AUDIO STEGANOGRAPHY FOR HIDING SECRET MESSAGE IN AUDIO

Pushnay Bhutada*, **Prof. Akshay Dhande****
*(P.G. Student, Electronics and Telecommunication department, P. R. Patil College, Amravati, India
Email: pushnaybhutada@gmail.com)
** (Associate professor, Electronics and Telecommunication department, P. R. Patil College, Amravati, India)

------------------------------*************************--------------------------------

Abstract:

In today's world internet applications requires data to be transmitted in a secure manner. Data transmission in public communication system is not secure because of interception and improper manipulation. Audio steganography deals with a method to hide a secret message in an audio file. Also, Audio steganography can be used for secret watermarking or concealing ownership or copyright information in the audio that can be verified later to justify ownership right. A direct Least Significant Bit (LSB) substitution method is one of the most simple and popular techniques used for audio steganography. Audio steganography is the scheme of hiding the existence of secret information by concealing it into another medium such as audio file.

Keywords - **Audio Steganography, LSB, Data Hiding, Security.**

------------------------------*************************--------------------------------

I. INTRODUCTION

Steganography is an art of hiding a secret message in another message which everybody does not know about presence of the secret message except the intended receiver. The message used to hide the secret message is called a host message or cover. The secret message can be a text, image, audio, or video. The combination of host message and secret message is called stego message. Image, audio and video files are considered as excellent cover files due to presence of redundancy. The hidden data can only be visible to the sender and the receiver of the message. The hidden information is encrypted by using encryption mechanisms no-one can even find that there is hidden information behind the cover file.

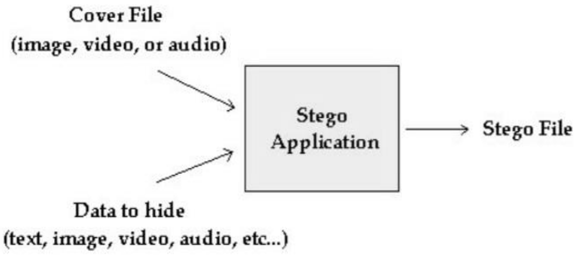


Fig1. Basic Steganography Model

The steganography application hides different types of data within a cover file. The resulting stego also contains hidden information, although it is virtually identical to the cover file. What Steganography essentially does is exploit human perception; human senses are not trained to look for files that have information hidden inside of them.

II. LITERATURE REVIEW

In the process of steganography, the message is used to embed on the cover file and the hidden message is known as the host message or cover message. When the cover message is modified then the resultant message is known as stego-message. In simple words, it can be said that the combination of stego message and cover message results to the stego message. In the case of audio steganography, the message and cover file both are in audio formats. Due to the replication, the cover audio message before the process of steganography and the stego message after the process of steganography remains similar.

A. Binny and M. Koilakuntla [3] presented an audio steganography technique by using the LSB technique. This technique hides the text data in an audio cover file. In this work, the audio signals were first converted to the bits and then the textual message was embedded. While embedding, the text is converted to the binary format. With the help of developed mechanisms, it has been seen that the data hiding capacity had been increased. After implementation, the performance evaluation was done in terms of SNR.

K. Kaur and D. Verma [5] had proposed a multi-level steganography algorithm by implementing three of the most prominent techniques i.e. LSB, parity coding and phase coding. This technique had the advantage that it is difficult to decode the message by an unauthorized person. The study had also represented a review of the three-layered audio steganography approach for multi-level steganography. The study was found to be effective to attain higher security.

S. Divya and M. R. M. Reddy [6] had developed a substitution mechanism for audio based steganography with the objective to enhance the capacity of cover audio for embedding the additional data on it. The LSB data embedding technique was used up to 7 LSBs to hide the data. The implementation analysis was done for multiple lengths and variable length LSBs. On the basis of the obtained results, it was concluded that the data hiding capacity of the proposed work was 35% to 70% higher than the standard LSB algorithm.

A. Nagarajan and K.Alagarsamy [8], gave a novel idea for audio steganography by utilizing the enhanced run length encoding algorithm. The author had focused to overcome the backlogs of run-length encoding scheme with the perspective of data compression. The major steps of the technique were to apply the ERLE encoding to the byte level, layer partition, to assign alpha index value, to organize the separated layer the link list data structure was used, data storage and decoding.

In the process of steganography, the message is used to embed on the cover file and the hidden message is known as the host message or cover message. When the cover message is modified then the resultant message is known as stego-message. In simple words, it can be said that the combination of stego message and cover message results to the stego message. In the case of audio steganography, the message and cover file both are in audio formats. Due to the replication, the cover audio message

before the process of steganography and the stego message after the process of steganography remains similar. Various kinds of audio steganography techniques are presented with their pros and cons in [2].

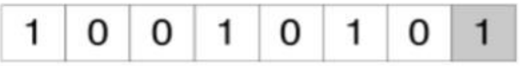
III. PROPOSED WORK & METHODOLOGY

The watermarking of audio signals is a challenge because we have to concentrate on some parameters very effectively such as the quality of signal should not reduce embedding messages in the form of a watermark on it. The power range for sound should be greater than 109:1 & the range of frequencies for it should be greater than 103:1, signal to noise ratio should be greater than 20 dB. The sensitivity of the human audio system to the AWGN noise, i.e. additive white Gaussian noise should be as low as 70 dB below ambient level so that noise level should be low and the quality of audio signal remains good in strength. There is a large variety of techniques available that can be used for hiding the information behind an audio cover file without affecting its signal quality. These techniques enable the sender to hide the data so efficiently that the alterations performed on the audio file are indiscernible and it is not detectable by the third party [6], [8]. The categorization of audio steganography techniques can be done on the basis of different domains such as time-based domain, frequency based domain, transformation-based domain, etc.

Least Significant Bit (LSB) Coding Method

A very popular methodology is the LSB (Least Significant Bit) algorithm, which replaces the least significant bit in some bytes of the cover file to hide a sequence of bytes containing the hidden data. That's usually an effective technique in cases where the LSB substitution doesn't cause significant quality degradation, such as in 24-bit bitmaps. . In this technique the user can convert the image into audio and audio into the image by replacing the least significant bits in the cover file in order to embed a sequence of bytes [3]. This is performed to upsurge safety by reshuffling the information message before hiding it to the audio document. This is done to secure the data from the attacker. In case the attacker comes to know about the hidden data, then he will not be capable to crack the originality of data as it is in the coded format. This happens because of the shuffling of the message that is performed by the dynamic generation of the random sequence. The random sequence generation relies upon the criteria of file selection for hiding the data. That is normally a successful procedure in situations where the LSB substitution doesn't cause quality degradation as there is a high channel bit rate. In terms of computing, the LSB can be defined as the bit position in a binary integer with respect to the available unit value which evaluates whether the number is odd or even. Therefore, its complexity is lower and consumes less time and less delay for data hiding and extracting.

In computing, the least significant bit (LSB) is the bit position in a binary integer giving the units value, that is, determining whether the number is even or odd. The LSB is sometimes referred to as the right-most bit, due to the convention in positional notation of writing less significant digit further to the right. It is analogous to the least significant digit of a decimal integer, which is the digit in the ones (right-most) position.



1	0	0	1	0	1	0	1

Fig 2. Binary representation of decimal 149

The binary representation of decimal 149, with the LSB highlighted. The MSB in an 8-bit binary number represents a value of 128 decimal. The LSB represents a value of 1. For example, to hide the letter "a" (ASCII code 97, which is 01100001) inside eight bytes of a cover, you can set the LSB of each byte like this:

10010010

01010011

10011011

11010010

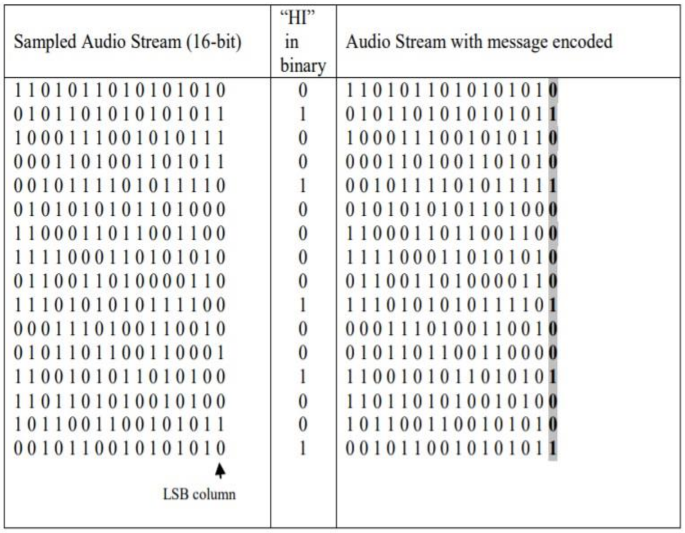
10001010

00000010

01110010

00101011

The application decoding the cover reads the eight Least Significant Bits of those bytes to recreate the hidden byte—that is 0110001—the letter "a." As you may realize, using this technique let you hide a byte every eight bytes of the cover. Note that there's a fifty percent chance that the bit you're replacing is the same as its replacement, in other words, half the time, the bit doesn't change, which helps to minimize quality degradation.



Sampled Audio Stream (16-bit)	"HI" in binary	Audio Stream with message encoded
1101011010101010	0	1101011010101010
0101101010101011	1	0101101010101011
1000111001010111	0	1000111001010110
0001101001101011	0	0001101001101010
0010111101011110	1	0010111101011111
0101010101101000	0	0101010101101000
1100011011001100	0	1100011011001100
1111000110101010	0	1111000110101010
0110011010000110	0	0110011010000110
1110101010111100	1	1110101010111101
0001110100110010	0	0001110100110010
0101101100110001	0	0101101100110000
1100101011010100	1	1100101011010101
1101101010010100	0	1101101010010100
1011001100101011	0	1011001100101010
0010110010101010	1	0010110010101011
LSB column		

Fig 3. LSB Coding Example for HI Message

Steps to hide secret information using LSB are:

a. Covert the audio file into bit stream.
b. Convert each character in the secret information into bit stream.
c. Replace the LSB bit of audio file with the LSB bit of character in the secret information.

This proposed method provides greater security and it is an efficient method for hiding the secret information from hackers and sent to the destination in a safe and undetectable manner.

IV. AUDIO STEGANOGRAPHY APPLICATIONS

Audio data hiding can be used anytime you want to hide data. There are many reasons to hide data but most important is to prevent unauthorized persons from becoming aware of the existence of a message. In the business world Audio data hiding can be used to hide a secret chemical formula or plans for a new invention [9, 7]. Audio data hiding can also be used in the noncommercial sector to hide information that someone wants to keep private. Terrorists can also use Audio data hiding to keep their communications secret and to coordinate attacks. Data hiding in video and audio is of interest for the protection of copyrighted digital media, and to the government for information systems security and for covert communications [8]. It can also be used in forensic applications for inserting hidden data into audio files for the authentication of spoken words and other sounds, and in the music business for the monitoring of the songs over broadcast radio.

V. CONCLUSIONS AND FUTURE WORK

Information security is very important since information is exchanged on the publicly accessible Internet. Both cryptography and steganography can be used to provide information security. Steganography techniques allow hiding valuable information in an apparently innocent document. A well-defined audio steganography scheme should satisfy at least three requirements: capacity, transparency and robustness. This scheme not only hides a secret message as big as possible but also minimizes distortion in the resultant audio as much as possible to avoid detection. This scheme can be used to embed one or many secret bits in a cover audio sample depending on the relative strength of the audio sample as the sample is measured against a scale of multi-level threshold value. The future research can combine some cryptographic techniques with this scheme. In that situation, if hackers can retrieve the secret message, they will not be able to reveal the secret message due to encryption. Another extension to this work would be to select samples chaotically instead of sequentially during embedding of the secret message bits.

REFERENCES

[1]. Jintao Zhou, Wee-wee Sun, Li Dong,Xian Ming Liu, OscarTareekPattewar C. Au, Yuan Yan Tang, "Secure Reversible Image Data Hiding over Encrypted Domain via Key Modulation", IEEE, 2014.

[2] P. Jayaram, H. R. Ranganatha, H.S. Anupama, “Information Hiding Using Audio Steganography –A Survey”, International Journal of Multimedia & Its Application, Vol.3, No.3, pp.86-96, 2011.

[3] A.Binny, M. Koilakuntla, “Hiding secret information using LSB based audio steganography”, IEEE International Conference on Soft Computing & Machine Intelligence, pp.56-59, 2014.

[4] Sajad Shirali-Shahreza M.T. Manzuri-Shalmani “High capacity error free wavelet domain speech steganography” ICASSP 2008.

[5] K. Kaur, D. Verma, “Multi-Level steganographic algorithm for audio steganography using LSB, parity coding and phase coding technique”, International Journal of Advanced Research In Computer Science and Software Engineering, Vol.4, No.1, 2014.

[6] S. Divya, M. R. M. Reddy, “Hiding text in audio using multiple LSB steganography and provide security using cryptography”, International Journal of Science and Technology Research, Vol.1, No.6, 2012.

[7] M. Nosrati, R. Karimi, M. Hariri, “Audio Steganography: A Survey on Recent Approaches”, World Applied Programming, Vol.2, No.3, pp.202-205, 2012.

[8] A. Nagarajan, K.Alagarsamy, “An Enhanced Approach in Run Length Encoding Scheme (EARLE)”, International Journal of Engineering Trends and Technology, pp.43-48, 2011.

[9] Sheelu, “Enhancement of Data Hiding Capacity in Audio Steganography”, IOSR Journal of Computer Engineering (IOSRJCE), Vol.13, No.3, pp.30-35, 2013.

[10] N. Cvejic, T. Seppanen, “ Digital Audio Watermarking Technique and Technologies: Applications and Benchmarks”, Book 2007.