A Novel Technique for Data Hiding in Audio by Using DWTS

Preeti Jain[1], Vijay Kumar Trivedi [2]

[1] LNCT, Bhopal, M.P., India.
preetijainsinghai@gmail.com
[2] Asst. Prof., Deptt. of Computer Science and Engineering, LNCT, Bhopal, M.P., India.
vkt911@gmail.com

Abstract

A secure data transfer is limited due to its attack made on data communication internet community. 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. Hidden message is information that is not immediately noticeable, and that must be discovered or uncovered and interpreted before it can be known. In this paper, we propose a novel approach for high capacity audio steganography algorithm based on the wavelet packet transform with adaptive hiding in least significant bits. The adaptive hiding is determined depend on the cover samples strength and bits block matching between message and cover signals. We propose two main stages, Input stage and secret message hiding stage. After the stages of input audio segmenting hide secret message by using preprocessing and developed in matlab.

Keywords- *component Steganalysis, Data Hiding data, audio hiding wavelet packet transform, least significant bit. adaptive hiding.*

INTRODUCTION

The Internet has revolutionized the modern world and the numerous Internet based applications that get introduced these days add to the high levels of comfort and connectivity in every aspects of human life. Audio is an important communication way for people, and therefore is a convenient medium secure communications. Audio steganography is a useful means for transmitting convert battlefield information via and innocuous cover audio signal. This paper focuses on WAV files. In order to discriminate stegno audios from clear normal ones, that embed random data into a (possibly) stego WAV file by using a certain steganography tool. It was found that the variation in some statistical features of WAV file is significantly different between clear WAV files and stego ones which already contain hidden messages embedded by the same tool. In this paper, that can detect the existence of hidden messages, and also identify the tools used to hide them.

The rapid proliferation of Voice over Internet Protocol (VoIP) and other Peer-to-Peer (P2P) audio services provide vast opportunities for covert communications. By slightly altering the binary sequence of the audio samples with existing steganography tools, covert communication channels may be relatively easy to establish. Moreover, the inherent redundancy in the audio signal and its transient and unpredictable characteristics imply a high hidden capacity [1]. This is further aided by the fact that the human ear is insensitive to small distortions in the audio signal.

To achieve secure and undetectable communication, *stego-objects*, documents containing a secret message, should be indistinguishable from *cover-objects*, documents not containing any secret message. In this respect, S*teganalysis* is the set of techniques that aim to distinguish between cover-objects and stego-objects.

Digital representation of signals brings many advantages when compared to analog representations, such as lossless recording and copying, convenient distribution over networks, easy editing and modification, and durable, cheaper, easily reachable archival. Unfortunately, these advantages also present serious problems including wide spread copyright violation, illegal copying and distribution, problematic authentication, and easy forging.

Information hiding in digital documents provides a means for overcoming those problems. Depending on what information in which form is hidden in the audio, one can distinguish at least two types of data hiding schemes: non-robust, undetectable data hiding, and robust audio watermarking. In the first case, a digital audio serves as a container for a secret message. In the second application, robust audio watermarking, a short message (a watermark) is embedded in the audio in a robust manner. By robustness we mean the ability to survive common audio processing operations, such as lossy compression, filtering, noise adding, geometrical transformations, etc. Such robust watermark can be obviously used for copyright protection, fraud detection (verification of audio integrity), authentication, etc. At this point we emphasize that cryptographic authentication protocols cannot solve all the issues related to authentication.

Cryptographic authentication deals with authenticating the sender of the message over insecure channels. However, once the message (audio) is decrypted, the audio is unprotected and can be copied and further distributed. Unlike classical paintings that can be studied for authenticity using sophisticated experimental techniques, a digital artwork is just a collection of bits. A visible signature in the corner of the audio can be easily replaced or removed with advanced audio processing software packages, such as Photo-Shop. Additional information in the audio file header can be erased or changed as well. In other words, any attempt to authenticate the digital audio file by appending information will fail. Digital watermarking provides an appealing alternative by embedding rather than appending information directly into the audio data itself. The embedded information will be transparent to the human ear, but it should be detectable using a sophisticated algorithm provided a secret key is available [2] and [3] and [4].

LITERATURE SURVEY

In this research paper, 2011, Haider Ismael Shahadi et. al.[5], they propose a new high capacity audio steganography algorithm based on the wavelet packet transform with adaptive hiding in least significant bits. The results show that message can be embedded up to 42 % of the total size of the cover audio signal with at least of 50 dB signal to noise ratio.

The following four main stages are repeated to hide each secret message segment in one cover segment:

a. *Cover Signal Decomposition and Preparing Stage*

Each segment of the input audio cover signal is decomposed using L-levels of Haar DWPT to obtain 2^L signals one represents the approximation coefficients signal and the others represent details coefficients signals. Each one of the produced signal has length of $Z/2^L$samples. They select 2^L-2 from the details signal starting from the highest frequency component for embedding of the secret message.

b. *Key Generating and Secret Message Embedding Stage*

The preprocessed message segment (*MP*) that has size of M_xN and the matrix of embedding positions contents that has size W_xM are fed to the bits block matching process. In the bits block matching process, the bits blocks of *MP* and *EPC* matrix are compared to compute matching between each bits block (row) of *MP* and whole blocks (rows) of *EPC* to obtain the blocks matching matrix *BM* which has size of M_xW.

c. *Stego-Key Embedding Stage*

Because of the arbitrary distribution of the message blocks in embedding process in the previous section, the recovery algorithm of the proposed scheme will need stego key and message size to extract the message blocks from the stego-signal. Therefore, the stego-key with the message size will embed in the lowest frequency details signal ($D_2{}^{L}$ *-1*). They choose this signal to embed the stego-key because it has maximum power between all other details signals and that make the stego-key more resistance against distortion or lost.

PROPOSED TECHNIQUE

When hiding information inside Audio files the technique usually used is low bit encoding which is somewhat similar to LSB that is generally used in Images. The problem with low bit encoding is that it is usually noticeable to the human ear, so it is a rather risky method for someone to use if they are trying to mask information inside of an audio file. Spread Spectrum is another method used to conceal information inside of an audio file. This method works by adding random noises to the signal the information is conceal inside a carrier and spread across the frequency spectrum. Echo data hiding is yet another method of hiding information inside an audio file. This method uses the echoes in sound files in order to try and hide information. By simply adding extra sound to an echo inside an audio file, information can be concealed. The thing that makes this method of concealing information inside of audio files better than other methods is that it can actually improve the sound of the audio inside an audio file.

There are four major audio steganography algorithms: Low-bit encoding, Phase encoding, Spread spectrum coding and Echo data hiding.

Low-bit Encoding

Low-bit encoding [6], the binary version of the secret data message is substituted with the least significant bit (LSB) of each sample of the audio cover file. Though this method is simple and can be used to embed larger messages, the method cannot protect the hidden message from small modifications that can arise as a result of format conversion or lossy compression.

Spread Spectrum Coding

The basic Spread Spectrum (SS) coding method [7] randomly spreads the bits of the secret data message across the frequency spectrum of the audio signal. However, unlike LSB coding, the SS coding method spreads the secret message using a code that is independent of the actual cover signal. The SS coding method can perform better than LSB coding and phase coding techniques by virtue of a moderate data transmission rate coupled with a high level of robustness against Steganalysis techniques. However, like the LSB coding method, the SS method can introduce noise to the audio file. This vulnerability can be tapped for Steganalysis.

Phase Coding

Phase coding [8] is based on the fact that the phase components of sound are not as perceptible to the human ear as noise is. Message bits are encoded as phase shifts in the phase spectrum of a digital signal. This leads to inaudible encoding in terms of the Signal-to-Perceived Noise Ratio (SPNR) and the secret message gets camouflaged in the audio signal, not detectable by the Steganalysis methods based on SPNR.

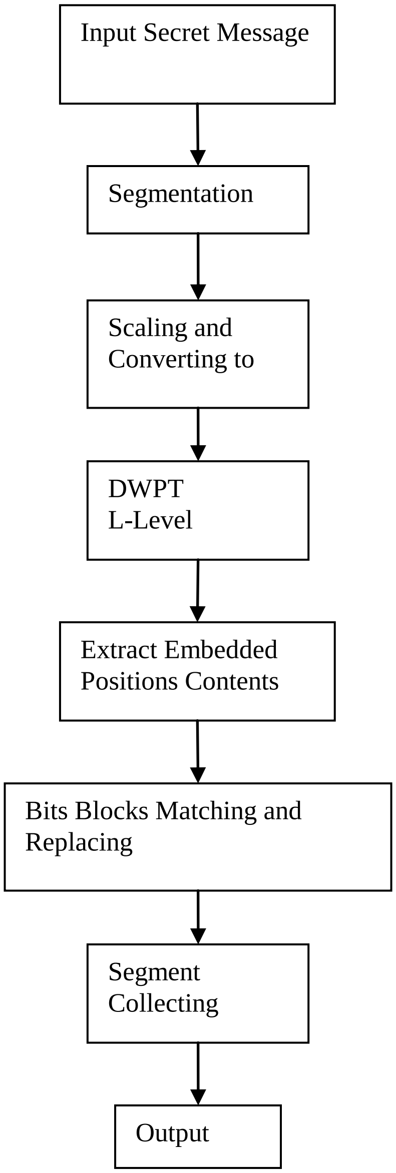
Input Secret Message
Segmentation
Scaling and Converting to
DWPT L-Level
Extract Embedded Positions Contents
Bits Blocks Matching and Replacing
Segment Collecting
Output

Fig. 1. Proposed Embedding algorithm

Steps involved in phase coding:

- ✓ The original audio signal is decomposed into smaller segments such that their length equals the size of the message that needs to be encoded.
- ✓ A Discrete Fourier Transform (DCT) is then applied to each segment in order to create a phase matrix.
- ✓ Phase differences between every pair of consecutive segments are computed.
- ✓ Phase shifts between adjacent segments are identified. Although, the absolute phases of the segments can be altered, the relative phase differences between consecutive segments must be unchanged.
- ✓ The new phase matrix is created using the new phase of the signal's first segment and the set of original phase differences.
- ✓ Based on the new phase matrix and the original magnitude matrix, the sound signal is regenerated by using inverse DFT and then by joining the sound segments together.

The receiver is mandated to know the message length in order to use DFT and extract the embedded message from the cover signal. A characteristic feature of phase coding is the low data transmission rate owing to the fact that the secret message is encoded only in the first segment of the audio signal. On the contrary, an increase in the length of the segment would have a ripple effect by altering the phase relations between the frequency components of the segment; thereby making detection easier.

Echo Hiding

With echo hiding [9], information is embedded by introducing an echo into the discrete audio signal. Like SS coding, echo hiding allows for a higher data transmission rate and provides superior robustness when compared to the noise-inducing methods. To successfully hide the data, three parameters of the echo need to be altered: amplitude, decay rate and offset (delay time) from the original signal. The echo is not easily resolved as all the three parameters reset below the human audible threshold limit. Also, the offset is altered to represent the binary message to be hidden. The first offset value represents a one (binary), and the second offset value represents a zero (binary).

CONCLUSION

In this research paper proposed algorithm hiding data in audio 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. The arbitrary results of the block matching generate an arbitrary key for embedding process, and that help in increasing the security of steganographic information in the proposed algorithm In the business world data hiding in audio can be used to hide a secret chemical formula or plans for a new invention. Audio data hiding can also be used in corporate world.

Hiding data can also be used in the noncommercial sector to hide information that someone wants to keep private. Terrorists can also use data hiding to keep their communications secret and to coordinate attacks.

Another advantage for the proposed algorithm is the reconstruction of the actual secret messages does not require the original cover audio signal and therefore, the cover signal can be any recorded audio by the hiding side. and implemented using a Matlab tools.

REFERENCES

[1]. Er. Niranjan Singh and Dr. Bhupendra Verma, “Quality and Distortion Evaluation of Audio Signal by Spectrum” *International Journal of Computer Science and Security (IJCSS)*, Volume (6) : Issue (1), PP 629-636, 2012.

[2]. Masoud Nosrati, Ronak Karimi and Mehdi Hariri, “An introduction to steganography methods”, *World Applied Programming, Vol (1), No (3), August 2011*, pp.191-195.

[3]. Mohammed Salem Atoum, Mamoun Suleiman Al Rababaa, Dr. Subariah Ibrahim, Osamah Abdulgader Ahmed, “A Steganography Method Based on Hiding secrete data in MPEG/Audio Layer III”, *IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.5*, May 2011, pp 184-188.

[4]. M. L. Mat Kiah1, B. B. Zaidan, A. A. Zaidan, A. Mohammed Ahmed1 and Sameer Hasan Al-bakri, “A review of audio based steganography and digital watermarking”, *International Journal of the Physical Sciences Vol. 6(16),* 18 August, 2011, pp. 3837-3850.

[5]. Haider Ismael Shahadi, Razali Jidin, "High Capacity and Inaudibility Audio Steganography Scheme", *7th International Conference on Information Assurance and Security (IAS)*, IEEE 2011.

[6]. R. Sridevi, A. Damodaram and S.V.L. Narasimham, “Efficient Method of Audio Steganography by Modified LSB Algorithm and Strong Encryption Key with Enhanced Security,” *Journal of Theoretical and Applied Information Technology*, vol. 5, no. 6, pp. 768 – 771, June *2009*.

[7]. D. Kirovski and H. Malvar, “Spread-spectrum Watermarking of Audio Signals,” *IEEE Transactions on Signal Processing*, vol. 51, no. 4, pp. 1020 – 1033, April *2003*.

[8]. W. Bender, D. Gruhl and N. Morimoto, “Techniques for Data Hiding,” *IBM Systems Journal*, vol. 35, no. 3, pp. 313 – 336 ,1996.

[9]. D. Huang and T. Yeo, “Robust and Inaudible Multi-echo Audio Watermarking,” *Proceedings of the IEEE Pacific-Rim Conference on Multimedia*, pp. 615 – 622, Taipei, China, December 2002.