Hiding Data in Wave Files

Pushpa Aigal
Department of Computer Science,
Shivaji University, Kolhapur,
Maharashtra 416004.

Pramod Vasambekar
Department of Computer Science,
Shivaji University, Kolhapur,
Maharashtra 416004.

ABSTRACT

Hiding information is an art and science of communication technology. Using Steganography information can be hidden within other information that it cannot be detected, but only by its intended recipient. Now a days for hiding information there are different multimedia systems like audio etc. Embedding secret message in sound is a difficult process. There are varying techniques for embedding information in audio. In this paper we will attempt the general principles of hiding secret information using audio techniques and an overview of its functions.

General Terms

Audio Steganography, Security, Secret data transmission

Keywords

Steganography, Encryption, Decryption, Audio, LSB Method

1. INTRODUCTION

Steganography is the technique of hiding information in some media for the safe communication. This technique relies on encoding messages in transport layers in such a manner that the existence of the message is unknown to an observer. The aim of Audio Steganography is to hide a message in some cover media and to obtain new data which is indistinguishable from the original message, by people in such a way that any eavesdropper cannot detect the presence of the original message in new data. Computers and Networks, has made information hiding in Covert channels and text possible. Now days audio files are available everywhere and moreover; today's technology allows the copying and redistribution of audio files over the Internet at a very low or almost no cost. So it is necessary to have methods that confine access to these audio files and also for its security. Audio Steganography is one of the solutions.

In Audio Steganography, the weakness of the Human Auditory System (HAS) is used to hide information in the audio [1]. Many programs are available in the internet that use Steganography to hide the secret information. The media's that use digitally embedding message are plain text, hypertext, audio/video, still image and network traffic. There exists a large variety of Steganography techniques with varying complexity and possessing, some with strong and weak aspects. Information hiding in text is the most popular method of Steganography. It is used to hide a secret message in every nth character or altering the amount of white space after lines or between words of a text message [2]. It is used in the initial decade of the internet era. But it is not used frequently because the text files have a small amount of redundant data. This technique lacks in payload capacity and robustness. To hide data in audio files, the secret message is embedded into the digitized audio signal. The audio data hiding method provides the most effective way to protect privacy. A key aspect of embedding text in audio files is that, no extra bytes are generated for embedding. Hence it is more comfortable to transmit the huge amount of data using audio signal. Embedding the secret messages in digital sound is usually a very difficult process [3]. A famous illustration of Steganography is Simmons' Prisoners' Problem [4]. Based on this model we can assume that that both the sender and receiver share some common secret information. This corresponding Steganography protocol is known as secret key Steganography. If the public key of the receiver is known to the sender, the Steganography protocol is called public key Steganography [5], [6], [7].

A thorough knowledge of Steganography methodology and its model with high security features has been presented in [5], [6], [7], [9].

Almost all digital file formats can be used for Steganography, but the image and audio files are more suitable because of their high degree of redundancy [6].

2. Different kinds of Steganography

The five main categories of file formats that can be used for steganography are:

1. Text
2. Images
3. Audio
4. Video
5. Protocol

1. **Text steganography**: Hiding information in text is one of the most important methods of steganography. This method is used to hide a secret message in every nth letter of a word in the text message. It has lost its importance in the internet era internet and because of different type of digital file formats. Using digital files Text stenography is not used very often because the text files have a very small amount of redundant data.

2**. Image steganography**: Images are used as the popular cover objects for steganography. A message is embedded in a digital image through an embedding algorithm, using the secret key. The resulting stego image is send to the receiver. On the other side, using the extraction algorithm and the same key it is processed. During the transmission of stego image unauthorized persons can only notice the transmission of an image but can't guess the existence of the hidden message.

3. **Audio Steganography**: Audio stenography is masking, which exploits the properties of the human ear to hide information unnoticeably. An audible, sound can be inaudible in the presence of another louder audible sound .This property allows to select the channel in which to hide information.

4. **Video Steganography**: Video files are generally a collection of images and sounds. So most of the techniques used in images files and audio files can be applied to video files also. The great advantages of video is that large amount of data that can be hidden inside and since it is a moving stream of images and sounds, the continuous flow of information otherwise noticeable distortions might go unobserved by humans beings.

5. **Protocol Steganography**: The protocol steganography is used to embed information within the network protocols, such as TCP/IP. Information can be hidden in the header part of a TCP/IP packet and in some fields which are either optional or are never used.

3. Techniques of Audio Steganography

Some commonly used techniques of audio Steganography are listed and discussed below.

3.1 Temporal Domain

The main techniques under temporal domain are

- Least Significant Bit (LSB) Coding
- Parity Coding
- Echo data hiding

The Least Significant Bit Coding (LSB) : LSB is one of the earliest techniques in the information hiding of digital audio, as well as other media types. In this technique LSB of binary sequences of each sample of digitized audio file is replaced with the binary equivalent of secret message [9]. For example if we want to hide the letter A, (binary equivalent **1000001**) into a digitized audio file where each sample is represented with 16 bits, then LSB of 7 consecutive samples (each of 16 bit size) is replaced with each bit of the binary equivalent of the letter, A [8] .

Advantages: It is the simplest form to embed information in a digital audio file. It allows a large amount of data to be concealed within an audio file. Use of only one LSB of the host audio sample gives a capacity equivalent to the sampling rate which could vary from 8 kbps to 44.1 kbps (all samples used) [9]. This method is more widely used, as modifications to LSB's usually do not create audible changes to the sounds.

Disadvantage: It has considerably low robustness against attacks.

Parity Coding [10]: In Parity coding method instead of breaking a signal down into individual samples, it breaks the signal down into separate regions of samples and encodes each bit from the secret message into a sample region's parity bit. If the secret bit to be encoded does not match the parity bit of a selected region the process flips the LSB of one of the samples in the region.

Advantage: The sender has more of a choice in encoding the secret bit, and the signal can be changed in a more unobtrusive manner.

Disadvantage: LSB coding is not robust in nature, in this method.

Echo data hiding [11]: In Echo hiding data is embedded in the audio file by introducing an echo to the original signal. This method allows high data transmission rate and provides superior robustness against noise inducing method. The encoded data successfully, the three parameters of the echo are varied: amplitude, decay rate, and offset (delay time) from the original signal. All parameters are set below the human hearing threshold, so the echo is not resolved easily. If only one echo is produced from the original signal, then only one bit of information could be encoded. So original signal is broken into blocks before encoding process and then concatenated to create a final signal.

Advantage: The main benefit is that to extract the secret message from the stego-signal, the receiver must be able to break the signal into the same block sequence used during the encoding process.

Disadvantage: The autocorrelation function of the signal's frequency can be used to decode the message because it reveals a spike at each echo time offset, allowing the message to be reconstructed.

3.2 Frequency Domain

Frequency domain and wavelet domain techniques come under transform domain. The main techniques under frequency domain are

- Tone Insertion
- Phase Encoding
- Spread Spectrum

Tone Insertion: [12] In Tone insertion method frequency masking property is exploited. In the presence of a stronger tone a weak pure tone is masked. For embedding the information masking property of inaudibility is used in different ways.

Advantage: It exploits the masking property.

Disadvantage: It has low embedding capacity.

Phase Coding [10]**:** Phase coding relies on the fact that the phase components of sound are not as perceptible to the human ear as noise is. This method works by replacing the phase of an initial audio segment with a reference phase that represents the data. The phase of subsequent segments is then adjusted in order to preserve the relative phase between segments.

Advantage: The secret message can't be extracted easily from sound file as the receiver should know the segment length, to use the Discrete Fourier Transform (DFT) to get the phases extract.

Disadvantage: It is a complex method and data embedding rate is very low, so secret messages are encoded in first signal only.

Spread Spectrum (SS) [9]: Spread Spectrum attempts to spread the encoded data across the signal's frequency spectrum as much as possible. It is equivalent to a system using the LSB coding, which randomly spreads the message bits over the entire sound file. The main difference is that unlike LSB coding, the SS method spreads the secret message over the sound file's frequency spectrum, using a code that is independent of the actual signal. As a result, the final signal occupies a bandwidth which is excess of what is actually required for transmission.

Advantage: It offers moderate data transmission rate while maintaining a high level of robustness.

Disadvantage: Noise can be introduced into a sound file.

3.3 Wavelet Domain

Wavelet domain [13] 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 work with wavelet coefficient. Upon applying the inverse transform, the stegano signal can be reconstructed.

Advantage: It has high data hiding capacity and transparency.

Disadvantage: Lossy data retrieval.

4. AUDIO STEGANOGRAPHY

The audio files may be modified for hiding data like other digital media like image, text or video. The methods that embeds data in sound files use the properties of the Human Auditory System (HAS). The HAS perceives the additive random noise and also the perturbations in an audio file can also be detected. While the HAS have a large dynamic range, but it has a fairly small different range. As a result, loud sounds tend to mask out quiet sounds. And there are also some distortions that are so common that the HAS ignores them. When we observe the audio wave file before embedding and after embedding secret data respectively in Fig.1 and Fig.2 the human auditory system can’t recognize the small change.

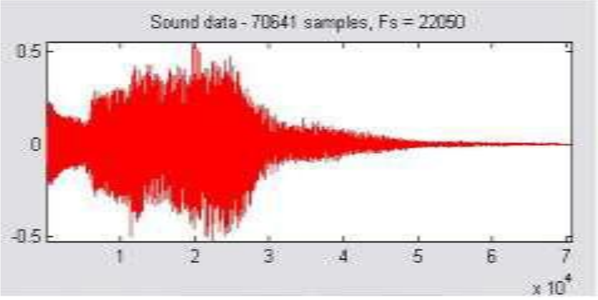

Fig...1: Before embedding the text

The digital sound is obtained from the analog sound by converting it to digital domain. This process implies two sub processes: sampling and quantization. Sampling is the process in which the analogue values are only captured at regular time intervals.

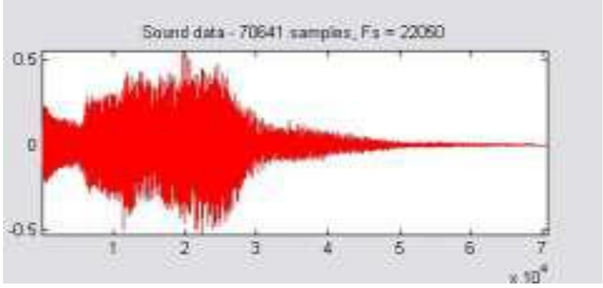

Fig.2: After embedding the text

Quantization converts each input value into one of a discrete value. Popular sampling rates for audio include 8 kHz, 9.6 kHz, 10 kHz, 12 kHz, 16 kHz, 22.05 kHz and 44.1 kHz. The most popular file formats for kHz and 44.1 kHz. The most popular file formats for sounds are the Windows Audio-Visual (WAV) and the Audio Interchange File Format (AIFF). There are also compression algorithms such as the International Standards Organization Motion Pictures Expert Group-Audio (ISO MPEG-AUDIO). When developing a data hiding method for audio, one of the first considerations is the likely environments the sound signal will t ravel between encoding and decoding. The two main areas of modification to be considered are, the storage environment or digital representation of the signal that will be used and the transmission pathway the signal might travel [3, 4]. In order to conceal secret messages successfully, a variety of methods for embedding information in digital audio have been introduced. These methods range from rather simple algorithms that insert information in the form of signal noise to more powerful methods that exploit sophisticated signal processing techniques to hide information. This section of the paper is organized as follows. First, the clarification of the Audio Environment. Secondly, this section describes as one of the wide range of techniques that have been used in Audio Steganography.

4.1 Technique used for Data Hiding in Audio

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 a large amount of data to be encoded [14]. The following Fig.3 demonstrates how the message 'HEY' is encoded in A 16-bit CD quality sample using the LSB method: In LSB coding, the ideal data transmission rate is 1 kbps per 1 kHz. However, in some implementations of LSB coding, the two least significant bits of a sample are replaced with two message bits. This increases the amount of data that can be encoded but also increases the amount of resulting noise in the audio file as well. Thus, one should consider the signal content before deciding on the LSB operation to use. For example, a sound file that was recorded in a bustling subway station would mask low-bit encoding noise. On the other hand, the same noise would be audible in a sound file containing a piano solo.

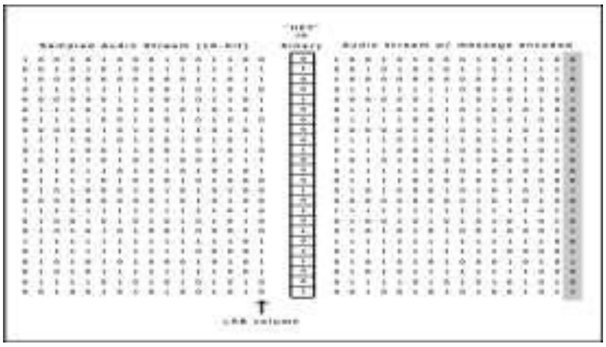

Fig .3: Embedding secret text in the LSB posit ion of Audio Stream

To extract a secret message from an LSB encoded sound file, the receiver needs access to the sequence of sample indices used in the embedding process. Normally, the length of the secret message to be encoded is smaller than the total number of samples in a sound file. One must decide then on how to choose the subset of samples that will contain the secret message and communicate that decision to the receiver. One trivial technique is to start at the beginning of the sound file and perform LSB coding until the message has been completely embedded, leaving the remaining samples unchanged. This creates a security problem, however in that the first part of the sound file will have different statistical properties than the second part of the sound file that was not modified. One solution to this problem is to pad the secret message with random bits so that the length of the message is equal to the total number of samples. Yet now the embedding process ends up changing far more samples than the transmission of the secret required. This increases the probability, that a would-be attacker will suspect secret communication.

A more sophisticated approach is to use a pseudo random number generator to spread the message over the sound file in a random manner. One popular approach is to use the random interval method, in which a secret key possessed by the sender is used as a seed in a pseudo random number generator to create a random sequence of sample indices. The receiver also has access to the secret key and knowledge of the pseudo random number generator, allowing the random sequence of sample indices to be reconstructed. Checks must be put in place, however, to prevent the pseudo random number generator from generating the same sample index twice. If this happened, a collision would occur where a sample already modified with part of the message is modified again. The problem of collisions can be overcome by keeping track of all the samples that have already been used. Another approach is to calculate the subset of samples via a pseudo random permutation of the entire set through the use of a secure hash function. This technique ensures that the same index is never generated more than once. There are two main disadvantages associated with the use of methods like LSB coding. The human ear is very sensitive and can often detect even the slightest bit of noise introduced into a sound file, Second disadvantage however, is that this is not robust. If a sound file embedded with a secret message using either LSB coding was resampled the embedded information would be lost. Robustness can be improved somehow by using a redundancy technique while encoding the secret message. However, redundancy techniques reduce the data transmission rate significantly.

4.2 Proposed Method

4.2.1 Advantages of Proposed Method

- Imperceptibility – The imperceptibility is one of the important factor of a steganography system, as its strength system depends on its ability to be unnoticed by the human senses (HAS/HVS).
- Robustness - Robustness defines how strong this technique against changes is. It measures the capability of the embedded secret data against different types of changes intended or unintended.
- Payload capacity - Payload capacity is the amount of embedded data that can be hidden into a particular innocent cover medium relative to the size of this medium.
- Real Time Suitability - Steganography in real time audio signals involves relative requirements such as system complexity, throughput, bandwidth, delay, and absence of duplications, failure recovery, and service setup time.

4.3 LSB based Audio Steganography

- ❖ Here we select an audio file with ".wav" extension as host file.
- ❖ The LSB positions of a file have a very little Contribution in the audio perception
- ❖ So we assume that the least significant bit of that file has to be modified, without degrading the sound quality.

5. Embedding Secret Text in Audio

The process of embedding the text in audio file, Here we select audio file i.e. Windows Audio-Visual (WAV) file to input data. The file has 16-bit linear quantized digital audio samples. The header and data parts are separated. The secret text is placed in the header part and the LSB positions of the data element in alternate samples of LSB data element. Thus Stego audio file is created. It's a WAV file having hidden text, but there is no change in audibility of the Cover file.

5.1 Embedding Process

- ❖ The technique used is LSB coding. The audio file consists of data in bytes.
- ❖ To encode the message, we first find the length of the string.
- ❖ The offset in the original file, from which the encoding process must start.
- ❖ By default it is set to 500. This is done because, the WAV file has a header. In the initial offsets and if that header is tampered with, the destination file will not be able to access its header in the appropriate format.
- ❖ Encode that length which can be up to 256 Characters into the 1st 8 bytes of the audio file. This will assist us in the decoding process. Take each character from the message string, convert it into byte and change the LSB of the next 8 bytes of the audio file as per each of the bit of the character type.
- ❖ Repeat the same procedure till the message string gets exhausted.
- ❖ Thus on writing byte after byte to the new file, we get a new audio file ―output .wav having a message hidden into it which can be sent to the receiver without any fear of eavesdropper.

6. Extraction of secret text from Stego Audio

The Process of extracting the hidden text from a WAV audio file is as follows. The input file is Stego audio (WAV) file and then separated header and data parts. The header consists of size of secret text. Store LSB of data part and perform a left shift of the previous bit. Then convert binary to ASCII values. Thus the secret text can be extracted.

6.1 Extraction Process

- ❖ Select the audio file ―output .wav which has the message hidden in it.
- ❖ From the selected offset that was specified at the sending side (i.e. 500) , take the LSB of the next 8 bytes to get the length of the message (that was encoded in the first 8 bytes from the given offset) which will help us to get the encoded message only from the next 8 * length bytes of audio file.
- ❖ Create a byte from the LSB of the next consecutive 8 bytes and go on printing each of the character of the message string in the text box.
- ❖ Continue this process till the length of the string is reached. Finally we get the hidden message from the received audio file into the provided text box.
- ❖ Thus we have achieved the process of decoding a message from the audio file.

7. RESULT

The results can be obtained using MATLAB GUI tools, after compiling the program in MAT Lab, a GUI (Graphical User Interface). In this manner the secret text can be hidden and regenerated, which is difficult even to intruders imagination of getting the information.

8. CONCLUSIONS

Here we have proposed a very efficient audio Steganography system, in which the LSB technique is used to get high data hiding capacity and low perceptibility. So by using this technique the capacity of data hiding has increased and also the clarity of the covering medium (.wav audio), remains unchanged even after hiding text. This can be implemented on image Steganography also.

Future Scope: Security for this system can be boosted by using a concept called Cryptography (i.e., encryption and decryption) to the text data. The system can be further developed to hide a secret image in covert audio as well as in two dimensional and three dimensional signals.

9. REFERENCES

[1] Shahreza S.S. and Shalmani M.T.M., “Adaptive wavelet domain Audio Steganography with high capacity and low error rate”, in Proc. IEEE International Conference on Acoustics, Speech and Signal Processing, pp: 1729 – 1732, 2008.

[2] Bethany Delman, 'Genetic Algorithms in Cryptography Published in July 2004. https://ritdml.rit.edu/handle/1850/263, Accessed on 22nd Jan 2012

[3] Darrell Whitley,'A Genetic Algorithm Tutorial', Computer Science Department, Colorado State University, Fort Collins, CO 80523.

[4] Gustavus J. Simmons, The Prisoners' Problem and the Subliminal Channel, Proceedings of CRYPTO ,83(1984)51-57.

[5] RJ Anderson, Stretching the Limits of Steganography, Information Hiding, Springer Lecture Notes in Computer Science, 1174 (1996) 39-48.

[6] Scott. Craver, On Public-key Steganography in the Presence of an Active Warden, Proceedings of 2nd International Workshop on Information Hiding., (1998) 355-368.

[7] Ross J. Anderson. and Fabien A.P.Petitcolas, On the limits of Steganography, IEEE Journal on Selected Areas in Communications (J- SAC), Special Issue on Copyright and Privacy Protection,16(1998) 474- 481.

[8] Soumyendu Das, Subhendu Das, Bijoy Bandyopadhyay and Sugata Sanyal, “Steganography and Steganalysis:different_Steganograpy_Steganalysis_different_approaches.pdf.

[9] “Audio steg: methods”, Internet publication on www.snotmonkey.com http://www.snotmonkey.com/work/school/405/methods.htm. Accessed on 22nd Jan 2012

[10] N. Cvejic, T. Seppanen, "Increasing Robustness of LSB Audio Steganography using a novel embedding method", in Proc. IEEE Int. Conf Info. tech.: Coding and Computing, Vol. 2, pp.533-537, April 2004.

[11] Samir K Bandyopadhyay, Debnath Bhattacharyya, Debashis Ganguly, Swarnendu Mukherjee and Poulami Das, “A Tutorial Review on Steganography” http://www.jiit.ac.in/jiit/ic3/IC3_2008/IC32008/APP2_21.pdf, Accessed on 22nd Jan 2012

[12] K. Gopalan and S. Wenndt, “Audio Steganography for covert data transmission by imperceptible tone insertion “, Proceedings of Communications Systems and Application, IEEE, 2011.

[13] N. Cvejic, T. Seppanen, “A wavelet domain lsb Insertion algorithm for high capacity audio Steganography “, IEEE International Conference on Acoustics, speech and Signal Processing, ICASSP 2008.

[14] P. Ramesh Yadav, V. Usha Shree, K. Padmapriya, Hiding Data in Audio Using Audio Steganography, International Journal of Computer Applications in Engineering Sciences, ISSN: 2231-4946 .