Data Hiding in Audio Wave File

Asst. Inst. Muna M. Lafta*

Date of Acceptance 4/6/2008

Abstract

Perceptual audio coding has become a customary technology for storage and transmission of audio signals. Watermarking enables the robust and imperceptible transmission of data within audio signals, thus allowing to attach valuable information to the content, such as song title, name of the composer and artist or property rights related data [1].

This paper presents improved LSB (least significant bits) algorithm for embedding a watermark of text type in wave audio file. From Experimental results in this paper conclude that the improved algorithm gives the robust by repeating the watermark on the cover file and gives imperceptible for lessener so there is no noticeable difference between the original and watermarked file, testing to check that there is no noticeable difference between original and watermarked wave file depending on the watermark bit error rate measurements.

1 –Introduction

Today, watermarking is a well-known technology for attaching property rights information or additional valuable data for the customer to audio material [2]. Currently, there are a number of systems available to transmit a watermark in a hidden channel within uncompressed audio signals. However, music distribution over the Internet becomes a more and more important business and, therefore, Embedding a watermark in the PCM domain and encoding afterwards is a common way [3]. This paper presents a method for inserting a watermarking of type text in audio wave file by using improved LSB, audio wave file is an audio file format that was developed by Microsoft. The Wave file format stores information about the file's number of tracks (mono or stereo), sample rate, bit depth, as well as the uncompressed raw audio data.

2-Data Hiding in Audio

Audio files can also be used to hide information. With programs such as Napster, steganography is often used to copyright audio files to protect the rights of music artists. Techniques such as least significant bit insertion, phase coding, spread spectrum coding, and echo hiding can be used to protect the content of

* Baghdad University - College of Education for Women - Computer Science Department.

audio files. The biggest challenge all these methods face is the sensitivity of the human auditory system or HAS. Because the HAS is so sensitive, people can often pick up randomly added noise making it hard to successfully hide data within audio files [4].

Data hiding in the least significant bits (LSBs) of audio samples in the time domain is one of the common algorithms with very high data rate of additional information. 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. Extraction process simply retrieves the watermark by reading the value of these bits from the audio stego object. Therefore, the decoder needs all the samples of the stego audio that were used during the embedding process. The random selection of the samples used for embedding introduces low power additive white Gaussian noise (AWGN). It is well known from the psychoacoustics literature that the human auditory system (HAS) is highly sensitive to AWGN [5]. That fact limits the number of LSBs that can be imperceptibly modified during watermark embedding. The main advantage of the LSB coding method is a very high watermark channel bit rate; use of only one LSB of the host audio sample gives capacity of 44.1 kbps (sampling rate 44 kHz, all samples used for data hiding) and a low computational complexity. The obvious disadvantage is considerably low robustness, due to fact that simple random changes of the LSBs destroy the coded watermark. In this paper improved LSB techniques used to reduce noise and increase the robustness by repeated the watermark more than one and decrease or increase the host byte depending on the bit stream of the watermark text[5].

3- Watermarking in Audio

The basic idea of watermarking is to provide a hidden channel that can be used in existing distribution channels. This channel offers the possibility to transmit user to transmit specific data. Various schemes are available for embedding a watermark into some audio material, such as echo hiding, direct modification of the time domain signal, narrow band systems and the group of systems based on the spread spectrum technology [6]. The following terms are commonly used to classify and/or to describe the properties of the different watermarking schemes:

- Inaudibility: In most cases inaudibility, i.e. perceptual transparency of the watermark signal is considered to be the most important issue in audio watermarking. In other words, the noise introduced by the watermark should not alter the audio quality noticeably. However, the maximum allowed disturbance should always relate to the target sound quality. If the target sound quality is very low an adequate watermark does not need to fulfull absolute inaudibility, while in application areas with very high target sound quality inaudibility must be ensured[7,8].
- Robustness: Often, the robustness of the watermark signal is also a very demanding aspect. It refers to the idea that the unintentional or intentional attempt to remove the watermark should only lead to

success by accepting a clear degradation of the audio quality.

- Data Rate: The data rate specifies the number of bits per second that can be transmitted by the watermarking system. It depends on the underlying technology and the choice of parameters of the watermark scheme. Watermark systems using the spread spectrum technology typically offer bit rates between a few to a few hundred bits/s[7,8].
- Operation Domain: Both the input signal and the output signal of the watermark embedder can either be uncompressed or compressed. Accordingly, the term PCM watermarking is used to describe a system expecting and producing an uncompressed audio signal.
- Complexity: Both, the maximum tolerated complexity of the watermark embedding process and the complexity of the extracting process depend on the application. This is due to the fact that various trade-offs exist between the watermark system complexity and other system properties, e.g. “complexity vs. audibility" in the watermark embedder or “complexity vs. reliability" in the watermark extractor.
- Blind vs. Non-Blind Watermark Detection: Most of the watermarking systems are currently capable of extracting the watermark without knowledge of the unwatermarked original signal. This is called blind, public or oblivious watermarking. However, the extraction performance can be greatly enhanced if the original audio signal is available since in this case the disturbing cover signal for the extraction can be eliminated [7,8].

4- Proposed Improved LSB

In this section a method for hiding secret text into audio media was proposed, this method implemented into direct time domain, the cover audio signal considered a file of wave type as described above insertion of LSB most common steganography method so, for increasing immunity to some modifications the third bit in specific host type of audio cover can be used to hide secret information, the specific host byte calculated depending on the displacement equation explained in algorithm below, the host byte found on the right position calculated by displacement, naturally the noise level of stego cover increase ,therefore, to reduce this error or noise, the first or second bit of the cover will increased or decreased according to the secret bit , if the secret changes the host bit to one, the first and second bits of the cover will be decreased and vice versa. After hiding bits complete, the same process will repeat to improve the robustness of watermarking.

Proposed Hide algorithm

- Input the audio wave file as a cover and convert it into a sequence of bytes.
- Extract wave file size from header.
- Input the secret text and convert it into a sequence of bits.
- Calculate displacement=Wave file size/ (message/secret text size).
- Hide each bit of the sequence of text watermarking in the third bit of each host byte that placed on the right channel byte calculated by displacement.
- Move forward by displacement.
- Repeat the above process until the end of secret text.

Proposed Unhide algorithm

- Extract wave file size from header and secret text size.
- Calculate displacement=Wave file size/ (message/secret text size).
- Extract secret text from the third bit of each host byte which placed on the right channel byte calculated by displacement.
- Move forward by displacement.
- Do the above until the end of file.

5- Results And Test

5-1 Experimental Tests and Results

In this paper, we only focus on the experimental results regarding to sound distortion caused by adding watermark.

Our test use 5 different audio clips, they are all of wave type. Table 1 shows the detail information of all clips. They are (light music, classical and segment of symphony), we try to use short clips because it is always difficult for testers to memorize longer clips and then compare the audio clips between the original and watermarked versions.

Our tests involve 8 people with different music and technical background. Table 2 shows the testing results on improved LSB watermarking, each entry in the table indicates, out of 8 testers, the number of testers who notice difference between the original and the watermarked audio clips.

5-2 Watermark Bit Error Rate Measurement

This section presents the results of the watermark bit error rate (WBER) measurements. The watermarked bit error rate is defined as the ratio of erroneous extracted watermark bits and the overall number of watermark bits. For this purpose a fixed watermark sequence is embedded into the test items. During the extraction process the retrieved watermark bits are compared

with the known sequence on a bit-by-bit basis and the number of unequal bit is measured.

The resulting watermark bit error rates (0.00125) are low enough for a multitude of applications.

Table1: Basic characteristics of tested audio clips.

Audio clip	Type	Sampling Frequency	Frame Size (byte)	Bit Rate
Ringin	Wav	11KHz	9.79KB	88kbps
Chims	Wav	22KHz	54KB	705kbps
Tatles	Wav	16KHz	824KB	128kbps
Alsndmgr	Wav	44KHz	137KB	705kbps
Tada	Wav	22KHz	167KB	705kbps

Table2: Testing result on improved LSB. Each entry in the table indicates out of 8 testers, the number of testers who notice difference between the original and the watermarked audio clips, "-" indicate no one of entry discover the difference

Audioclip name	Improved LSB
Ringin	1
Chims	1
Tatles	-
Alsndmgr	-
Tada	-

7-Conclusions

From the result of the proposed system, one can deduce the following:

1. The amount of data which can be embedded as watermark is very limited and depends on the content of the audio stream, because the human ear is more sensitive to audio distortion than human eye to image distortion.
2. The amount of data, which can be embedded without significant distortion, depends on the contents and the natures of the testing audio clips.
3. There is no noticeable difference between the original and the watermarked file

References

[1] Chansheng X.. , Wu Jiankang W. , Sun Quibin S. , and Kai X. , "**Applications of digital watermarking technology in audio signals"**. Journal of Audio Engineering, Sociecty, vol.47, pp805-812, Oct., 1999.

[2] Katzenbeisser, S., Fabien A.P.," **Information Hiding: Techniques for Steganography and Digital Watermarking",** Artech House, Inc., Norwood, MA, 2000.

[3] Xu C. , Sun Q. , " **A robust digital audio watermarking techniques**", proceeding of the fifth international symposium on signal processing and its applications, Vol.1, PP 91-94, Australia, Aug,1999.

[4] Swanson M. , Zhu B. ,Tewfik A. , " **Current state of the art-challenges and future directions for audio**

watermarking", proceeding of the international conference on on multimedia computing and systems, Vol.11, pp 19-24, Florence,Italy,June,1999.

[5] Lee,L., " **Method and apparatus for transporting, auxiliary data in audio signals"**. International Application Published under the Patent, Cooperation Treaty, Mar. 1997.

[6] Boney,L., Ahmed H. Tew, k., and Khaled N.H. "**Digital watermarks for audio signals"**. IEEE Int. Conf. on Multimedia Computing, and Systems, PP 473-480, Hiroshima, Japan, 1996.

[7] Ricardo A. G**. , "Digital watermarking of audio signals using a psychoacoustic auditory model and spread spectrum theory"**. In 107th AES Convention, New York, Sep. 1999.

[8] Brandenburg k., and Bosi M.," **Overview of MPEG Audio: Current and Future Standards for Low-Bit-Rate Audio Coding**". J. Audio Eng. Soc., PP 4-21, 1997.

اخفاء البيانات في الملف الصوتي من نوع موجة (wave)

م.م.منى مجيد لفتة
جامعة بغداد/ كلية التربية للبنات/ قسم علوم الحاسبات

الخلاصة:

تعتبر عملية تشفير البيانات الصوتية من التكنولوجيا المألوفة لخزن ونقل الاشارات الصوتية. العلامة المائية تعطي القوة في عدم التحسس بوجود البيانات المنقولة بواسطة الاشارات الصوتية وهكذا تسمح بالحاق المعلومات القيمة بالمحتوى مثل اسم المؤلف او الفنان او حقوق الطباعة المتعلقة بالبيانات.

قدم هذا البحث خوارزمية محسنة لاخفاء العلامة المائية من نوع نص في ملف صوتي من نوع موجة (wave) وذلك بالتعامل مع المواقع ذات الاهمية الدنيا (least significant bits) ، من النتائج الموضحة في هذا البحث تم التوصل الى ان استخدام الخوارزمية المحسنة تعطينا في القوة لبعض انواع الهجمات من خلال تكرار العلامة المائية على الملف وعدم التحسس بوجود البيانات بحيث ان الفرق يصبح غير محسوس للشخص المستمع . النتائج المستحصلة من التنفيذ موضحة في البحث، الاختبارات لفحص انه ليس هناك فرق بين الملف الاصلي والملف الحاوي على العلامة المائية تم استعراضها اعتمادا على مقياس فحص الخطأ للعلامة المائية .