IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 9, Issue 1 (Jan. - Feb. 2013), PP 30-34
www.iosrjournals.org

Review of an Improved Audio Steganographic Technique over LSB through Random Based Approach

Bhagyashri A. Patil[1], Vrishali A. Chakkarwar[2]
[1]*(Student of ME CSE, Government Engineering College Aurangabad MS, India)*
[2]*(Assistant Professor, CSE Department, Government Engineering College Aurangabad MS, India)*

Abstract: *In this digital world, huge amount information exchange takes place due to enhanced facilities of networking. Therefore it is necessary to secure the information which we transmit. The need for secured communication introduces the concept of "Steganography". Steganography, the word itself indicates that information within information; it is the best technique to hide the secret information by using cover objects. Secret information may be a text, image or an audio file. But as per secret information format there are different steganographic techniques are available. This paper proposes a method of audio steganographic system that provides a unique platform to hide the secret information in audio file though the information is in text, image or in an audio format. So there is no need to go for different techniques of steganography as per information format. Many steganographic methods follow the LSB insertion technique to hide the secret information. But there are many statistical techniques available to determine if a stego object has been subjected to LSB Embedding. The proposed system hides secret information in audio file through random based approach and provides security by using PKE algorithm. This paper focuses on combining the strengths of cryptography and steganography for secured communication.*

Keywords – *Audio Steganography, PKE algorithm, Random based approach etc.*

I. INTRODUCTION

Due to digitization, information and other works become easily available in digital form. So it is possible that when information exchange takes place during communication, an intruder may interpret with secret message to make copy of our secret information or to destroy our information.

The first possibility may result in to large-scale unauthorized copying which might undermine the music, film, book, and software publishing industries. And the second possibility may result to destroy of information which again results in to miscommunication. These two problems had given an importance to "Information Security".

Steganography plays a very important role in information security as various methods to hide the information in cover object are available. Steganography means "concealed writing" which is originated from Greek words "stegano" i.e. covered and "graphie" means writing. Information security using steganography is the way of writing hidden messages in such a way that other than sender and intended recipient, nobody knows the existence of the message in cover object. Here the secret message and cover object may be in any format like text or image or audio file. For each format of information, steganography provides different way to hide the secret message. Various modern techniques of steganography are

a) Text Steganography b) Image Steganography c) Audio Steganography

Only the drawback is that as per information format, steganography method is selected. Why to go for method selection? This paper overcomes the problem of steganographic method selection.

The proposed system of audio steganography combines the features of both cryptography and steganography. It allows the user to select any format of information among text, image and audio which is to be transmitted. Cryptography is used to encrypt the secret message. For encrypting secret message PKE (Public Key Encryption) algorithm is used. This encrypted message is then hidden in cover object i.e. in an audio file. Finally this stego audio file is transmitted to intended recipient to avoid the possible vulnerable attacks of intruder.

In digital audio steganography system, secret message is embedded in audio file. The binary sequence of an audio file (cover object) is slightly changed by adding secret message in it. The audio file formats used by currently existing audio steganography software are WAV, AU, and even MP3 sound files. Audio steganography is a way of embedding information inside an audio signal. As data is embedded in the signal, the signal is get modified. This modification should not be made identified to the human ear.

Embedding secret messages in audio file is more difficult than embedding messages in digital image. In order to hide secret messages, various methods for embedding information in digital audio have been introduced. These methods range from simple algorithms which insert information in the form of noise in audio signal to more powerful methods that uses signal processing techniques to hide information. Maximum steganographic method uses Least Significant Bit (LSB) insertion method to hide the secret message in cover object [1-3]. But there are various techniques available to detect secret message which is present at LSB position. Therefore in proposed system, the secret message is hidden in cover object through random based approach. This process can be represented in simple equation as:

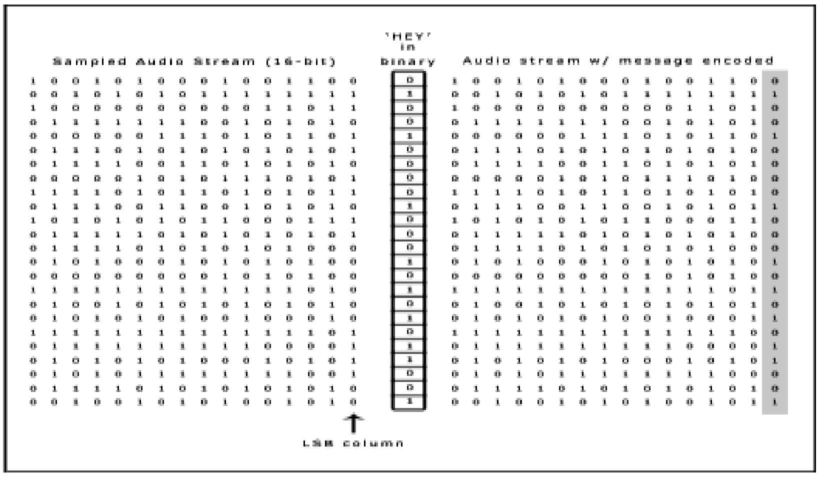
Cover Signal + Secret Information (text/image/audio format) = Stego Audio Signal

II. AUDIO STEGANOGRAPHIC TECHNIQUES

1.1 Temporal domain:

1.1.1 LSB:

LSB [4-5] is one of the earliest and simplest methods for hiding information in audio signals. It is the commonly used technique for audio steganography. In LSB encoding, the least significant bits of the cover media/original audio is altered to include the secret message. Even though this is a simple method, an attacker can easily extract the secret message from the stego object.



```
                                                   'HEY'
                                                     in
  Sampled Audio Stream (16-bit)                    binary     Audio stream w/ message encoded
1 0 0 1 0 1 0 0 0 1 0 0 1 1 0 0                      0       1 0 0 1 0 1 0 0 0 1 0 0 1 1 0 0
0 0 1 0 1 0 1 0 1 1 1 1 1 1 1 1                      1       0 0 1 0 1 0 1 0 1 1 1 1 1 1 1 1
1 0 0 0 0 0 0 0 0 0 0 1 1 0 1 1                      0       1 0 0 0 0 0 0 0 0 0 0 1 1 0 1 0
0 1 1 1 1 1 1 1 0 0 1 0 1 0 1 0                      0       0 1 1 1 1 1 1 1 0 0 1 0 1 0 1 0
0 0 0 0 0 0 1 1 1 0 1 0 1 1 0 1                      1       0 0 0 0 0 0 1 1 1 0 1 0 1 1 0 1
0 1 1 1 0 1 0 1 0 1 0 1 0 1 0 1                      0       0 1 1 1 0 1 0 1 0 1 0 1 0 1 0 0
0 1 1 1 1 0 0 1 1 0 1 0 1 0 1 0                      0       0 1 1 1 1 0 0 1 1 0 1 0 1 0 1 0
0 0 0 0 0 1 0 1 0 1 1 1 0 1 0 1                      0       0 0 0 0 0 1 0 1 0 1 1 1 0 1 0 0
1 1 1 1 0 1 0 1 1 0 1 0 1 0 1 1                      0       1 1 1 1 0 1 0 1 1 0 1 0 1 0 1 0
0 1 1 1 0 0 1 1 0 0 1 0 1 0 1 0                      1       0 1 1 1 0 0 1 1 0 0 1 0 1 0 1 1
1 0 1 0 1 0 1 0 1 1 0 0 0 1 1 1                      0       1 0 1 0 1 0 1 0 1 1 0 0 0 1 1 0
0 1 1 1 1 1 0 1 0 1 0 1 0 1 0 1                      0       0 1 1 1 1 1 0 1 0 1 0 1 0 1 0 0
0 1 1 1 1 0 1 0 1 0 1 0 1 0 0 0                      0       0 1 1 1 1 0 1 0 1 0 1 0 1 0 0 0
0 1 0 1 0 0 0 1 0 1 0 1 0 1 0 0                      1       0 1 0 1 0 0 0 1 0 1 0 1 0 1 0 1
0 0 0 0 0 0 0 0 0 1 0 1 0 1 0 0                      0       0 0 0 0 0 0 0 0 0 1 0 1 0 1 0 0
1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 0                      1       1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 1
0 1 0 0 1 0 1 0 1 0 1 0 1 0 1 0                      0       0 1 0 0 1 0 1 0 1 0 1 0 1 0 1 0
0 1 0 1 0 1 0 1 0 0 1 0 0 0 1 0                      1       0 1 0 1 0 1 0 1 0 0 1 0 0 0 1 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1                      0       1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0
0 1 1 1 1 1 1 1 1 1 1 0 0 0 0 1                      1       0 1 1 1 1 1 1 1 1 1 1 0 0 0 0 1
0 1 0 1 0 1 0 1 0 0 0 1 0 1 0 1                      1       0 1 0 1 0 1 0 1 0 0 0 1 0 1 0 1
0 1 0 1 0 1 1 1 1 1 1 1 1 0 0 1                      0       0 1 0 1 0 1 1 1 1 1 1 1 1 0 0 0
0 1 1 1 1 0 1 0 1 0 1 0 1 0 1 0                      0       0 1 1 1 1 0 1 0 1 0 1 0 1 0 1 0
0 0 1 0 0 1 0 1 0 1 0 0 1 0 1 0                      1       0 0 1 0 0 1 0 1 0 1 0 0 1 0 1 1
                              ↑
                          LSB column
```

Figure (1) LSB Insertion

1.1.2 Parity coding:

Parity coding technique [6] operates on a group of samples instead of individual samples. Here individual samples are grouped and parity of each group is calculated. For inserting message bit one by one, check the parity bit of a group of samples. If the parity bit and message bit matches do nothing. Otherwise change the LSB's of any one of the individual samples in that group to make the parity bit equal to the message bit.

1.1.3 Echo hiding:

In echo hiding [7] method data is embedded in the echo part of the host audio signal. The echo is a resonance added to the host signal and hence the problem with the additive noise is avoided here. While using echo hiding three parameters are to be considered: they are initial amplitude, offset (delay), and decay rate, so that echo is not audible. The main disadvantage of this method is lenient detection and low detection ratio. Due to its low embedding rate and low security no researches are going on echo hiding technique.

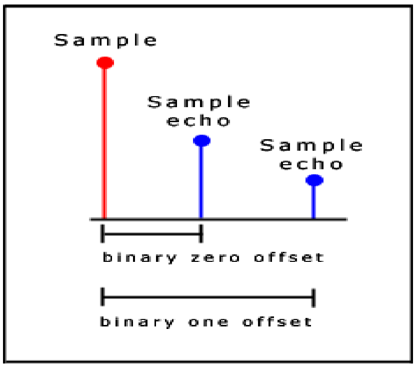


Figure (2) Echo Hiding

1.2 Frequency domain:

Frequency domain techniques and wavelet domain technique comes under transform domain. The main techniques under frequency domain are: tone insertion, phase coding and spread spectrum technique.

1.2.1 Tone insertion:

Frequency masking property is exploited in tone insertion method [9]. A weak pure tone is masked in the presence of a stronger tone. This property of inaudibility is used in different ways to embed information.

1.2.2 Phase coding:

Phase coding method [8] is based on the fact that the phase components are not audible to human as noise components. This method embeds the secret message bits as phase shift in the phase spectrum of the original audio signal. The method tolerates better signal distortion, better robustness but it does not survive low pass filtering. Here the secret message is inserted only at the phase vector of the first signal segment.

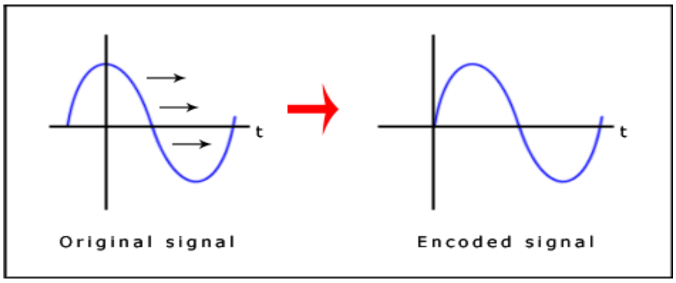


Figure (3) Phase Coding

1.2.3 Spread spectrum technique:

This technique takes the advantage of masking property of HAS. A masking threshold is calculated using a psycho-acoustic model. The spread signal now lies below the masking threshold. Apart from phase shifting, here the secret message is distributed along with the host signal. Here the final signal occupies a bandwidth which is more than what is actually required for transmission.

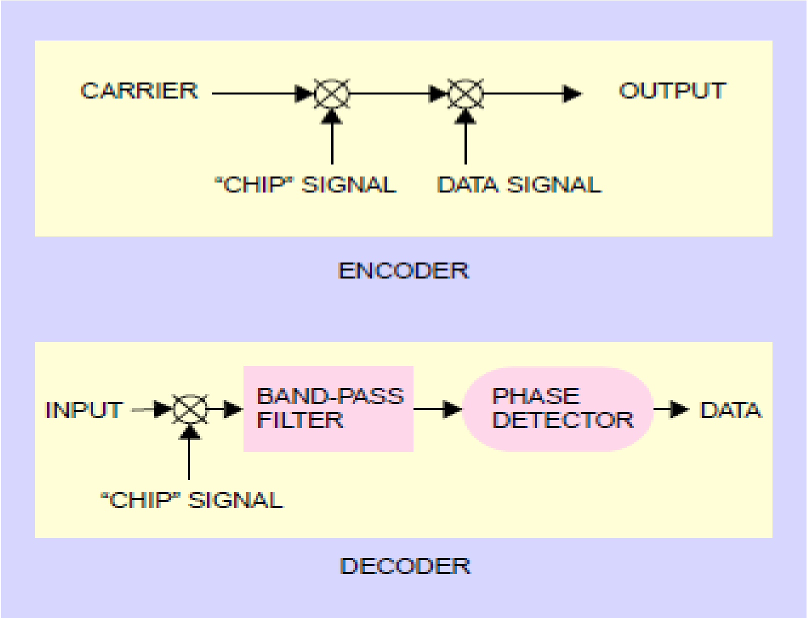


Figure (4) Spread Spectrum

1.3 Wavelet domain:

Wavelet domain [10] is suitable for frequency analysis because of its multi-resolution properties that provides access to both most significant parts and details of spectrum. Wavelet domain techniques works with wavelet coefficients. Upon applying the inverse transform, the stegano signal can be reconstructed.

Table 1. Summary of audio steganography techniques:

Method	Strength	Weakness
LSB	Simple	Easy to extract
Parity coding	More robust than LSB	Easy to extract
Echo hiding	Avoids problem with additive noise	Low capacity
Tone insertion	Exploits masking property	Low embedding capacity
Phase coding	Robust	Low capacity
Spread spectrum	Increases transparency	Occupies more bandwidth
Wavelet domain	High hiding capacity and transparency	Lossy data retrieval

III. DRAWBACKS OF EXISTING SYSTEMS

Now days, multiple techniques of steganography are present but are in scattered format. For example text to audio steganography, image to audio steganography, audio to audio steganography. The proposed system combines the above specified techniques of steganography in to one system along with each methods good quality features. Maximum audio steganographic algorithms basically work with LSB insertion method. But these techniques are having many drawbacks as specified below:

- These systems are less secure
- Algorithms used in LSB insertion method are easily decryptable
- Steganographic systems may suffer from vulnerability attacks
- LSB insertion method adds the noise to cover data
- Sometimes the audio file may get corrupted
- At a time only one technique can be used *i.e.* either text to audio or image to audio or audio to audio steganography.

IV. PROPOSED METHODOLOGY

To overcome the drawbacks of existing system, an efficient encryption algorithm should be used. So the proposed system uses public key encryption algorithm through random based approach. It also provides a good platform of to perform all steganographic techniques under one system as shown in Fig. This system consists of text to audio, image to audio as well as audio to audio steganography.

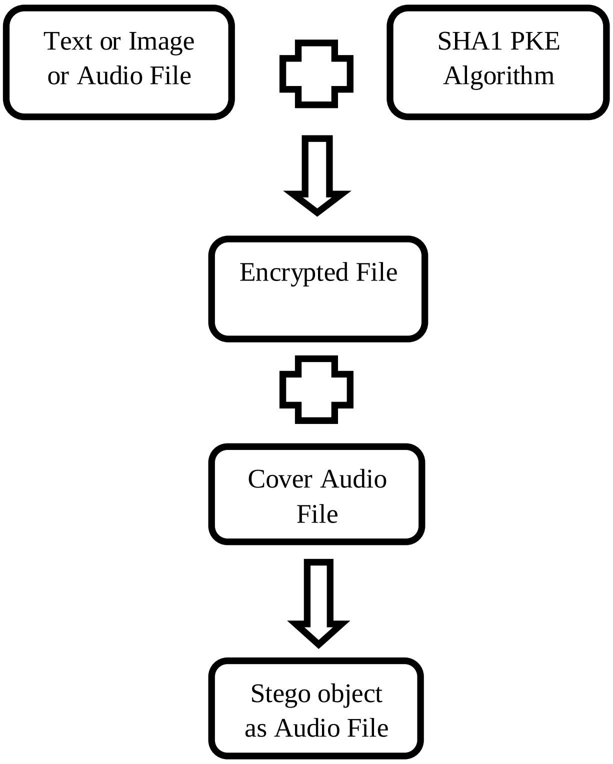


Figure 3.1 Block Diagram of Proposed System

4.1 Working:

Input given to the system is secret message which is either a text file or image file or an audio file. After this a cover object i.e. audio file (.WAV format) is selected to perform encryption as well as to hide the encrypted data. Secret message file is converted to binary file format. Among this binary format, a salt of 1024 byte is selected for encryption. Simultaneously a salt is also taken from audio file, where salt is nothing but a small part of file which is to be read. Audio file salt selection is based upon random based approach means random salt from cover audio file is selected.

After receiving secret message's binary file salt and cover audio file salt; public key encryption algorithm i.e. SHA-1 is applied to get the encrypted file. Finally this encrypted data is hidden in cover audio (.WAV) file by using random based approach. Hiding the encrypted data is the last step of steganography at sender side. Among many different data hiding techniques proposed to embed secret message within audio file, the random rit data hiding technique is one of the secured methods for inserting data into audio signals in noise free environments, which merely embeds secret message-bits in a subset of the random bit planes of the audio stream. The following steps are used to hide the encrypted data in audio signal:

a. Receives the audio file in the form of bytes and converted in to bit pattern.

b. Each character in the message is converted in bit pattern.

c. Replaces the random bits of audio with encrypted bit in the message.

This proposed system is to provide a good, efficient method for hiding the data from hackers and sent to the destination in a safe manner. This proposed 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 have been used to make the security system robust.

V. CONCLUSION

Information security is a big challenge for computer users. This proposed method is one of the tool which allows the user to embed text or image or an audio data in cover media which is nothing but an audio signal under a single platform. There is no need to go for different methods of steganography. The stego object produced by described method is highly secured and prevent from vulnerability attacks. Review of proposed scheme has been discussed in this paper for embedding text or image or an audio data in cover audio file using public key encryption algorithm i.e. SHA-1 through random based approach. Emphasis is on comparing proposed scheme with simple LSB based data hiding in audio.

This steganography technique is used for the transportation of high level or top secret documents between international governments also it allows for copyright protection on digital files using the message as a digital watermark.

ACKNOWLEDGEMENT

We sincerely thank everyone associated with this work.

REFERENCES

Journal Papers:

[1] Manoj .T.H, Vimalanathan P, A Santha Rubia, R Sri Vidya, Secured way of encrypted message transmission using audio file, *IJCTA Vol 3 July-August 2012*

[2] Dalal N. Hmood, Khamael A. Khudhiar, Mohammed S. Altaei, A new steganographic method for embedded image in audio file, *International Journal of Computer Science and Security (IJCSS), Volume (6) : Issue (2) : 2012)*

[3] Jeddy Nafeesa Begum1, Krishnan Kumar1, Vembu Sumathy, Design and implementation of multilevel access control in synchronized audio to audio steganography, *Journal of Information Security, 2010)*

[4] M. Asad, J. Gilani, and A. Khalid, An enhanced least significant bit modification technique for audio steganography, *International Conference on Computer Networks and Information Technology (ICCNIT), IEEE, 2011.*

[5] K. Bhowal, A. Pal, G. Tomar, and P. Sarkar, Audio steganography using GA, *International Conference on Computational Intelligence and Communication Networks (CICN), IEEE, 2010.*

[6] P. Jayaram, H. Ranganatha, and H. Anupama, Information hiding using audio steganography-a survey, *International Journal of Multimedia and its Applications, 2011.*

[7] F. Djebbar, B. Ayad, H. Hassmam, and K. Abed-Meraim, A view on latest audio steganography techniques, *International Conference on Innovations in Information Technology (IIT), IEEE, 2011.*

[8] M. Nutzinger and J. Wurzer, A novel phase coding technique for steganography in auditive media, *Sixth International Conference on Availability, Reliability and Security (ARES), IEEE, 2011.*

Proceedings Papers:

[9] K. Gopalan and S. Wenndt, Audio steganography for covert data transmission by imperceptible tone insertion, *Proceedings of Communications Systems and Applications, IEEE, 2004.*

[10] Cvejic and T. Seppanen, A wavelet domain lsb insertion algorithm for high capacity audio steganography, *Proceedings of 2002 IEEE 10th Digital Signal Processing Workshop, 2002 and the 2nd Signal Processing Education Workshop, IEEE, 2002.*