple Echo Hiding Method", ICSV21 The 21st International Congress on Sound and Vibration, Beijing, China, 13-17 July 2014

[10] Arup kumar Bhaumik, Minkya choi, "Data hiding in video" IEEE International journal of da ta base a application,vol.2no.2 june 2009.pp.9-15

[11] Sherly A P and Amritha P P," A Compressed Video Steganography using TPVD", IJDMS International Journal of Database Management Systems Vol.2, No.3, August 2010

[12] Hemant Gupta, Setu Chaturvedi , " Video Steganography through LSB Based Hybrid Approach " ,IJCSNS International Journal of Computer Science and Network Security, VOL.14 No.3, March 2014

[13] Matthew CStamm,KJ Ray Liu, "Forensic detection of image manipulation using Sta tistical intrinsic fingerprints"lEEE transction on information forensic and security,Vol No.3 September 2010,pp492-506.