ISSN : 2231-0711
Nishant Sharma et al | IJCSET(www.ijcset.net) | June 2015 | Vol 5, Issue 6, 138-141

Review: To Study Scope of Data Hiding in MP3 Files

*Nishant Sharma **Er. Gaurav Deep

*Student (M.Tech), Deptt. Of Computer Engg,
Punjabi University
**Asst. Professor, Deptt. Of Computer Engg,
Punjabi University, Patiala

Abstract: **Steganography is a kind of secret communication method used to hide secret data in some digital media such as images, audio etc. Hiding secret data using audio files as carrier is known as "Audio Steganography". The availability and the popularity of audio files make them eligible to carry hidden information, and thus hold significance. With the advancement in digital audio media, many audio steganography techniques have been developed and also used. After the events of September 11, 2001, there was immediate concern voiced regarding the possible use of steganography by the al Qaida network. There has been additional concern voiced regarding the television broadcast of bin Laden. There is the possibility that there could have been hidden messages in the audio portion of the broadcasts. MP3 file format has been very popular since its inception due to its ability to minimize the file size without compromising audible quality. Several techniques have been devised for steganography in mp3 files. One such padding byte stuffing techniques hides data by replacing padding byte in a MP3 frame by secret data. In this paper, we look at various audio steganography techniques and we study about MP3 files and techniques for data hiding in MP3 files. We study about concept of padding in MP3 file and how this can be used to implement steganography in MP3 file.**

1. INTRODUCTION

Steganography is the science of hiding information so that it remains undetected except by its intended receiver. Need of steganography arises when one needs to communicate privately and he cannot risk to arouse the suspicion by sending encrypted message in plain sight. The main goals of steganography are:

1. Data must remain hidden.
2. Data should be visible, but not recognizable.
3. It should provide better imperceptibility.
4. Data should be hidden directly in carrier.
5. Quality of carrier should not be compromised.

Steganography in digital media, also known as "audio steganography" is hiding some message in audio files. Steganography techniques are mostly used for images there are not many methods for audio steganalysis. Thus, audio Steganography provides considerably better security. Three major parameters to compare audio steganography techniques with each other are:

1. Perceptual Transparency: Stego file and original cover file should be indistinguishable.
2. Robustness: Capability to face intentional/unintentional attacks such as resampling etc.
3. Capacity: Amount of data that can be embedded without compromising perceptual transparency.

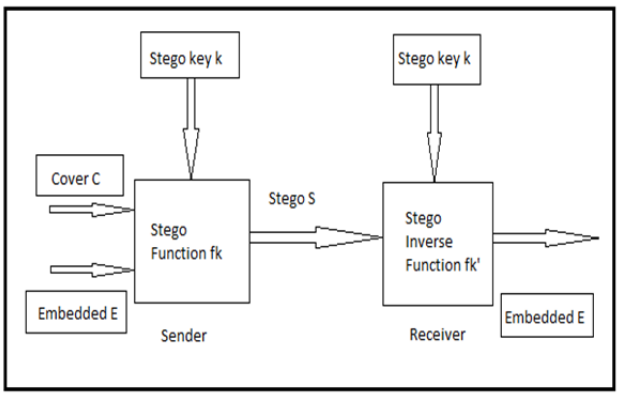

Fig.1 Steganography model

Various audio steganography techniques with their advantages and drawbacks have been listed in table1.

In audio Steganography, many types of file can be used as a cover of steganography such as Waveform Audio File Format (WAVE, or more commonly known as WAV due to its filename extension) or MPEG-1 or MPEG-2 Audio Layer III (MP3). Similarly, secret messages that are embedded can be of secured types such as text or speech.

MP3 file format – MP3 refers to layer 3 [highest complexity] of MPEG – 1 compression mode. The mp3 format has been designed to store audio data, which is different from visual information stored in images. Therefore image stegonography techniques may not always work with audio data. Furthermore, unlike some image data formats, mp3 files are compressed and encoded in a very storage-conscious way. Thus they are not the best host files for stegonographic data. Though it is considered lossy, it can achieve transparent or perceptually lossless compression.

MP3 file structure: The content of MP3 file depends on the type of encoding used. The common structures of MP3 files consist of three components:

a. Tags
b. Padding bytes
c. Frames

Methods	Embedding techniques	Advantages	Drawbacks
LSB encoding	LSB of each sample is replaced by one bit of hidden information	easy way of hiding Information, high bit rate	Easy to extract and to destroy
Parity coding	Encodes each bit from the secret message in a sample region's parity bit	More choice in encoding the secret bit, Signal can be changed in unobtrusive fashion.	If secret message is resampled, embedded message is lost.
Phase coding	Modulate the phase of the cover signal	Robust against signal processing Manipulation, data retrieval needs original signal	Low capacity
Spread Spectrum	Spread the data over all signal frequencies	Provide better robustness	Vulnerable to time scale modification
Echo hiding	Embeds data by introducing echo in the cover signal	Resilient to lossy data compression Algorithms	Low security and Capacity

Table1. Audio steganography techniques

Tags are of two types: ID3V1 and ID3V2.
Tags in mp3 file usually carry metadata information such as artist name, track name etc. ID3V1 tags are of static size and also less flexible. ID3v2 on the other hand are more flexible. Also, ID3V2 has its own frames which can store data, so they can be used for steganographic purposes.
Padding byte provides additional data embedding; the data provided are added to the frame. Its working principle is that on the event of the encoding, additional data are evenly filled to the frame; this byte can be found in Constant Bit Rate (CBR) so as to ensure that frames are of the same size.
Frames: MP3 audio file is just built up from a succession of smaller parts called frames. Each frame is a data block with its own header and audio information. There is no main header in mp3. While retrieving information about an MP3 audio file, we need to simply locate the first frame, and retrieve information from its header. Information within other frames should be consistent with the first one, except for the bitrate, if it is a variable bitrate (VBR) file.
MP3 Encoding: MP3 encoding refers to quality enhancer of both compressed sound and the size of compressed sound file. The three encoding bit rates used by different encoders include the CBR, Variable Bit Rate (VBR) and Average Bit Rate (ABR). CBR refers to a standard encoding mechanism used by basic encoders. In this encoding mechanism, each frame used the same bit rate in the audio data. The bit rate is fixed in the whole of MP3 file, as the same number of bits is used for each part of the MP3 file. However, the quality of MP3 is variable. These techniques can be used to predict the size of encoded file and can be calculated by multiplying the bit rate chosen to encode with the length of a song. VBR is a technique that can keep the quality of audio files during the encoding process. In this technology the quality of the sound can be specified but the size of the sound file remains unpredictable. ABR is a mode that uses higher bit rate for the part of music by choosing the encoder adds bits. The final result showed that the quality is higher than CBR. Moreover, the average file size remains predictable.
Techniques used for steganography have been classified in three categories:

1. Embedding before compression. This category includes methods that hide secret data in metadata of mp3 file such as in ID3V1/ID3V2 tags or in song lyrics.
2. Embedding during compression. This category includes general audio steganography techniques described earlier.
3. Embedding after compression. This category includes techniques that work with mp3 file after it is compressed. Not much research has been done in this area. This is due to the fact that these techniques are difficult to implement and sometimes desirable results are not achieved.

Padding byte stuffing technique comes under third category. To understand this, one should be familiar with

MP3 file structure and padding bytes. As an example, let us take a file with bitrate as 128k and with sample rate 44kHz. Now frame length for such file is 418 bytes. Now some frames actually has 417 bytes and to fit the bitrate as 128K, these frames are padded with extra byte.

There are various challenges in working with padding byte stuffing technique. There has not been much research in this area so information regarding this technique is limited. Furthermore, there is limited information about how frames are padded. One can assume that one byte is added at the end of frame, but that does not necessarily be true in all cases. To find information about a MP3 file, we need to read its header, and that will give the information about frames in the file. Now each frame needs to be checked for padding bit, that is whether padding bit has been added or not. After identifying the frames without padding bytes, we need to replace those bytes with our secret message. This itself poses a big challenge. So, there are many challenges related to this technique but if we overcome those challenges, it will surely be a big step forward in an area which has not been explored much.

2. LITERATURE SURVEY

AUTHOR NAME	YEAR	TITLE	WORK DONE BY AUTHOR	RESULT ANALYSIS
Huynh Ba Dieu,Nguyen Xuan Huy	2014 IEEE	An improved technique for hiding data in audio	Author presents an improved technique for hiding data in audio that modifies the amplitude of the cover audio to embed the secret message and increases the security by using a secret key. Results show that the proposed method is inaudible and suitable for hiding data in audio.	The experiment shows that our method is secure, imperceptible and can be used for hiding data in the audio file.
Neha Gupta, Ms. Nidhi Sharma	2014 ICROIT	DWT and LSB based audio steganography	The author proposes a system that uses the concept of DWT (Discrete Wavelet Transform) and LSB (Least Significant Bit)to develop a new method of Audio Steganography. Paper focuses on hiding an image in audio file and comparing it with simple LSB technique.	Taking Peak signal to noise ratio as a measure, we see that there is no audiblbe difference in the audio file before and after hiding the image.
Rohit Tanwar, Monika Bisla	2014 ICROIT	Audio Steganography	In this paper, author presents us with different techniques that can be applied over a audio file to hide data in it. Each method has been described in detail with its merits and demerits.	Audio steganography is more challenging than its counterparts, as Human Auditory System is more sensitive than Human Visual System. Each technique has its own merits and demerits and their usage depends upon various parameters such as need of security, length of message etc.
Mohammed Salem Atoum, Subariah Ibrahimn, Ghazali Sulong, Akram Zeki, Adamu Abubakar	2013 IEEE	Exploring the challenges of audio steganography	This paper presents the issues and challenges faced for steganographic techniques that uses MP3 files as the cover or carrier file. Some techniques for data hiding in MP3 are reviewed, and the possibility of finding other new techniques hiding information in MP3 files has been reviewed..	MP3 files can be embedded before, during and after compression. After compression is the best strategy among them because of high robustness and security.
Mohammed Salem Atoum, Subariah Ibrahim, Ghazali Sulong3 and Ali M-Ahmad	2012 IJCSI	MP3 steganography review	Author presents a thorough analysis on the techniques used in audio files technologies, with more emphasis on MP3 steganography technique. Detailed information about MP3 has also been provided.	This paper reviewed existing steganography techniques that can be used with MP3 as carrier file. Conclusion on each technique Have been drawn that could likely offer better results
Xuping Huang, Ryota Kawashima, NorihisaSegawa, Yoshihiko Abe	2013 IEEE	Design and implementation of synchronized audio to audio steganography scheme	Author proposes a synchronized steganography system for acoustic data such that the secret data is to be recorded and steganographically embedded and subsequently sent or broadcasted to multiple receivers.	Author has developed a synchronized audio-to-audio steganography Solution in which secret speech data is recorded and embedded into audio data when it is playing. Results show that it is difficult to realize the difference by human perception.

3. CONCLUSION

While doing this literature review, we come to know about various techniques that are being used for audio steganography. Steganography is an area that holds its significance because it relates to security. Due to this, it also needs development with changing times. So, various other techniques are coming into play and many other areas are being discovered to hide data in audio files. Padding byte stuffing technique is one such area, and it can be avenue for future research work. However there are challenges to it, which if we overcome, it will be a big step forward in information security. We need accurate methods for finding exact location of paddings in mp3, and also we need to reduce signal-to-noise ratio.

REFERENCES

[1]. Mohammed Salem Atoum, Subariah Ibrahim, Ghazali Sulong3 and Ali M-Ahmad, "MP3 steganography : review", IJCSI, Nov. 2012

[2]. Mohammed Salem Atoum, Subariah Ibrahimn, Ghazali Sulong, Akram Zeki, Adamu Abubakar, "Exploring the challenges of mp3 steganography", International Conference on Advanced Computer Science Applications and Technologies, 2013

[3]. Rohit Tanwar, Monika Bisla, "Audio Steganography", ICROIT 2014

[4]. Ritej Gaba, Gaurav Deep, "Comparison of various video steganography techniques", IJAIR 2013

[5]. Huynh Ba Dieu, Nguyen Xuan Huy, "An Improved Technique for Hiding Data in Audio", 2014 IEEE

[6]. Neha Gupta, Ms. Nidhi Sharma, " DWT and LSB based audio steganography", 2014 ICROIT

[7]. Xuping Huang, Ryota Kawashima, Norihisa Segawa, Yoshihiko Abe, "Design and implementation of synchronized audio to audio steganography scheme", 2008 IEEE

[8]. James C. Judge, "Steganography: past, present and future", SANS institute

[9]. Padding bytes, Nov 2014, URL: www.compuphase.com/mp3/mp3loops.htm