International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 1 Issue 8, October - 2012

SECURE COMMUNICATION THROUGH AUDIO SIGNALS

NAMITA VERMA
M.E.(COMMUNICATION)
S.S.C.E.T.BHILAI

MR.VINAY JAIN
ASST. PROFESSOR
S.S.C.E.T.BHILAI

ABSTRACT

The issue of network security of information has gained special significances with the development of computer and the expansion of its use in different areas of life and work. Today's large demand of 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. Steganography is an attractive solution to this problem. In steganography prevents an unintended recipient from suspecting that the data exists. It adds another layer of security since it is much more difficult to decrypt a message if it is not known that there is a message. This paper proposes the basic idea of hiding information (audio, image or text) in cover audio signal. This method is characterized by perfect transparency, robustness, high bit rate, low processing load and high security.

KEYWORDS: steganography, cryptography, LSB technique, wave file

1. INTRODUCTION

In cryptography, the structure of a message is scrambled to make it meaningless and unintelligible unless the decryption key is available. It does not hide the encoded message but prevents a third party from reading it[1].

In steganography, the structure of the secret message is not altered. It hides the secret message inside a cover signal so that it cannot be seen. It prevents an unintended recipient from suspecting that the data exists[2].

Steganography includes a vast array of techniques for hiding messages in a variety of media. Among these methods are invisible ink, microdots, covert channels and digital signature. Due to modern technology, steganography is used on text, images, sound signals and more.

This paper introduces a novel technique of data hiding in wave audio file. The hiding results show no noise that can be heard in the stego-wave file after embedding process.

For all communication means like internet, mobiles, computer etc. the wave files are used commonly. Since the wave file has huge data, it is considered a good carrier of big message. Data hiding in the least significant bits (LSBs) of audio samples in the time domain is one of the simplest algorithms with very high data rate additional information[8]. The proposed method has high bit rate, robustness, high security and low processing load.

BASIC METHOD OF DATA HIDING

Each steganographic technique consists of a data hiding algorithm and data recovery algorithm. The hiding algorithm hides secret message inside a cover document. It is usually protected by a keyword so that the only one who possesses the secret keyword can access the hidden message. The recovery algorithm is applied to the stego document and results the hidden secret message.

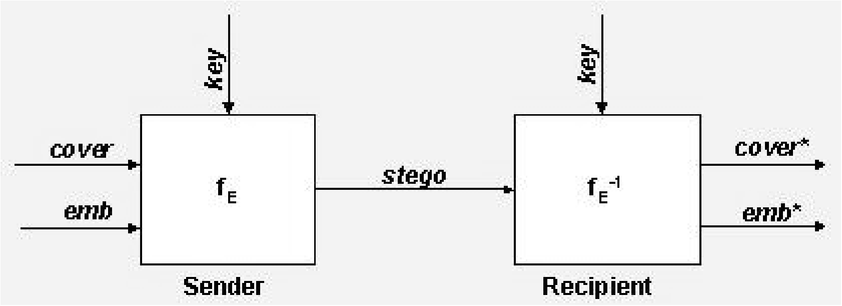


Fig.1.Data Hiding

The process can be represented as[3]

Cover media + embedded message + stego key = stego media

For secure covert communication, it is important that by inserting secret message in cover document, no detectable changes are introduced.

DATA HIDING IN AUDIO SIGNALS

The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data[3].

Presently, audio files are available everywhere and the technology allows the copying and redistribution of audio files over internet etc. at a low cost or almost no cost. So it is necessary to have methods that confines access to these audio files and its security. An effective audio steganography technique should have inaudibility of distortion, data rate and robustness.

The data hiding process consists of two steps as follows:-

1) Identification of redundant bits in a cover file that can be modified without corrupting the quality of the cover file.
2) To embed the secret information in the cover file by replacing the redundant bits in the cover file by the secret information bits.

There have been many techniques for data hiding in audio. The common methods are discussed as follows:-

1. **LEAST SIGNIFICANT BIT(LSB) CODING:-** It is one of the earliest technique studied in information hiding in digital audio etc. Each LSB of sample of digitized audio file is replaced with binary equivalent of the secret message[4]. For example, to hide the letter "a"(ASCII code 97,which is 01100001)into a digitized audio file where each sample is represented with 16 bits, the LSB of 8 consecutive samples is replaced with each bit of binary equivalent of the letter "a".

1001001**0**
0101001**1**
1001101**1**
1101001**0**
1000101**0**
0000001**0**
0111001**0**
0010101**1**

2. PARITY CODING:-This method breaks a signal into separate samples and embeds each bit of the secret message from a parity bit. If the parity bit of a selected region does not match secret bit to be encoded, the process inverts the LSB of one of the samples in the region[5].

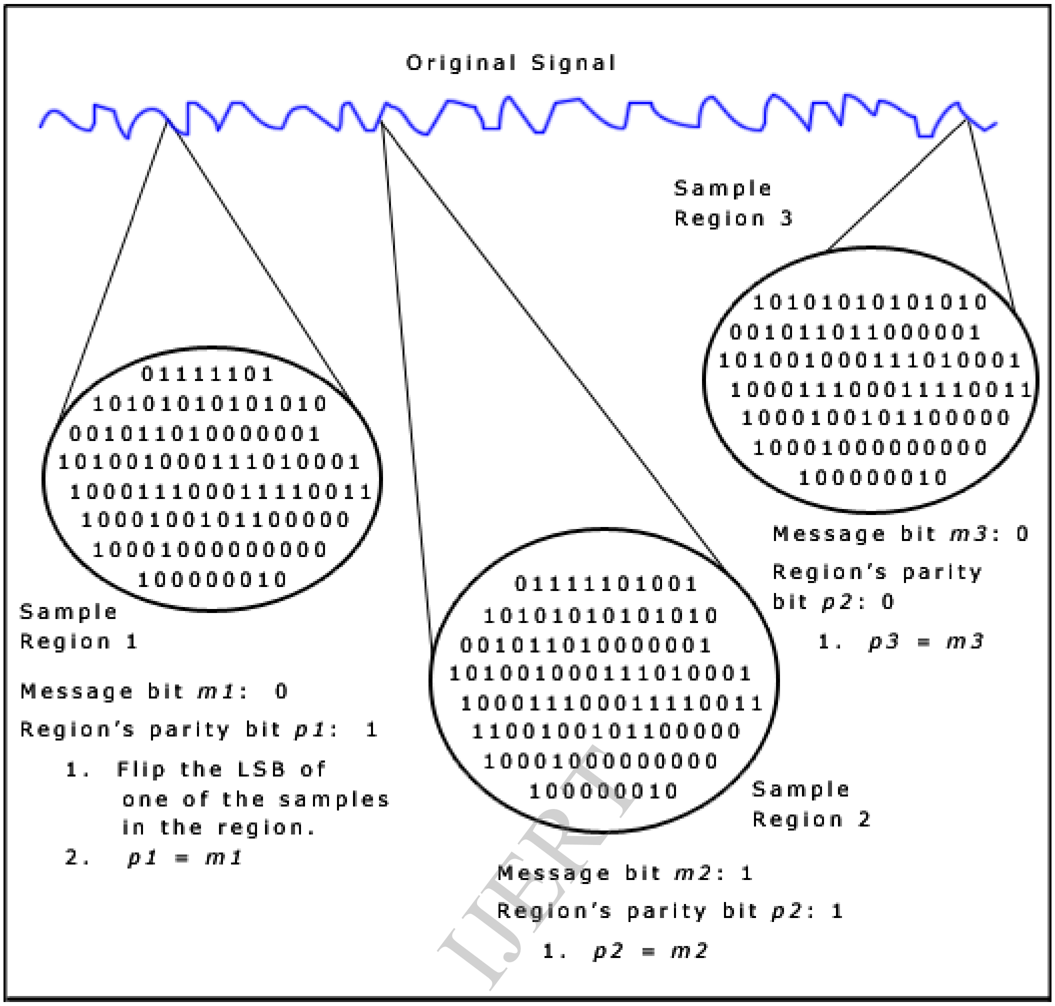


Fig.2..Parity Coding

3. PHASE CODING:-This method works by substituting the phase of an initial audio segment with a reference phase that represents the data. The phase of subsequent segments is adjusted in order to preserve the relative phase between segments[6].

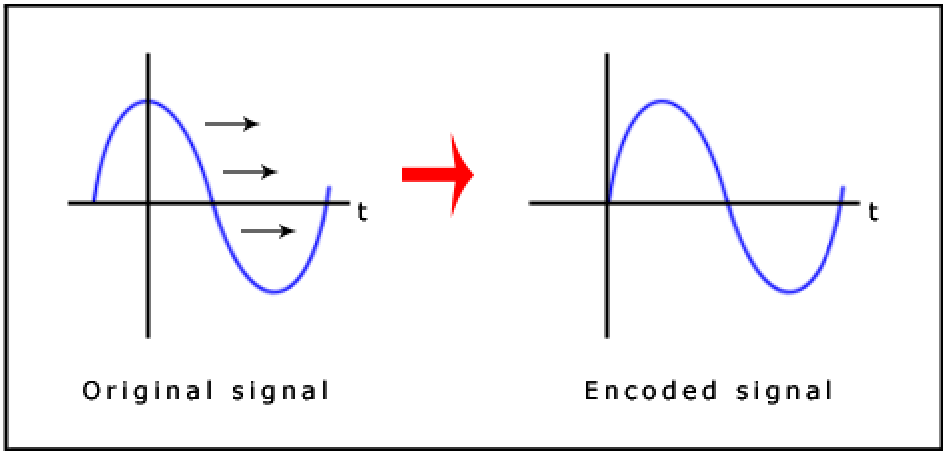
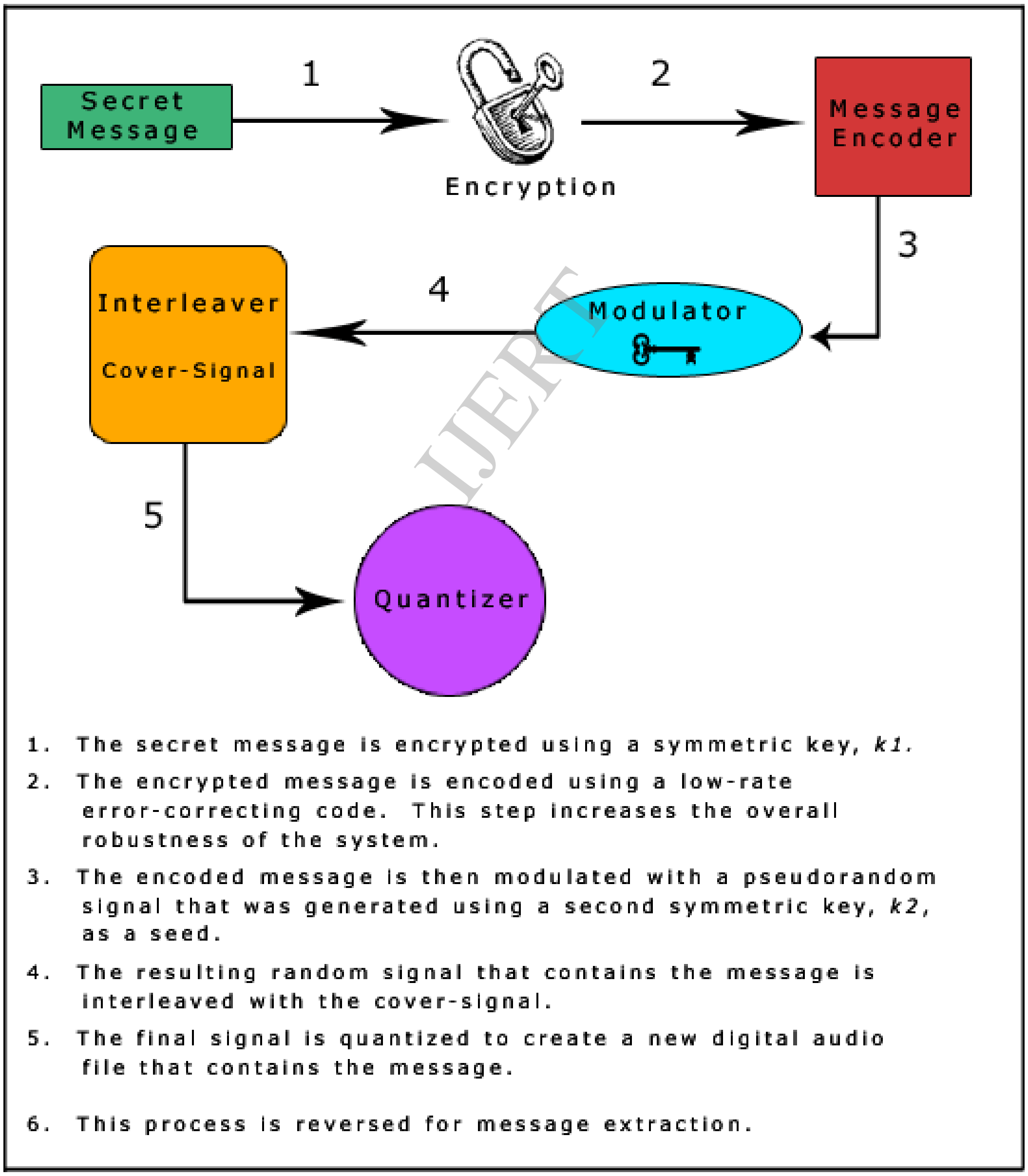


fig.3.Phase Coding

4. **SPREAD SPECTRUM:-**This method spreads out the encoded data across the available frequencies as much as possible. However, unlike LSB coding the SS method spreads the secret message over the sound file’s frequency spectrum using a code that is independent of actual signal. The final signal occupies a bandwidth in excess to that is actually required for transmission.



1. The secret message is encrypted using a symmetric key, *k1*.
2. The encrypted message is encoded using a low-rate error-correcting code. This step increases the overall robustness of the system.
3. The encoded message is then modulated with a pseudorandom signal that was generated using a second symmetric key, *k2*, as a seed.
4. The resulting random signal that contains the message is interleaved with the cover-signal.
5. The final signal is quantized to create a new digital audio file that contains the message.

6. This process is reversed for message extraction.

Fig.4.Spread Spectrum

5. ECHO DATA HIDING:- This method embeds data in a sound file by introducing an echo into the discrete signal. The data is then hidden by varying three parameters of the echo: initial amplitude, decay rate and offset. One bit of data is encoded if only echo from signal is produced. So, the original signal is broken down into blocks before the encoding process begins and concatenated back when encoding is completed[7].

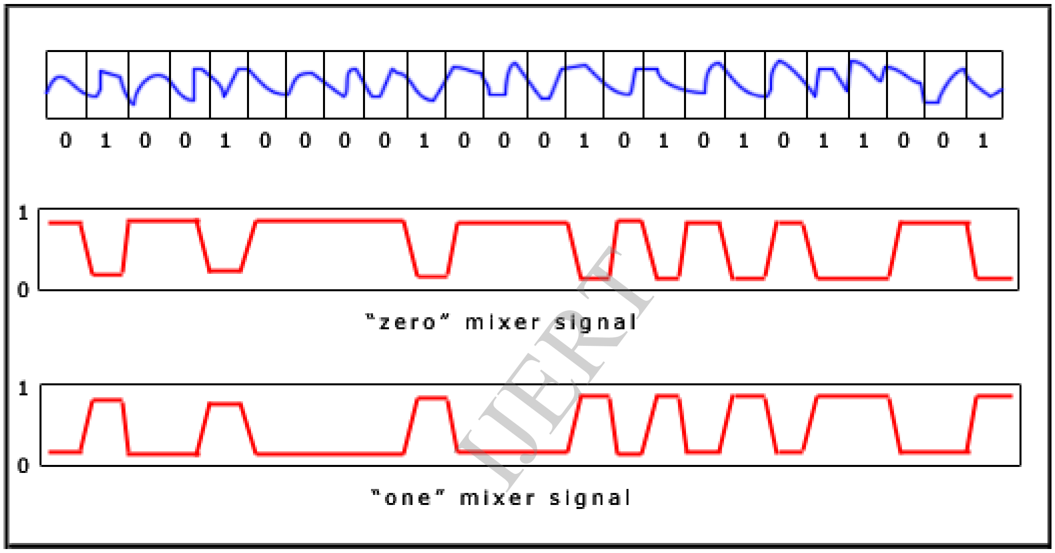


Fig.5.Echo Hiding

PROPOSED METHOD OF AUDIO STEGANOGRAPHY

The aim of this paper is to implement an algorithm for an information hiding technique using LSB coding in digital wave files. The proposed method for data hiding consists of two algorithms

1) Hiding algorithm for hiding text in wave cover file

2) Recovery algorithm for retrieving text from stego wave file.

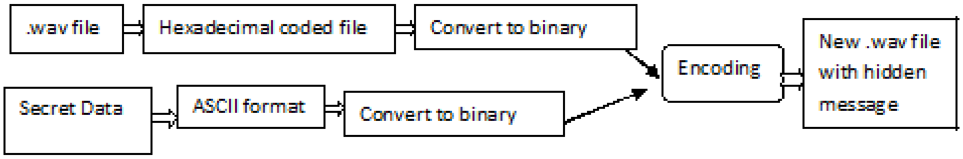


fig.6.Data Hiding In Audio File

Hiding Algorithm:-

1) A wave file is opened.

2) Convert the text message and the length of text message to binary.

3) Hide three contents in data samples—Identifier, length of text message and text message itself.

4) Identifier helps in the recovery of text. If identifier is not in the file the code stop execution assuming that the wav file has no hidden text message.

5) LSB of first 8 data samples has the identifier.

6) LSB of next 10 data samples has length of text message.

7) Then all the LSB of data samples have bits of binary text message.

Recovery Algorithm:-

1) Open the wave file containing the hidden message.

2) Check for the identifier in the LSB of first 8 data samples. If it is not present then the file has no hidden message.

3) Take out the LSBs of next 10 data samples which is the length of the text message.

4) Now take out the LSBs of rest of the data samples up to the length of text message.

5) Convert this to text and reshape them.

AUDIO STEGANOGRAPHY APPLICATIONS

Audio steganography can be used for a number of purposes. It prevents unauthorized persons from becoming aware of the existence of a message[10]. It is of interest for the protection of copyrighted digital media, for information systems security and for covert communication. It can also be used in forensic applications for inserting secret data into audio files for the authentication of spoken words and other sounds. In business world, it can be used to hide a secret formula or plan for a new invention[11].

CONCLUSION

In this paper, a robust method of imperceptible audio data hiding is introduced. This method provides- an efficient way for hiding the secret information from hackers and send to the destination in a safe and undetectable manner. It ensures that the size of the carrier file is not changed even after encoding. The LSB technique can be used when the cover file is uncompressed file but it can be used when the cover file is lossless compressed file. The robustness of this system can be further improved by introducing encryption along with the mentioned data hiding technique.

REFERENCES

[1] Poluami D., Debnath B., and Tai-hoon K., "Data Hiding in audio signal : A review", International Journal of Database Theory and Application, vol.2, No.2, June, 2009

[2]Stallings, W. " Cryptography and Network Security: Principles and Practice," 3rd edition, Prentice-Hall, 2003

[3] Gary C. Kessler, "Steganography: Hiding Data Within Data", *http://www.garykessler.net/library/steganography.html*,
September 2001.

[4] Dr.H.B.Kekre and A.A.Archana, "Information hiding using LSB technique with increased capacity", *International Journal of Cryptography and Security*, vol. 1, No.2, October 2008.

[5] Johnson, N. F., "Steganography", http://www.jjtc.com/stegdoc/, George Mason University, 2003.

[6] 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.

[7] 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.

[8] Nedeljko Cvejic, Tapio Seppben “Increasing the capacity of LSB-based audio steganography ” FIN- 90014 University of Oulu, Finland ,2002.

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

[10] Neil F.Johnson, Z.Duric and S.Jajodia. “Information Hiding Steganography and Watermarking-Attacks and Countermeasures”,Kluwer Academic Publishers, 2001

[11] F.A.P.Petitcolas, R.J.Anderson, M.G.Kuhn:”Information Hiding- A Survey”, Process of IEEE, vol.87, of IEICE, ISEC, vol.106 pp.15-22, September 2006. no.7, pp.1062-1078, July, 1999.

[12] Min Wu, Bede Liu. “Multimedia Data Hiding”, Springer- Verlag New York, 2003.