



INTERNATIONAL JOURNAL OF
RESEARCH IN COMPUTER
APPLICATIONS AND ROBOTICS
ISSN 2320-7345

**A NOVEL LSB BASED AUDIO
STEGANOGRAPHY**

A. Seetha Rama Raju¹, V. Srinivasa Rao², Mohammed Imamuddin³

¹M.Tech (ECE) Aurora's Scientific Technological & Research Academy, JNTU -Hyderabad.
Seetharaju601@gmail.com

²Associate prof (ECE) Aurora's Scientific Technological & Research Academy, JNTU Hyderabad .

³Associate prof (ECE) Aurora's Scientific Technological & Research Academy, JNTU Hyderabad

Abstract

Steganography is the art and science of hiding information in an audio file. This paper proposes a novel steganography scheme for hiding data in an audio file for increasing the hiding capacity and robustness. In the proposed technique, first the audio file is sampled and then an appropriate bit of each alternate sample is altered to embed the textual information. As a steganography approach the perceptual quality of the host audio signal was not to be degraded.

Keywords: Audio steganography, LSB, Robust-ness, Audio signals

1. Introduction

Steganography has importance in the past few years due to the increasing need for providing secrecy in an open environment like the internet, tenders for business deals etc. With almost anyone can observe the communicated data all around, steganography attempts to hide the very existence of the message and make communication undetectable and secure. Many techniques are introduced to secure information.

Modern steganography is generally understood to deal with electronic media rather than physical objects. There have been numerous proposals for protocols to hide data in channels containing pictures[1,2,3], video [3,4], audio [1,3] and even typeset text [1,3]. This makes sense for a number of reasons. First of all, because the size of the information is generally quite small compared to the size of the data in which it must be hidden (the cover text), electronic media is much easier to manipulate in order to hide data and execute the algorithms necessary to

retrieve the messages. Electronic data also often includes redundant, unnecessary and unnoticed data spaces which can be manipulated in order to hide messages.

The main goal of this paper was to a way that an audio file can be used as a host media to hide textual message without affecting the file structure and content of the audio file. Because degradation in the perceptual quality of the cover object may leads to a noticeable change in the cover object which may leads to the failure of objective of steganography.

2. Assumption and Scope

Modern steganography based on embedding of secret data into electronic media like image [1, 2, 3], audio [1, 3], video [3, 4] and text [1, 3]. For example, to a computer, an image is an array of numbers that represent light intensities at various pixels. A common image size is 640 x 480 pixels and 256 colors (or 8 bits per pixel). Scan image could contain about 300kilobits of data[5] Digital images are typically stored in either 24 bit or 8 bit files. A

24 bit image provides the most space for hiding information. A data – embedding technique into an audio file can based on frequency masking [6], temporal masking [7], bit modification [8], LSB based method based on lifting wavelet transform [9] etc. It has been already proved that modification of the least significant bit creates a minimal change in the audio file format [1]. So while embedding text into an audio file LSB modification creates an imperceptible change in the host audio file.

A steganography system, in general, is expected to meet there key requirements, namely, imperceptibility of embedding, accurate recovery of embedded information, and large payload (payload is the bits that get delivered to the end use at the destination) [1]. In a pure steganography framework, the technique for embedding the message is unknown to anyone other than the sender and the receiver. An effective stenographic scheme should possess the following desired characteristics [10-11]:

Secrecy: a person should not be able to extract the covert data from the host medium without the knowledge of the proper secret key used in the extracting procedure. **Imperceptibility:** the medium after being embedded with the covert data should be indiscernible from the original 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 as possible.

Resistance: the covert data should be able to survive when the host medium has been manipulated, for example by some lossy- compression scheme [12].

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 communication like cryptography. But steganography must not be confused with cryptography [13], where one transforms the message so as to make its meaning obscure to malicious people who intercept it. Therefore, the definition of breaking the system is different [14]. In cryptography, the system is broken when the attacker can read the secret message. Breaking a stenographic system needs the attacker to detect that steganography has been used and he is able to read the embedded message.

3. Related Works

A Survey of stenographic techniques [15] reveals that there have been several techniques for hiding information or message in host messages in such manner that the embedded data should be imperceptible.

Substitution system [15] substitutes redundant parts of a cover with a secret message. Spread spectrum techniques adopt ideas from spread spectrum communication [3]. The statistical method encodes information by changing several statistical properties of a cover and use hypothesis testing in the extraction process [3]. Distortion process stores information by signal distortion and measure the deviation from the original cover in the decoding step [15]. The cover generation method encodes information in the way a cover for secret communication is created [3]. In case of hiding information in digital sound, phase Coding [16] embeds data by altering the phase a predefined manner. To a certain extent, modification of the phase of a signal cannot be perceived by the human auditory system (HAS)[6].

All these stenographic techniques deal with a few common types of steganography procedure depending on the variation of the host media. That means the cover object [13] or the carrier object which will be used to hide the secret data. Different media like images, text, video and audio has been used as a carrier or host media in different times [17].

Using audio file as cover object directs to Audio steganography. Practical audio embedding systems face hard challenges in fulfilling all three requirements due to the large power and dynamic range of hearing, and the large range of audible frequency of the [1].

The human auditory system (HAS) perceives sounds over a range of power greater than 10:1 and a range of frequencies greater than 10:1. The sensitivity of the HAS to the Additive White Gaussian Noise (AWGN) is high as well; this noise in a sound file can be detected as low as 70 dB below ambient level. On the other hand, opposite to its large dynamic range, HAS contains fairly small different range, i.e. loud sounds generally tend to mask out weaker sound [18]. Additionally, HAS is insensitive to a constant relative phase shift in a stationary audio signal and some spectral distortions interprets as natural, perceptually non-annoying ones.

Two properties of the HAS dominantly used in steganography techniques are frequency masking [18] and temporal masking [7]. The concept using the perceptual holes of the HAS is taken form wideband audio coding (e.g. MPEG compression 1, layer 3, usually called mp3) [19]. In the compression algorithms [7], the holes are used in order to decrease the amount of the bits needed to encode audio signal, without causing a perceptual distortion to the coded audio. On the other hand, in the information hiding scenarios, masking[18] properties are used to embed additional bits into an existing bit stream, again without generating audible noise in the audio sequence use for data hiding.

Some of the audio stenographic techniques are Lossless Adaptive Digital Audio Steganography [7], LSB based Audio Steganography [9], Audio Steganography using bit modification [8] etc.

4. Design Methodology

In the current endeavour, an audio file with “.wav” extension has been selected as host file. It is assumed that the least significant bits of that file should be modified without degrading the sound quality.

To do that, first one needs to know the file structure of the audio file. Like most files, WAV files have two basic parts, the header and the data. In normal wav files, the header is situated in the first 44 bytes of the file. Except the first 44 bytes, the rest of the bytes of the file are all about the data. The data is just one giant chunk of samples that represents data, one can't deal with the header section. That is because a minimal change in the header section leads to a corrupted audio file.

A program has been developed which can read the audio file bit by bit and stores then in a different file. The first 44 bytes should be left without any changes in them because these are the data of the header section. Then start with the remaining data field to modify them to embed textual information. For example, if the word “Audio” has to be embedded into an audio file one has to embed the binary values of the word “Audio” into the audio data field.

Consider the following table: TABLE I

Letter	ASCII	Corresponding Binary
A	065	01000001
U	117	01110101
D	100	01100100
I	105	01101001
O	111	01101111

TABLE I

LETTERS WITH ASCII VALUES AND CORRESPONDING BINARY VALUES

From the table, one can come to a point that to embed the word “Audio” into the host audio file actually the corresponding eight bit binary values have to be embedded into the data field of that audio file.

4.1 Algorithm

To develop this algorithm multiple bits of each sample of the file have been changed or modified to insert text data in it. It has also been observed the degradation of the host audio file after modification of the bits. The bit modification was done by various ways, like

1,2,3,4 bits were changed in turn.

But after a going through all the modification it has been observed that 1 bit change in LSB gave the best result. Thus, data can be embedded according to the following algorithm.

A. Algorithm (For Embedding of Data): RSA cryptography

Leave the header section of the audio file untouched

Start from a suitable position of the data bytes. (For the experiment purpose the present start byte was the 51st byte). Edit the least significant bit with the data that have to be embedded. Take every alternative sample and change the least significant bit to embed the whole message.

The data retrieving algorithm at the receiver's end follows the logic as the embedding algorithm

B. Algorithm (For Extracting of Data):

Leave first 50 bytes Start from the 51st byte and store the least significant bit in a queue.

Check every alternate sample and store the least significant bit in the previous bit. Convert the binary values to decimal to get the ASCII values of the secret message. From the ASCII find the secret message.

5. Experimentation, Result and Interpretation

An audio file named audio.wav has been selected for this experiment. After checking the binary values of each sample, first 44 samples were left without any changes. The data embedding with LSB modification has been started after the header section. If the data embedding process is started from 51st sample then the LSB value of the 51 sample value of the corresponding sample is "01110100" then "1" should be modified.

From table 1 it can be observed that to embed the letter "A", the sender has to embed the binary value "01000001". That is why according to the embedding algorithm "A" should be embedded according to Table II.

Sample No.	Binary values of corresponding sample	Binary value to be embed	Binary values after modification
51	01110100	0	0111010
53	01011110	1	0101111
55	10001011	0	1000101
57	01111011	0	0111101
59	10100010	0	1010001
61	00110010	0	0011001
63	11101110	0	1110111
65	01011100	1	0101110

TABLE II

SAMPLES OF AUDIO FILE WITH BINARY VALUES BEFORE AND AFTER EMBEDDING

According to the same way the remaining consecutive letters of the word “Audio” is embedded in the file audio.wav

From the table, it is clearly observed that after getting 01000001 in the queue it is converted into the equivalent decimal that is 65, the ASCII of “A”. Thus “A” is retrieved. Like the same way, the next letters also have been retrieved and hence the complete word “Audio”.

6. Conclusion

A method of embedding text-based data into a host audio file using the method of bit modification has been presented in this paper. A procedure has been developed in which the data field is edited to embed intended data into the audio file. To proceed with this, the header section of the audio has been checked perfectly because a minimal change in the header section may leads to a corruption of whole audio file.

In this algorithm, as an experiment first 50 bytes have left untouched and starting from the 51st bytes every alternate sample has been modified to embed textual information. How the performance is affected by changing different bit fields has not been reported in this work. However a rough study was made to see how the changing of a specific bit field creates degradation in the host audio file and in which point it leads to perceptible change in the audible sound quality to any other third party other than the sender or receiver. It was noticed than the sender or receiver. It was noticed that changing the least significant bit of the bytes gave the best results.

An audio file with size 952 KB has been used. The maximum text file size that can be embedded in this audio file without degrading the file structure can be traced through a survey.

The main goal of this research work was embedding of text into audio as a case of steganography. The two primary criteria for successful steganography are that the stego signal resulting from embedding is perceptually indistinguishable from the host audio signal, and the embedded message is recovered correctly at the receiver. In test cases the text-based data has been successfully embedded to the audio file to visualize in what extent the target has been achieved. However future scope appears endless.

REFERENCES

- [1] w. Bender, D. Gruhl, N. Morimoto and A. Lu”techniques for datahiding”, IBM systems Journal vol. 35, Issues 3&4, 1996, pp. 313-336.
- [2]Kharrazi, M., Sencar, Husrev T, and “Image Steganography: Concepts and Practice”, WSPC, April 22, 2004.
- [3]K. Matsui and K. Tanaka. Video steganography. In: IMA Intellectual Property Project Proceedings, volume 1, pp 187-206, 1994.
- [4]Matsuoka.H, “Spread Spectrum Audio Steganography using Sub-band phase shifting”. Proceedings of the 2006 International Conference on Intelligent Information Hiding and Multimedia Signal processing (IIHMSP’ 06), IEEE, 2006.
- [5]K. Gopalan, “Audio Steganography using bit modification”, Proc. IEEE INT. Conf. Acoustics, Speech, and Signal Processing, Vol.2, pp.421-424, April 2003.
- [6]B. Chen, “Design and analysis of digital watermarking, information embedding, and data hiding systems,” Ph.D. dissertation, MIT, Cambridge, MA, June 2000.
- [7]J. Zillner, H. Federrath, H. Klimant et al.,“Modelling the security of Steganographic Systems”, in 2nd Workshop on Information Hiding, Portland, April 1998, pp.345-355.
- [8]Noll P., “Wideband speech and audio coding”. IEEE Communication Magazine 31(11): 993, pp 34-44.

Authors Biography



Seetha Rama Raju M.Tech student in electronics and communication engineering (ASTRA) Aurora's Scientific Tech & Research Academy.



Mohammed Imamuddin Associate prof (ECE) Aurora's Scientific Tech & Research Academy Exp 9 years Teaching, M.Tech (DEC) JNTU Ananthapur.



V. Srinivas Rao Associate prof (ECE) Aurora's Scientific Tech & Research Academy Exp 9 years Teaching, M.Tech (DEC) JNTU Ananthapur.