Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 4, April 2015, pg.221 – 228

RESEARCH ARTICLE

DATA SECLUSION IN AUDIO WAVE FILE

Ms. Sejal V. Gawande[1], Dr. Prashant R. Deshmukh[2]
[1]Student, Computer Science and Engineering, Sipna C.O.E.T., Amravati, Maharashtra, India
[2]Professor, Computer Science and Engineering, Sipna C.O.E.T., Amravati, Maharashtra, India
[1] gawandesejal@gmail.com; [2] pr_deshmukh@yahoo.com

Abstract— Secret data hiding in Audio Files is more difficult than other formats since Audio Files require only one bit representation to indicate 0 and 1. The main intention this paper is to propose a new method for data hiding in binary Audio Files using optimized bit position to replace a secret bit. This method manipulates blocks, which are sub-divided. The parity bit for a specified block decides whether to change or not, to embed a secret bit. Steganography is an art of hiding messages inside an image/Audio file or a video file such that the very existence of the message is unknown to third party. Cryptography is used to encrypt the data so that it is unreadable by a third party. This system combines both the above techniques. To make the system more secured this system uses most powerful way in the first level of security which encrypts the data. In the second level the encrypted data is embedded in to the Audio file using modified LSB.

Keywords— Steganography, cryptography, Audio file, LSB, data hiding in binary Audio Files

I. INTRODUCTION

The fast improvement of the Internet and the digital information revolution caused major changes in the overall culture. Flexible and simple-to-use software and decreasing prices of digital devices have made it feasible for consumers from all over the world to create, edit and exchange multimedia data. In modern communication system Data Hiding is most essential for Network Security issue. Sending sensitive messages and files over the Internet are transmitted in an unsecured form but everyone has got something to keep in secret. Audio data hiding method is one of the most effective ways to protect your privacy.

A. Need of steganography

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. This technique relies on a message being encoded and hidden in a transport layer in such a way as to make the existence of the message unknown to an observer. Steganography works by replacing bits of useless or unused data in regular computer files.

Steganography hides messages in plain sight rather than encrypting the message; it is embedded in the data and doesn’t require secret transmission. The message is carried inside data. Steganography can be used in a large amount of data formats in the digital world such as .bmp, .doc, .gif, .jpeg, mp3, .txt and .wav. [1, 2, 3]

There are basically three main categories in Steganography. These are as follows:

i. *Pure Steganography*
In pure Steganography, the secret lies in the embedding and extracting algorithms that only the message sender and intended receiver should know.

i. *Secret Key Steganography*
Secret key Steganography is similar to a symmetric cipher. It is assumed that a party other than the sender and intended receiver knows the embedding and extraction algorithms. The sender embeds a message in a cover-object using a secret key known as a stego-key. Therefore, even if a third party intercepts the stego-object and extracts the information, the result will appear to be a random, garbled mess. Only the intended receiver who possesses the same key can extract the original message.

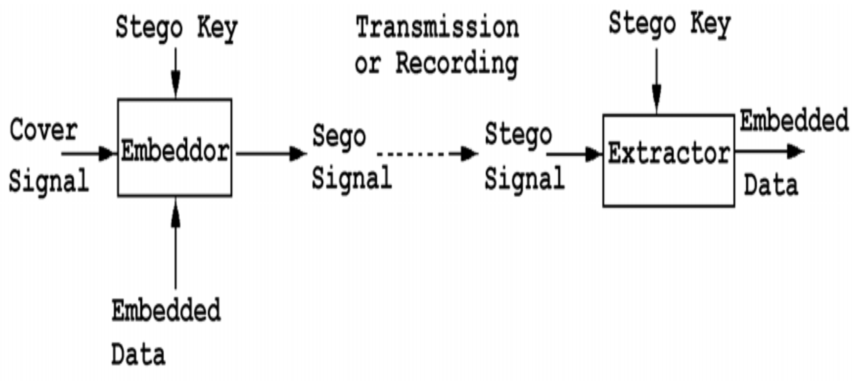

Fig. 1:- Block diagram of data hiding and retrieval.

ii. *Public Key Steganography*
In a public key Steganography system, two keys are used: a private key and a public key. The public key is used in the embedding process, and the private key is used in the extraction process. Public key Steganography allows the sender and receiver to avoid exchanging a secret key that might be compromised.

II. LITERATURE REVIEW

A. *Steganography in audio*

Data hiding in audio signals is specially challenging, because the Human Auditory System (HAS) operates over a wide dynamic range. The HAS perceives over a range of power greater than one billion to one and a range of frequencies greater than thousand to one. The perturbations in a sound file can be detected as low as one part in ten million which is 80dB below ambient level. However there are some 'holes' available. While it has a large dynamic range, it has a fairly small differential range. As a result, loud sounds tend to mask out the quieter sounds. Additionally, the HAS is unable to perceive absolute phase, only relative phase.

Steganography is a type of cryptography in which the secret message is hidden in a digital picture. While cryptography is preoccupied with the protection of the contents of a message or information, Steganography concentrates on concealing the very existence of such messages from detection.

In digital media, Steganography is mainly oriented around the undetectable transmission of one form of information within another. In order for a data hiding technique to be successful it must adhere to two rules:

- The embedded data must be undetectable within its carrier medium. The carrier should display no properties that flag it as suspicious, whether it is to the human visual/auditory system or in increased file size for the carrier file.
- The embedded data must maintain its integrity within the carrier and should be easily removable, under the right circumstances, by the receiving party.

The existing system of Audio Steganography poses more restrictions on the choosing of audio files. User can select only wav files to encode. Further embedding information into sound files is generally considered more difficult than images; according to the human ear is extremely sensitive to perturbations in sound and can in fact detect such turbulence as low as one part in 10 million. The four methods discussed further provide users with a large amount of choice and makes the technology more accessible to everyone.[3, 4]

B. *Types of steganography*

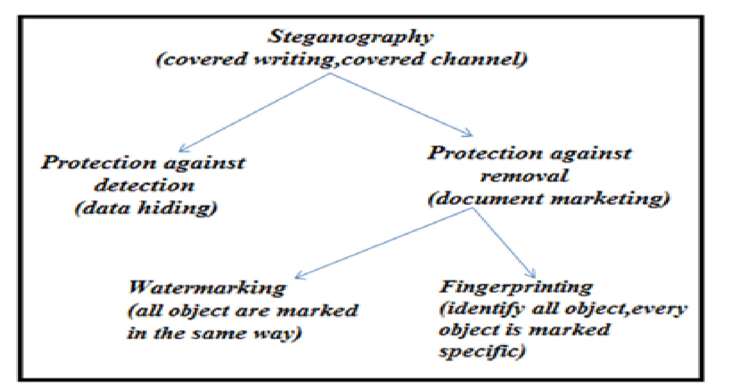
Steganography
(covered writing,covered channel)
Protection against detection (data hiding)
Protection against removal (document marketing)
Watermarking (all object are marked in the same way)
Fingerprinting (identify all object,every object is marked specific)

Fig. 2:- steganography types

There are different types of steganography in which it provides protection against detection and protection against removal. Types of steganography are discussed below:

i. *Spread Spectrum*

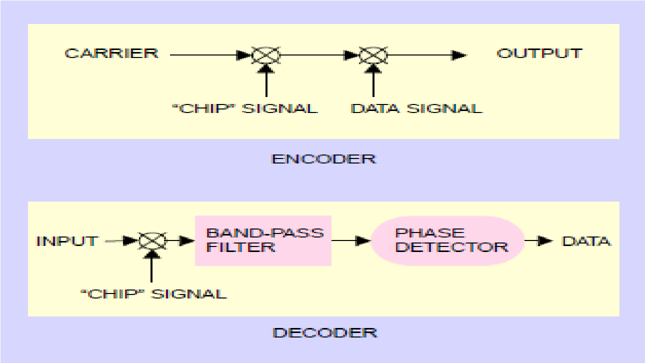

Fig. 3:- spread Spectrum

The basic spread spectrum (SS) method attempts to spread secret information across the audio signal's frequency spectrum as much as possible. The SS method spreads the secret message over the sound file's frequency spectrum, using a code that is independent of the actual signal.

Two versions of SS can be used in audio Steganography: the direct-sequence and frequency-hopping schemes. In direct-sequence SS, the secret message is spread out by a constant called the chip rate and then modulated with a pseudorandom signal. It is then interleaved with the cover-signal. In frequency -hopping SS, the audio file's frequency spectrum is altered so that it hops rapidly between frequencies. [4, 5]

ii. Low-Bit Encoding

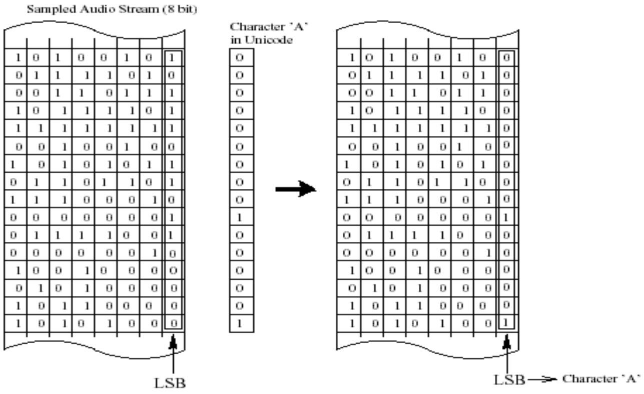

Fig. 4:- Low-Bit Encoding

Low-bit encoding is the one of the simplest way to embed data into other data structures. By replacing the least significant bit of each sampling point by a coded binary string, we can encode a large amount of data in an audio signal. Adaptive data attenuation has been used to compensate this variation. Encoded information can be destroyed by channel noise, re-sampling, etc., unless it is encoded using redundancy techniques.

In some implementations of LSB coding, the two least significant bits of a sample are replaced with two message bits. This increases the amount of data that can be encoded but also increases the amount of resulting noise in the audio file as well. Thus, one should consider the signal content before deciding on the LSB operation to use.

Advantage: Low computational complexity of the algorithm

Disadvantage: As the number of used LSBs during LSB coding increases, depth of the modified LSB layer becomes larger. [4]

iii. Phase Coding

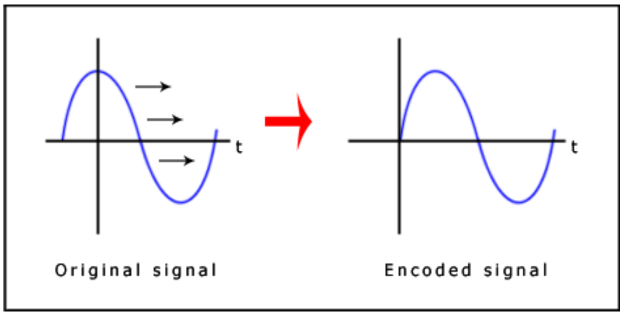

Fig. 5:- Phase Coding

Phase coding relies on the fact that the phase components of sound are not as perceptible to the human ear as noise is. This technique encodes the message bits as phase shifts in the phase spectrum of a digital signal, achieving an inaudible encoding in terms of signal-to-perceived noise ratio.

The phase coding method breaks down the sound file into a series of N segments. A Discrete Fourier Transform (DFT) is applied to each segment to create a matrix of the phase and magnitude. The phase difference between each segment is calculated, the first segment (s0) has an artificial absolute phase of p0 created, and all other segments have newly created phase frames. The new phase and original magnitude are combined to get the new segment, Sn. These new segments are then concatenated to create the encoded output and the frequency remains preserved. In order to decode the hidden information the receiver must know the length of the segments and the data interval used. The first segment is detected as a

0 or a 1 and this indicates where the message starts. Advantage: It is undetectable to the human ear. Weakness: Its lack of robustness to changes in the audio data.[5]

iv. Parity Coding

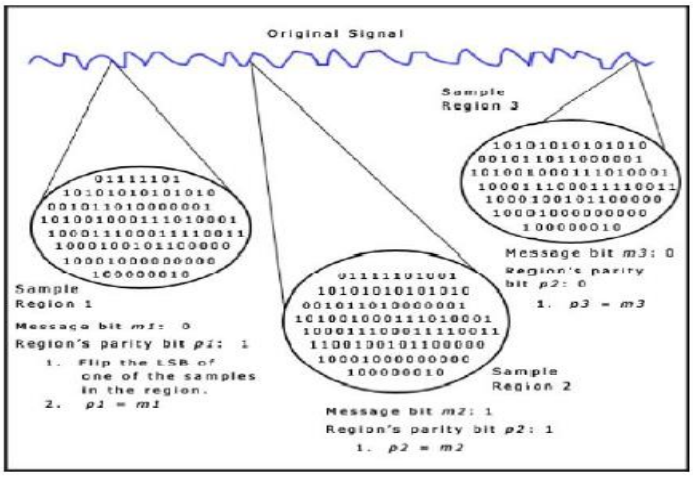

Fig. 6:- Parity Coding

The parity coding method breaks a signal down into separate regions of samples and encodes each bit from the secret message in a sample region's parity bit. If the parity bit of a selected region does not match the secret bit to be encoded, the process flips the LSB of one of the samples in the region. Using the parity coding method, the first three bits of the message 'HEY' are encoded in the above Fig. Even parity is desired. The decoding process extracts the secret message by calculating and lining up the parity bits of the regions used in the encoding process. Once again, the sender and receiver can use a shared secret key as a seed in a pseudorandom number generator to produce the same set of sample regions.[6]

v. Echo Hiding

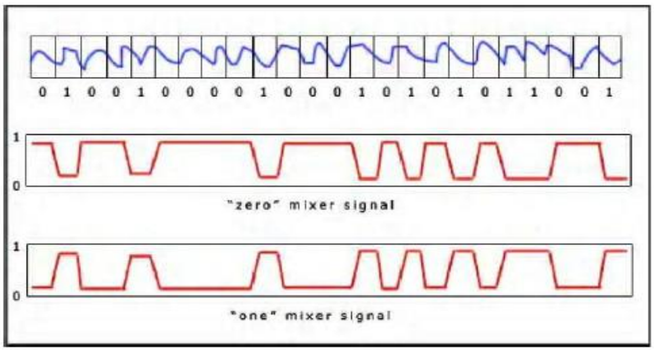

Fig. 7:- Echo Hiding

In echo hiding, information is embedded in a sound file by introducing an echo into the discrete signal. It provides advantages in that it allows for a high data transmission rate and provides superior robustness when compared to the noise inducing methods. To hide the data successfully, three parameters of the echo are varied**:** Amplitude, decay rate, and offset from the original signal. All three parameters are set below the human hearing threshold so the echo is not easily resolved. In addition, offset is varied to represent the binary message to be encoded. One offset value represents a binary one, and a second offset value represents a binary zero.[7, 8, 9]

III.PROPOSED APPROACH

The proposed approach of the system uses Audio file as a carrier medium which add another step in security. The objective is to create a system that makes it very difficult for an opponent to detect the existence of a secret message by encoding it in the carrier medium as a function of some secret key. The system will not change the size of the file even after encoding and also suitable for any type of audio file format. Encryption and Decryption techniques are used to make the security system robust. Low-bit encoding embeds secret data into the least significant bit of the audio file.

The system provides a basic view of audio steganographic process in sender and receiver side. At the sender side the text message is encrypted by symmetric encryption algorithm using a key shared both sender and receiver as shown in below Fig.

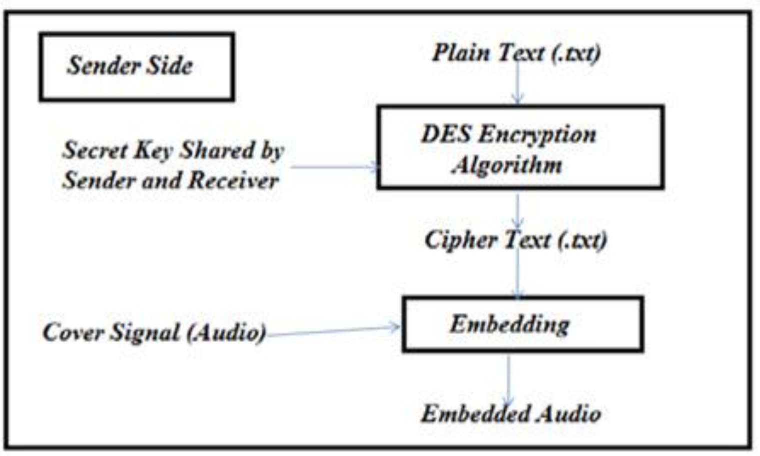

Fig. 8:- Steganographic System at sender side

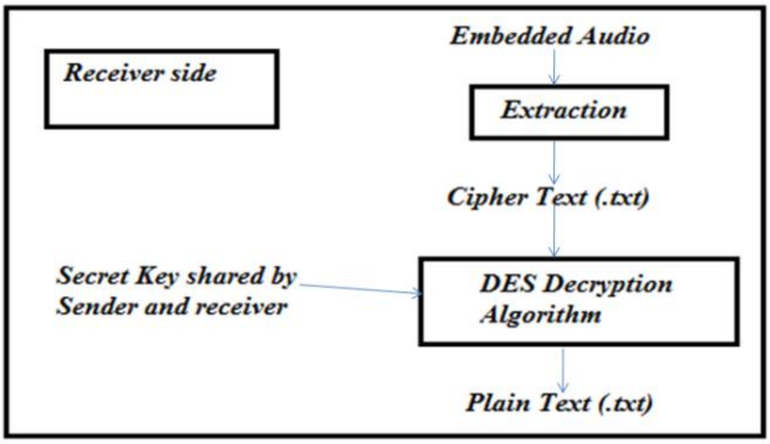

Fig. 9:- Steganographic System at receiver side

Symmetric encryption is an efficient process for providing security to the message. The encrypted text is passed to embedding phase. In embedding phase encrypted text will embedded into the cover signal which is in audio format .wav resulting a stego signal. The embedded audio or stego signal contains the encrypted text message which is extracted at the receiver side. When embedding secret message in audio, the size of the message must be lower than audio signal. At the receiver side, stego signal is passed to extractor phase. In extraction process encrypted text will be extracted from embedded audio signal and encrypted text is decrypted.

In decrypter, encrypted text will be decrypted using shared secret key. In symmetric encryption we use either DES or AES. AES provide more security than DES and also choose key size and block size for both encryption and decryption rest of embedding and extraction process is same for both AES and DES.

A. Steps for embedding data

Embed data(wav file, text file)
Step1:- Select an input audio file for encrypting the data.
Step2:- Select the Message or write a message.
Step2:- Select an output audio file folder.
Step3:- Select or enter text document which we want to encrypt.
Step4:- Select password text file.

Step6:-a) Convert the wave file and message file
(Text file + password) in binary format.
b) Generate the byte array for binary wav file and binary Message file.
Step7:- Replace the every LSB of wave byte array with every bit of message byte array
Step8:- First row LSB of wave byte array will indicate the password is given or not.
Step9:- Message will be embed in the audio file.

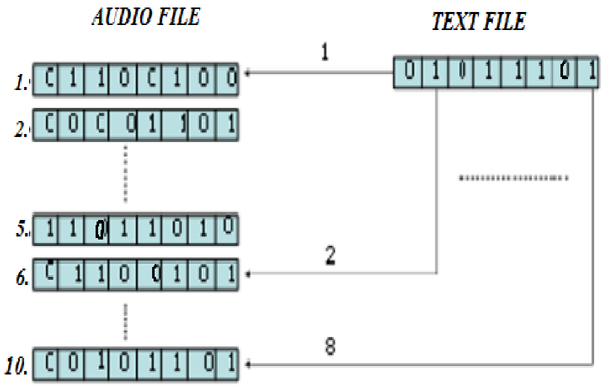

Fig.10:- Encoding text file in to the audio file

B. *Steps for extracting data*

Extract data (wav file, text file)
Step1:- Select an output audio file folder.
Step2:- Select an output text file to extract message
Step4:- Enter the password.
Step5:- The extracting process is start.
Step6:- Audio wave file and text file converted in to binary format. Then extract the byte array of LSB.
Step7:- Every byte array of LSB will be collected as an audio file and saved in binary object and convert into string and store in to text file.
Step8:- object will be readable and text document will be displayed in the notepad file
Step9:- Message is extracted from the audio file.

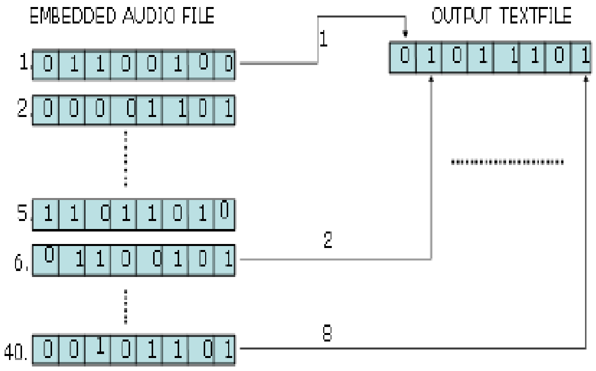

Fig. 11:- Extraction of text file from the audio file

IV. Conclusions

Data security has been a great importance since last few decades. The proposed approach designed for hiding information using Audio Steganography with encrypted data which increases the security of the audio Steganography and a key management is also used in both the sender and receiver to make the system more secured. The system is considered to be an efficient method for hiding text in audio files such that data can reach the destination in a safe manner without being modified. LSB data hiding technique is the simplest method for inserting data into audio signals and cryptography provides the more security for embedded audio file. Two parties can be communicated with a fairly high level of confidence about the communication not being detected.

REFERENCES

[1] Rade Petrovi, Kanaan Jemili, Joseph M.Winograd, Ilija Stojanovi, Eric Metois, "DATA HIDING WITHIN AUDIO SIGNALS", June 15, 1999, MIT Media Lab, Series: Electronics and Energetics vol. 12, No.2, pp. 103- 122.

[2] W. Bender, W. Butera, D. Gruhl, R. Hwang, F. J. Paiz, S. Pogreb, "Techniques for data hiding", IBM Systems Journal, Volume 39 , Issue 3-4, July 2000, pp. 547 – 568.

[3] Robert Krenn, "Steganography and steganalysis", an article, january 2004.

[4] Steve Czerwinski, Richard Fromm, Todd Hodes, "Digital Music Distribution and Audio Watermarking".

[5] Ingemar J. Cox, Ton Kalker, Georg Pakura and Mathias Scheel."Information Transmission and Steganography", Springer,Vol.3710/2005,pp.15-29.

[6] K.Geetha , P.V. Vanthia muthu ," International journal of Computer Science and Engineering" vol 2 No.4 Pg No: 1308-1312 , Year 2010

[7] Samir Kumar Bandyopadhyay, Debnath Bhattacharyya, Poulami Das, Debashis Ganguly and Swarnendu Mukherjee, "A tutorial review on Steganography", International Conference on Contemporary Computing (IC3-2008), Noida, India, August 7-9, 2008, pp. 105-114.

[8] B. Pfitzmann, "Information Hiding Terminology", First International Workshop on Information Hiding, May 30 – June 1, 1996, Cambridge, UK, pp. 347-350.

[9] J. Johnston and K. Brandenburg, "Wideband Coding Perceptual Consideration for Speech and Music". Advances in Speech Signal Processing, S. Furoi and M. Sondhi, Eds. New York: Marcel Dekker, 1992.