A High Capacity and Novel Steganography Technique for Hiding Data in an Audio Signal

Jyohtipriya Kothimira[1], D. Malleswari[2], DR.K. Veeraswamy[3]

[1]M.Tech, Depart of Electronics and Communication, QIS College, JNTU Kakinada, Ongole, India

[2]Associate Professor, Depart of Electronics and Communications, QIS College, JNTU Kakinada, Ongole, India

[3]Principal, Depart of Electronics and Communications, QIS College, JNTU Kakinada, Ongole, India

Abstract: This paper is that the study of audio steganography mistreatment formula like LSB approach. Here during this paper to enhance the protection to our secret message we've got designed a secrete key, so whoever understand the secrete key they solely will access the information. During this paper, we have a tendency of a unique high bit rate LSB technique that reduces embedding distortion of the host audio. As a steganographic approach the quality of the host audio signal wasn't to be degraded. By mistreatment this LSB formula we are able to come through the high sensory activity quality of the input audio signal. Our projected formula provides top quality of host audio and security than compared to previous ways.

Key words: audio signal, human sensory system, steganography, key.

I INTRODUCTION

The aim of steganography is to hide information into a cover, so that the presence of hiddendata cannot be diagnosed. Communication by embedding a message or data file in a cover media has been increasingly gaining importance in the all-encompassing field of information transfertechnology. Audio steganography is concerned with embedding information intoa cover audio in a secure and robust manner. Communication and transmission security and robustness are essential for transmitting vital information to intended sources while denying access to unauthorized persons. By hiding the information using a cover or host audio as a wrapper, the existence of the information is concealed during transmission. This is critical in applications such as battlefield communications and bank transactions, for example. Steganalysis aims to expose the presence of hidden data. Multimedia data hiding techniques have developed a strong basis for steganography area with a growing number of applications like digital rights management, covert communications, hiding executable for access control, annotation etc. In all application scenarios given above, multimedia steganography techniques have to satisfy two basic requirements. The first requirement is perceptual transparency, i.e. cover object (object not containing any additional data) and stego object (object containing secret message) must be perceptually indiscernible [1]. The second constraint is high data rate of the embedded data. All the stego-applications, besides requiring a high bit rate of the embedded data, have need of algorithms that detect and decode hidden bits without access to the original multimedia sequence (blind detection algorithm). While the robustness against intentional attack is not required.

LSB coding is one of the earliest techniques studied in the information hiding and watermarking area of digital audio [2, 3] [4, 5]. The main advantage of the LSB coding method is a high bit rate of hidden bits and a low computational complexity of the algorithm, while the main disadvantage is a low robustness against signal processing alterations.

Steganography, in general, relies on the imperfection of the human auditory and visual systems. Audio steganography takes advantage of the psycho acousticalmasking phenomenon of the human auditory system [HAS]. Psycho acousticalor auditory masking property renders a weak tone imperceptible in the presence of a strong tone in its temporal or spectral neighbourhood. This property arises because of the low differential range of the HAS even though the dynamic range covers 80 dB below ambient level [6, 7]. Frequency masking occurs when human ear cannot perceive frequencies at lower power level if these frequencies are present in the vicinity of tone- or noise-like frequencies at higher level. Additionally, a weak pure tone is masked by wide-band noise if the tone occurs within a critical band. This property of inaudibility of weaker sounds is used in different ways for embedding information. Embedding of data by inserting inaudible tones in cover audio signal has been presented recently [8, 9].

Encoding secret messages in audio is that the most difficult technique to use once managing Steganography will be as a result of the human sensory system (HAS) has such a dynamic vary that it can listen over. to place this in perspective, the (HAS) perceives over a variety of power bigger than a meg to at least one and a variety of frequencies bigger than one thousand to at least one creating it very arduous to feature or take away information from the first arrangement. the sole weakness within the (HAS) comes at attempting to differentiate sounds (loud sounds resound quiet sounds) and this is often what should be exploited to cipher secret messages in audio while not being detected.

A steganography system, in general, is anticipated to satisfy 3 key needs, namely, physical property of embedding, correct recovery of embedded info, and enormous payload (payload is that the bits that get delivered to the top user at the destination). In a very pure steganography framework, the technique for embedding the message is unknown to anyone apart from the sender and therefore the receiver. A good steganographic theme ought to possess the subsequent desired characteristics [10-11]:

Secrecy: A person should not be able to extract the covert data from the host medium without the knowledge ofthe proper secret key used in the extracting procedure.

Imperceptibility: The medium after being embedded with the covert data should be indiscernible from theoriginal medium. One should not become suspicious of the existence of the covert data within the medium.

High capacity: The maximum length of the covert message that can be embedded should be as long aspossible.

Resistance: The covert data should be able to survive when the host medium has been manipulated, for exampleby some lossy compression scheme.
Accurate extraction: The extraction of the covert data from the medium should be accurate and reliable.

Basically, the purpose of steganography is to provide secret communicate like cryptography. There are two concepts to consider before choosing an encoding technique for audio. They are the digital format of the audio and the transmission medium of the audio. There are three main digital audio formats typically in use. They are Sample Quantization, temporal Sampling Rate and Perceptual Sampling.

Sample Quantization which is a 16-bit linear sampling architecture used by popular audio formats such as (.WAV and. AIFF).

Least Significant bit

Least significant bit (LSB) coding is the simplest way to embed information in a digital audio file. By substituting the least significant bit of each sampling point with a binary message, LSB coding allows for large amount of data to be encoded. Among manydifferent data hiding techniques proposed to embed secret message within audio file, the LSB data hiding technique is one of the simplest methods for inserting data into digital signals in noise free environments, which merely embeds secret message-bits in a subset of the LSB planes of the audio stream.

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.

Embedding the data by using LSB Coding

Sampling technique followed by Quantization converts analog audio signal to digital binary sequence.

In this technique LSB of binary sequence of each sample of digitized audio file is replaced with binary equivalent of secret message. For example if we want to hide the letter 'A' (binary equivalent 01100101) to an digitized audio file where each sample is represented with 8 bits, and we consider the 2 samples at a time. Then LSB of 8 consecutive samples (each of 8 bit size) is replaced with each bit of binary equivalent of the letter 'A'.These 8 consecutive samples are divided into two parts, so the first 4 bits are replaced in first sample and the next 4 bits are replaced in the second sample. Finally the letter 'A' is successfully embedded into the 2 samples of audio file at a time. So this method is called as 4-bit replacement method.

Embedding process:

Consider the two samples of an audio file is 128 and 129.
The corresponding binary values are
10000000 and
10000001
Consider the secrete letter embedded into the two samples was 'A'
The ASCII value of A is 65, and the binary equivalent is 01000001.
The value of A is divided into
0100 and
0001
The LSB of the 128 and 129 values are
0000 and
0001
So the embedding is
0000 + 0100
0001 + 0001
The resultant values are
0100 and
0001
Finally these values are replaced in original binary values of 128 and 129 samples.
So the values before embedding the data are
10000000 and
10000001
And the values after embedding the data are
10000100 and

10000001
Which are the decimal equivalent of 132 and 129.

So by using this method we can hide the high amount of data without much degrading the audio quality.

Key generation:

Before embedding the secret data into the cover audio we have given a 4-bit key for maintaining more security to our system. So that whenever the second party wants to extract the secret data from the cover audio he must enter the same 4-bit key. Then only he can access the data.

Finally the audio which is having secret data called as stego audio was transferred to the particular receiver.

Extraction process

In the extraction process the receiver must enter the same 4-bit key to process and extract the data from the audio file. Once the key which was entered by the user is correct, all the audio samples were processed for extracting the data which is the revere process of LSB algorithm.

If the samples which consisting of secrete data are detected as 132 and 129 then the least significant bits of the particular 2 samples are decoded and the last 4 bits are extracted from the samples, they are as follows:

Binary equivalents of 132 and 129 are
10000100 and
10000001
And least significant bits of the corresponding samples are
0100 and
0001
Finally combine both the values
01000001
This is the decimal equivalent of 65
Convert this decimal value into the ASCII format which results the letter 'A'.

Like this manner we can hide any information in the cover audio and can extract the same secret information without any loss in it.

EXPERIMENTAL RESULTS:

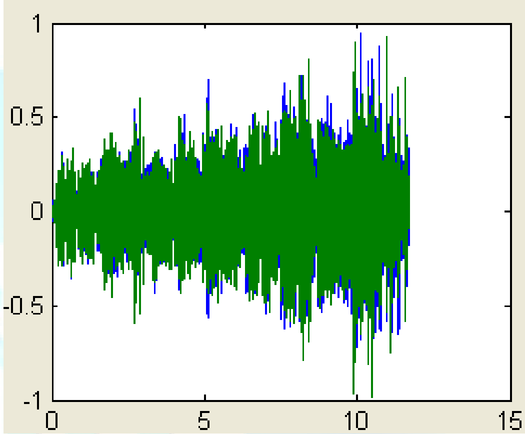

Fig 1: audio signal before embedding the data

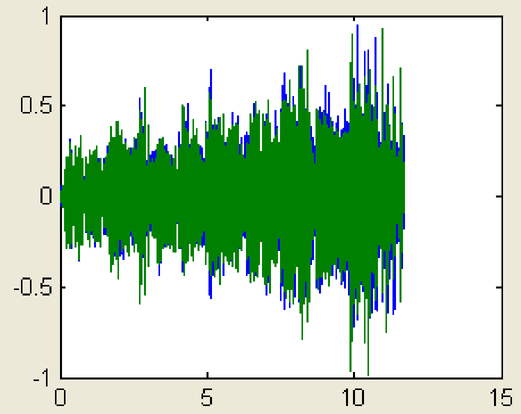

Fig 2: audio signal after embedding the data

CONCLUSION

In this paper we've got introduced a sturdy technique of unobservable audio knowledge concealing with high pay load because it uses the 4-bit replacement method of LSB. This method is to produce a decent, economical technique for concealing the information from hackers and sent to the destination in a very safe manner. This planned system won't amendment the scale of the file even when coding and additionally appropriate for any variety of audio file format. So we have a tendency to conclude that audio knowledge concealing techniques are often used for variety of functions apart from covert communication or deniable knowledge storage, data tracing and finger printing, tamper detection.

References

[1] R.J. Anderson and F. A. P. Petit colas (2001) On the limits of the steganography, IEEE Journal Selected Areas in Communications, 16(4), pp. 474-481.

[2] C. Yeh and C. Kuo (1999), Digital Watermarking through Quasi m-Arrays, Proc. IEEE Workshop on Signal Processing Systems, Taipei, Taiwan, pp. 456-461.

[3] T. Cedric, R. Adi and I. McLaughlin (2000), Data concealment in audio using a nonlinear frequency distribution of PRBS coded data and frequency-domain LSB insertion, Proc. IEEE International Conference on Electrical and Electronic Technology, Kuala Lumpur, Malaysia, pp. 275-278.

[4] Y. Lee and L. Chen (2000) High capacity image steganographic model, IEE Proceedings on Vision, Image and Signal Processing, 147(3), pp. 288-294.

[5] J. Fridrich, M. Goljan and R. Du (2002) Lossless Data Embedding - New Paradigm in Digital Watermarking, Applied Signal Processing, 2002(2), pp. 185-196.

[6] W. Bender, D. Gruhl, N. Morimoto and A.Lu, "Techniques for data hiding," IBM Systems Journal, Vol. 35, Nos. 3 & 4, pp. 313-336, 1996.

[7] M.D. Swanson, M. Kobayashi, and A.H. Tewfik, "Multimedia data-embedding and watermarking technologies," Proc. IEEE, Vol. 86, pp. 1064-1087, June 1998.

[8] K. Gopalan, S. Wenndt, A. Noga, D. Haddad, and S. Adams, "Covert Speech Communication via Cover Speech By Tone Insertion," Proc. of the 2003 IEEE Aerospace Conference, Big Sky, MT, Mar. 2003 (on CD).

[9] K. Gopalan, et al, "Covert Speech Communication via Cover Speech by Tone Insertion," U.S. Patent applied for, Oct. 2003.

[10] C. C. Chang, T. S. Chen and H. S. Hsia, "An Effective ImageSteganographic Scheme Based on Wavelet Transform and Pattern-BasedModification", IEEE Proceedings of the 2003 International Conferenceon Computer Networks and Mobile Computing, 2003.

[11] Chen and G.W. Womell, "Quantization index modulation: a class ofprovably good methods for digital watermarking and informationembedding", IEEE Transactions on Information Theory, Vol. 47, No. 4,pp. 1423-1443, May 2001.

[12] B. Chen, "Design and analysis of digital watermarking, informationembedding, and data hiding systems," Ph.D. dissertation, MIT, Cambridge, MA, June 2000.