World Applied Sciences Journal 20 (Mathematical Applications in Engineering): 79-83, 2012
ISSN 1818-4952

DOI: 10.5829/idosi.wasj.2012.20.mae.99926

Increasing the Hiding Capacity of Low-Bit Encoding Audio Steganography Using a Novel Embedding Technique

R.F. Olanrewaju, Othman Khalifa and Husna binti Abdul Rahman @ Suliman

Department of Electrical and Computer Engineering, Faculty of Engineering,
International Islamic University Malaysia, 50728, Kuala Lumpur, Malaysia

Abstract: The rapid growth of multimedia transmission leads to lose the owner identity of their products. Therefore, the demand to secure such input is crucial. In this paper, an overview of steganography and its technique applied is introduced. A data hiding within audio signals is studied. LSB technique is used and simulated result is presented. The result is characterized by robustness and high bit rate. It was shown that length of the embedded message (secret message) does not affect the stego signal audibility as long as it does not exceed the length of the original signal.

Key words: Data hiding % Audio signal % Steganography % Least Significant Bit

INTRODUCTION

Transmission of digital information and data has tremendously increased ever than before. The availability and efficiency of global computer networks for the communication of digital information have accelerated the popularity of digital media. Digital images, video, audio and text have been revolutionized in the way they can be captured, stored, transmitted and manipulated and this gives rise to a wide range of applications in education, entertainment industries, economic fore casting,, medicine and the military and among other field [1]. Computers and networking facilities are becoming less expensive and more widespread. Creative approaches to storage, access and distribution of data have generated a lot of benefits in all field of multimedia. Features such as distortion-free transmission, compact storage and easy editing have been the main drive for such success. However, unrestricted access to digital multimedia has virtually unprecedented opportunities to pirate copyrighted material. As a result, most of the work in data hiding has been concentrated on hiding small information such as copyright information or a watermark in images, audio and video segments. This might information in multimedia object has become very active in recent years and the developed techniques have grown and been improved a great deal. Data hiding is also known as steganography, from the Greek word stegano for "covered" and graphos "to write" is [2]. Steganography or stego is an art of concealing communication in such a way that no one apart from the sender and intended recipient knows there is a hidden message [3].

Multimedia data hiding techniques have been developed a strong basis for steganography area with an expanding number of applications like digital rights management, covert communications, hiding executables for access control and annotation [4]. In all application scenarios given above, multimedia steganography techniques have to meet two basic requirements. The first prerequisite is perceptual transparency, for example cover object (object not containing any additional data) and stego object (object containing secret message) must be perceptually indiscernible [5]. Then capacity of data rate to be embedded. Apart from capacity, all the stego application has need of algorithms that detect and decode hidden bits without access to the original multimedia sequence (blind detection algorithm) as well as robustness to attacks. Robustness to attacks is application dependent. Some application requires a high robustness while others such as authentication application could be fragile in nature. The general requirements, challenges and principles of hiding data in an audio are the same as those for embedding information in a video [6]. Robustness of the hidden data,

Corresponding Author: R.F. Olanrewaju, Department of Electrical and Computer Engineering,
Kulliyyah of Engineering, International Islamic University Malaysia, 50728, Kuala Lumpur, Malaysia.
Tel: +603 61965402, Fax: +6196 4463, E-mail: frashidah@iium.edu.my

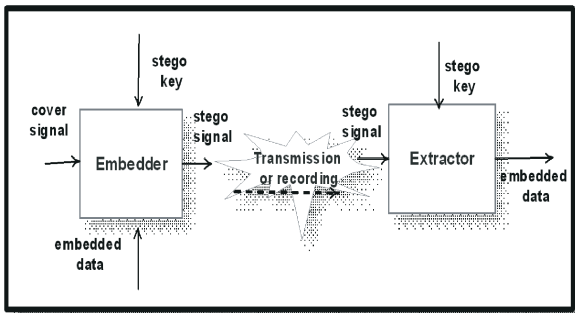

Fig. 1: Typical Block diagram of data hiding and retrieval.

for instance, is a key requirement for successful embedding and retrieval of the data. Furthermore, standard signal processing operations, such as noise removal and signal enhancement, must not result in loss or degradation of the embedded information. In addition, for covert communication, the embedded information must resist with channel noise and intentional attacks or jamming on the signal else a successful attack therefore consists of detecting the existence of this communication.

Background of Audio Steganography: The principle of data hiding was adopted at the first International Workshop on Information Hiding, Cambridge, U.K [7]. The terminology is illustrated in Figure 1.

A data message is hidden within a cover signal (object) in the block called embedder using a stego key, which is a secret parameter of a known hiding algorithm [8]. The output or the embedded signal is called stego signal. The embedded message is recovered by using the appropriate stego key in the block called extractor. There are many types of cover objects (signal) that can be used as a carrier of the hidden message; audio video, text and image. Nowadays data hiding in audio signal is one of the popular approaches. The idea of data hiding in audio signals comes from imperfection of human auditory system known as audio masking. In the presence of a load signal (masker), another weaker signal may be inaudible, depending on spectral and temporal characteristics of both masked signal and masker [9].

Related Work: Information hiding technique is a new kind of secret communication technology. Varieties of techniques for embedding information have been established. In much the same way most of the authors of the most journal papers mentioned that data hiding in audio signals exploits imperfection of Human Auditory System (HAS) known as audio masking. All the techniques have been introduced required knowledge of signal processing techniques, Fourier analysis and area of high level mathematics. When developing a hiding method for audio, one of the first considerations is the likely environments the sound signal will travel between encoding and decoding [10]. The two main areas of modification to be considered are; the storage environment, or digital representation of the signal that will be used and second the transmission pathway the signal might travel [11]

.

Least Significant Bit (LSB): LSB coding is one of the earliest techniques studied in the information hiding area of audio signal. The LSB watermark encoder usually selects a subset of all available host audio samples chosen by a secret key. The substitution operation on the LSBs is performed on this subset, where the bits to be hidden substitute the original bit values [4].

Advantages: Very high watermark channel bit rate and a low computational complexity of the algorithm

Disadvantage: Low robustness against signal processing modification.

Parity Coding: One of the earlier works in audio data hiding technique is parity. The parity coding method breaks a signal down into separate regions of samples and encodes each bit from the secret message in a sample region's parity bit. If the parity bit of a selected region does match the secret bit to be encoded, the process flips the LSB of one of the samples in the region. Thus, the sender has more of a choice in encoding the secret bit and the signal can be changed in a more unobtrusive fashion [12].

Advantage: Very high watermark channel bit rate and a low computational complexity of the algorithm

Disadvantage: Low robustness against signal processing modification.

Phase Coding: The phase coding method works by substituting the phase of an initial audio segment with a reference phase that represents the data. The phase of subsequent segments is adjusted in order to preserve the relative phase between segments [13,14]. Phase coding, when it can be used, is one of the most effective coding methods in term of the signal to perceived noise ratio.

When the phase relation between each frequency component is dramatically changed, noticeable phase dispersion will occur. However, as long as the modification of the phase is sufficiently small (sufficiently small depends on the observer; professional in broadcast radio can be detect modifications that are unperceivable to an average observer), an inaudible coding can be achieved [11].

Advantage: Robustness against signal modification

Disadvantage: Low data transmission rate

Spread Spectrum: In a normal communication channel, it is often desirable to concentrate the information in as narrow a region of the frequency spectrum as possible in order to conserve available bandwidth and to reduce power. The basic spread spectrum technique, on the other hand, is designed to encode a stream of information by spreading the encoded data across as much of the frequency spectrum as possible. This allows the signal reception, even if there is interference on some frequencies. While there are many variations on spread spectrum communication, we concentrate on Direct Sequence Spread Spectrum encoding (DSSS). The DSSS method spreads the signal by multiplying it by a chip, a maximal length pseudorandom sequence modulated at a known rate [11,12].

Advantage: Robustness against signal modification

Disadvantage: Vulnerability to a time scale modification.

Echo Hiding: In echo hiding, information is embedded in a sound file by introducing an echo into the discrete signal. Like the spread spectrum method, it too provides advantages in that it allows for a high data transmission rate and provides superior robustness when compared to the noise inducing methods. If only one echo was produced from the original signal, only one bit of information could be encoded. Therefore, the original signal is broken down into blocks before the encoding process begins. Once the encoding process is completed, the blocks are concatenated back together to create the final signal [8,15].

Advantage: High data transmission

Disadvantage: Low robustness against signal processing modification.

MATERIALS AND METHOD

The proposed scheme uses text as the secret data to be hidden in the LSB of audio file taken as cover object because the size of the file is generally small compared to the size of the audio file in which it must be taken. In order to hide the secret data, we use wave audio file at 44.1 kHz which have quality of sound characteristics.

The method steps are as follow:

- Receives the audio file in the form of bytes and converted into bit pattern.
- Each character in the message is converted in bit pattern.
- Replaces the LSB bit from audio with LSB bit from character in the message.

Embedding Process:

- Input the text that to be embedded and convert it into the binary.
- Read the selected audio file and convert it into binary.
- Encoding two binary data into the LSB part of the audio file.
- Hide message in audio file.

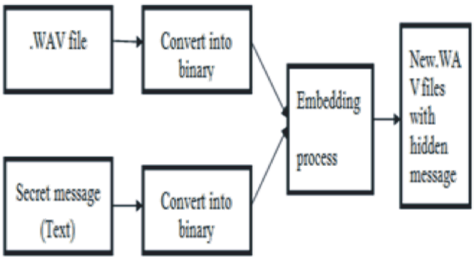

Fig. 2: Schematic Diagram of proposed embedding procedure

Table 1: Samples of audio sound, side and SNR values

SOUND	SIZE (kB)	SNR (dB)
Sound1	14.7	54.6
Sound2	42.2	55.3
Sound3	83.0	55.6
Sound4	83.0	58.7
Sound5	42.2	58.2
Sound6	82.3	54.5
Sound7	17.6	50.2
Sound8	11	40.0
Sound9	18.4	47.4
Sound10	42.2	54.7

Table 2: Embedded text and the SNR values

TEXT	SNR (dB)
Husna	54.7
Husnaa	54.7
Husnaab	54.7
Husnaabc	54.7
Husnaabcd	54.7
Husnaabcde	54.7
Husnaabcdef	54.7
Husnaabcdefg	54.7

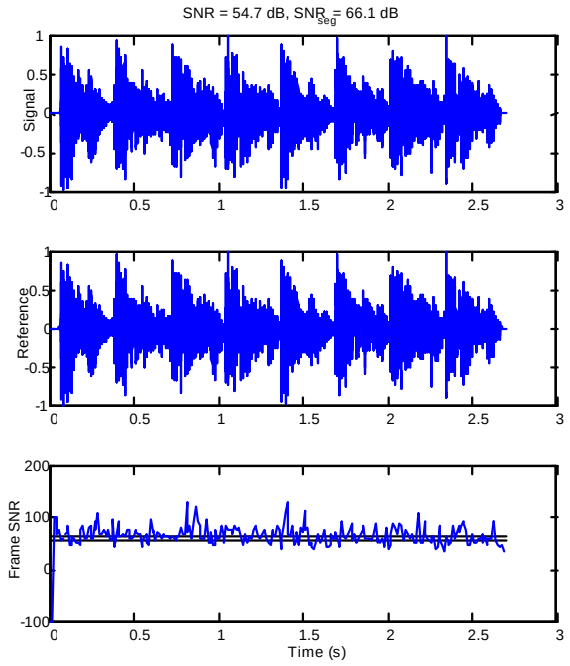

Fig. 3: Stego Signal, Original Signal and the SNR frame.

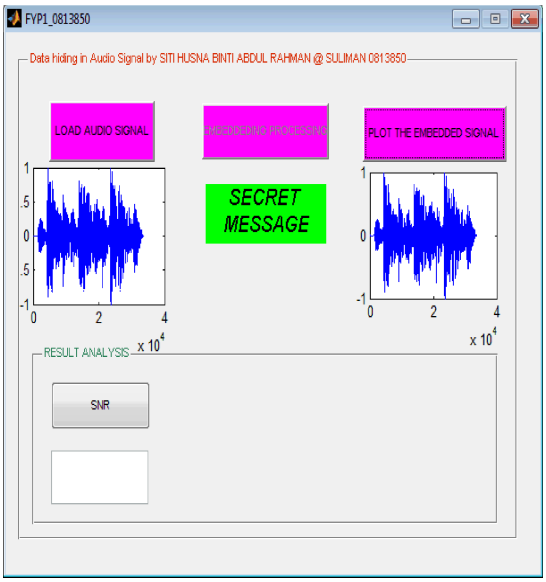

Fig. 4: Screen shot of embedding process

Experimental Result: The proposed LSB audio data hiding method was tested to 10 samples of sound. The SNR value between original audio and embedded audio signal was calculated. The text 'husna' was used to hide in the all sample of sound and each sound has difference size.

From result in table 1, it shows when the size of file is small the SNR value will drop this is an indication that availability space for embedding is not big if more bits are embedded, there could be distortion in the audio signal.

The second experiment was tested with different length of text embedded in the same audio file. The objective of this experiment was to investigate whether the size of secret message will give effect to the SNR value. Sound10 was selected (42.2 kB). The length of the text was increase by factor of 1.

From the result in Table 2, it shows that, there are no changes in SNR value when we increase the length of the text. Only when the size of secret message is larger than the audio signal, the embedding process cannot be performed. Figure 3 shows the shape of embedded signal, original signal and the frame SNR. While Figure 4 shows the GUI screen of shot the embedding process.

CONCLUSION

In this paper the LSB methods have been introduced as a robust method of hiding data in audio signal. The main objective of hiding data in audio signal is to send the secret data in the safe manner. The method does not changed the size of file even after encoding process, thus our method is suitable for hiding any type of audio data and this method can be used for many applications. Further work is to improve the robustness of the algorithm.

REFERENCES

1. Boney, L., A.H. Tewfik and K.N. Hamdy, 1996. Digital watermarks for audio signals. Proceedings of the Third IEEE International Conference on Multimedia Computing and Systems, pp: 473-480, 17-23 June.
2. Petrovic, R., J.M. Winograd, K. Jemili and E. Metois, 1999. Data hiding within audio signals. 4th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services, 1: 88-95.

3. Olanrewaju, R.F., and A.A. Aburas, 2008. Intensive Review on Digital Watermaking. Paper Presented at the International Conference on Science And Technology, Penang, Malaysia.
4. Cvejic, N. and T. Seppanen, 2005. Increasing robustness of LSB audio steganography by reduced distortion LSB coding. Journal of Universal Computer Science, 11(1): 56-65.
5. Cvejic, N. and T. Seppänen, 2008. Digital audio watermarking techniques and technologies: applications and benchmarks: Information Science Publishing.
6. Ansari, R., H. Malik and A. Khokhar, 2004. Data-hiding in audio using frequency-selective phase alteration.
7. Embedded, T., 1996. Information hiding terminology. precedding of the First International Workshop, Cambridge, U.K., May 30 ed by Ross Anderson.
8. Bandyopadhyay, S.K., D. Bhattacharyya, D. Ganguly, S. Mukherjee and P. Das, 2008. A tutorial review on steganography
9. Johnston, J. and K. Brandenburg, 1992. Wideband coding-Perceptual considerations for speech and music: New York: Dekker, pp: 109-140.
10. Cao, W., Y. Yan and S. Li, 2009. Bit Replacement Audio Watermarking Using Stereo Signals. International Conference on New Trends in Information and Service Science, NISS '09, pp: 603-606, June 30 2009-July 2.
11. Bender, W., D. Gruhl, N. Morimoto and A. Lu, 1996. Techniques for data hiding. IBM systems journal, 35(3.4): 313-336.
12. Meghanathan, N. and L. Nayak, 2010. A review of the audio and video steganalysis algorithms. Proceedings of the 48th Annual Southeast Regional Conference.
13. Chen, X.M., G. Doërr, M. Arnold and P.G. Baum, 2011. Efficient coherent phase quantization for audio watermarking. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp: 1844-1847, 22-27 May.
14. Dong, X., M.F. Bocko and Z. Ignjatovic, 2004. Data hiding via phase manipulation of audio signals.
15. Dutta, P., D. Bhattacharyya and T. Kim, 2009. Data Hiding in Audio Signal: A Review. International Journal of Database Theory and Application, 2(2): 1-8.