Audio Steganography using Probabilistic Global Search Lausanne Algorithm

Ei Thin Su
University Of Computer Studies (Yangon)
eithinsu.ucsy@gmail.com

Abstract

Audio Steganography is an art of hiding secret information within multimedia objects to prevent unauthorized persons. Information hiding technique using audio sound files is a new kind of secret communication technology. Fast improvement of Internet and digital information revolution caused major changes in the overall culture. Audio data hiding method is one of the most effective ways to protect our privacy. Nowadays, embedding message within audio files is still challenging problems. In this paper, we present one of the problem transformation method, PGSL algorithm is used for secure digital audio Steganography. Message bits are embedded within the best points of audio file through PGSL to have high security as well as robustness.

1. Introduction

The rapid development of multimedia and internet allows for wide distribution of digital media data. It becomes much easier to edit, modify and duplicate digital information. Besides that, digital documents are also easy to copy and distribute, therefore it will be faced by many threats. It is a big security and privacy issue, it become necessary to find appropriate protection because of the significance, accuracy and sensitivity of the information. Steganography considers one of the techniques which used to protect the important information. Steganography can be used in a large amount of data formats in the digital world. The most popular data formats used are .bmp, .doc, .gif, .jpeg, .mp3, .txt and .wav.

Information hiding technique using Audio sound files is a new kind of secret communication technology. With the popularity of internet services today, thousands of millions people are using internet daily for communication. Bandwidth of internet is growing wider and wider, and price of computer related devices is becoming cheaper and cheaper but security risks are highly raised. Fast improvement of the Internet and digital information revolution caused major changes in the overall culture. Audio data hiding method is one of the most effective ways to protect our privacy. Audio data hiding can also be used for the protection of copyrighted digital media, and to the government for information systems security and covert communication. Users can use audio cover channel to send security information without being detected and attacked by hackers easily, significantly reducing vulnerability to snooping and other attacks. It can also be used in forensic applications for inserting hidden data into audio files for the authentication of spoken words and other sounds, and music commercial for the monitoring of the songs over broadcast radio.

Audio Steganography can be characterized by a number of defining properties as transparency, fidelity and capacity, which are most important for audio steganography.

Transparency evaluates the audible distortion due to signal modifications like message embedding or attacking. In most of the applications, the secret data insert within audio file without affecting the perceptual quality of the audio host signal to robustness and withstand against intentional and unintentional attacks.

Fidelity measures perceptual similarity between cover object and stego object. However, the quality of the stego audio is usually degraded, either intentionally by an adversary or unintentionally in the transmission process, before a person perceives it. In order to meet fidelity constraint of the embedded information, the perceptual distortion introduced due to embedding should be below the masking threshold estimated based on the HAS and the host media.

Capacity in data hiding indicates the total number of bits hidden and successfully recovered by the Stego system.

2. Related Work

There has been a significant amount of research on audio steganography. The previous methods have been proposed in the Audio Steganography are Low-bit Encoding [2],[5], Phase coding [6], Echo data hiding [6] and Spread Spectrum coding [6]. General methods used (lower sensitivity of Human Auditory System) by a little changing of frequency, phase and amplitude of audio sound files have also been proposed.

In Low-bit encoding, the binary version of the secret data message is substituted with the least significant bit (LSB) of each sample of the audio cover file [2], [5]. 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.

Phase coding 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). 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. 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 [6]. Hence, the Phase Coding method is normally used only when a small amount of data embedded.

Spread Spectrum coding method spreads the secret message across the frequency spectrum of the audio signal. Spread Spectrum coding method can perform better than LSB coding and Phase coding techniques [6]. However, like LSB coding method, Spread Spectrum method can introduce noise to the audio file.

Wang et al [3], propose an audio watermarking algorithm based on HAS principles. The procedure involves selecting an audio clip immediately after a loud sound. The clip is transformed to the frequency domain and spectral components adjacent to high peaks are selected. A combination of a pn-sequence and secure data is embedded in a frequency band. Detection is achieved by autocorrelation properties of pn-sequences. High embedding capacity is achieved by QAM modulation techniques. In [7], Tian proposes an integer wavelet transform based watermarking algorithm. The algorithm uses the integer wavelet transform to obtain the integer coefficients in the transform domain. The binary representation of the coefficient is looked at and an additional bit representing secure information is added, thereby ‘expanding’ the coefficient. A location map is embedded that identifies the pixels that are changed. Tilki and Beex [4], propose an algorithm for encoding a 35 bit digital signature onto the audio component of a television signal.

The digital signature is encoded using 167 sinusoids in the 2.4 to 6.4 KHz range, specifically chosen as human sensitivity declines compared to its peak at 1 KHz. The 167 frequencies are chosen to correspond to the bin frequencies of the 4096 point FFT of the original audio segment. The digital signature is then added to the audio component. The signature is detected by comparing the magnitude of adjacent FFT bins to a threshold and making a decision.

To secure between sender and receiver, the new high secure audio steganography method (PGSL) is proposed in this work.

3. Background

Propose System performs global search using PGSL algorithm by sampling the solution space using a probability density function (PDF) within audio file. The beginning of search, a uniform probability density function is assumed for entire search space. Probabilities in these regions are increased when good solutions are found. Better sets of points are found in the neighborhood of good sets of points. Search space is narrowed down so convergence is achieved.

PGSL algorithm includes four nested cycles:

-Sampling Cycle
-Probability Updating Cycle
-Focusing Cycle
-Subdomain Cycle

Sampling Cycle- Number of samples are generated randomly according to current probability density function. Each point is evaluated by user-defined objective function and best point is selected.

Probability Updating Cycle- The sampling cycle is invoked number of probability updating cycle times. After each iteration, the probability density function of each variable is modified using the probability-updating algorithm. This ensures that the sampling frequencies in regions containing good points are increased and regions containing bad solutions are decreased.

Focusing Cycle- Search is focused on the interval containing the best solution after a number of Probability Updating Cycle, by further subdivision of interval.

Subdomain Cycle- Search space is progressively narrowed by selecting a subdomain of smaller size center on the best point after each Focusing Cycle.

4. Propose System

The propose system will resolve the problems of low robustness against attacks which try to reveal hidden message and less embedding capacity. An intelligent algorithm will try to embed the message bits in the best samples.

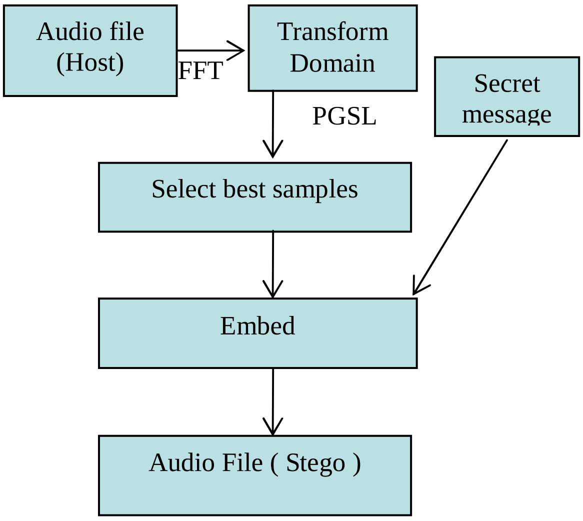

Fig: Approach Diagram

5. Expected Outcome

In this propose system where covert data is embedded into the coefficients of host audio (cover signal) in transform domain. Firstly, Statistical measures of audio features are calculated in the transform domain and the best coefficients are selected and then best point is searching by using Probabilistic Global Search Lausanne algorithm to embed secret message. The inverse transform is applied to the modified coefficients to form new audio sequence (stego signal). The propose system focus on to prevent intentional and unintentional attacks. All experiments will be carried out using the MATLAB software. Propose method might be support secure communication.

6. Conclusion

The propose system overcomes all the restrictions made on the existing systems. It provides to improve secure communication using digital media, to design robust covert communication system, to fulfill the requirement of weak points and to develop information hiding of audio steganography which can offer high embedding, unperceptibility and robustness. According to the literature review, most of past proposed system have not been perfect requirements. Some research concerned human imperceptibility, some desire capacity. Still weak of security. To reduce the weakness of above method, we will be used embedding message after searching the best points and using PGSL algorithm.Thus, our propose system might improve higher secret covert communication, higher imperceptibility of embedding, larger payload and correct recovery of embedded information and robustness.

7. References

[1]. K. Gopalan, "Audio steganography using bit modification, "*Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing", (ICASSP 03), Vol. 2, pp. 421-424,* April 2003.

[2]. N. Cvejic and T. Seppanen," Increasing Robustness of LSB Audio Steganography Using a Novel Embedding Method", *Proceedings of IEEE International Conference on Information Technology,* August 2004.

[3]. S. Wang, X. Zhang, and K. Zhang, "Data Hiding in Digital Audio by Frequency Domain Dithering," *MMMACNS, Springer-Verlag, Berlin Heidelberg,* 2003, pp.383-394.

[4]. J.F. Tilki and A.A. Beex, "Encoding a Hidden Digital Signature onto an Audio Signal Using Psychoacoustic Masking," *in Proc. 7th International Conference on Signal Processing Applications & Technology, Boston MA*, October 1996, pp. 476-480.

[5]. C. Psrthasarathy, Dr.S.K.Srivatsa " Increased Robustness of LSB Audio Steganography by Reduced Distortion LSB Coding " , *Journal of Theoretical and Applied Information Technology,* @ 2005-2009 JATIT.

[6]. F. Han, M. J. Tung, K. Xu, " Robust Audio Steganography using Direct-Sequence Spread Spectrum Technology", 2007.

[7]. Tian, Jun, "High Capacity Reversible Data Embedding and Content Authentication," *IEEE Conference on Acoustics, Speech and Signal Processing*, vol. 3, pp. 517-520, 2003.