Data Hiding in Audio Using Matlab Software

Bhuvnesh Kumar Singh (M.Tech.) 1, Alok Kumar Singh (Asstt. Prof.) 2
1Department of Electronics and Communication Engineering, ABES Engg. College
2Department of Electronics and Communication Engineering, ABES Engg. College

Email- bhuvnesh76@gmail.com

ABSTRACT- This paper presents a method of hiding the text message watermark into audio. This hiding technique is called amplitude modification in low bit encoding. The message embedded into higher LSB layers to increase the robustness. The technique is implemented in matlab since it is a language for data analysis and numerical computation. This proposed scheme includes dynamic coding approach for hiding the watermark. In this scheme no audible distortion after message insertion in audio signal.

Key words: Audio watermarking, matlab software, data hiding,

INTRODUCTION

Audio watermarking is a technique to hide the message into an audio to protect from unauthorized sources. If any information is delivered to another place, then to protect this information from illegal copying, it should be watermarked to provide security for information. In militaries, wireless communication which requires secret communication between sender and receiver point. Now a day because the growth of internet growing is very fast, there may be possibility to unauthorized distribution of digital data. As compared to image and video watermarking, audio watermarking methods are not easy due to Human Auditory System (HAS) is more sensitive than Human Visual System (HVS) [1]. Due to low sampling frequency [3], a small amount of noise in HAS system can be detected by ear [4]. It is a very popular research area in digital media data hiding [2]. There are many challenges to data hiding in audio. The watermark does not have any distortion; it should be audible, must be robust to signal processing and not removed by attacks. A digital watermark is invisible information inserted into image, audio or video. This watermark usually carries copyright information of the file. Digital watermarking takes its name from watermarking of paper or money. Digital watermarks are the signals hided into the digital data. These watermarks can be extracted or detected later. Watermarks may be visible or invisible. Digital watermark could also be robust or fragile depending of the requirements of the application. Robustness defines the ability to detect the watermark after some signal processing manipulations are applied. Robust watermarks are those designed to withstand attacks such as content alteration, compression, filtering, analog to digital, digital to analog conversion and cropping. Invisible watermarks: An invisible watermark is a hidden massage which cannot be perceived with human. Special software is used to extract the hidden information to identify the copyright owner. Invisible watermarks are used to mark a digital content (text, images or audio) to prove its authenticity. Visible watermarks: A visible watermark is a visible text or image overlaid on the original signal. Visible watermarks are more robust against transformation.

Time domain (Spatial domain) watermarking: According to this method the watermark is embedded into original audio signal using PN sequence noise generation which is added to audio [5]. This watermarking scheme is easy to implement as compared to transform domain schemes [1]. Least Significant Bit (LSB) technique is easy to implement to embedding watermark. In LSB watermark is embedded into the audio by changing the least significant bits of the audio samples. Watermark can be easily damaged. Its capacity is low.

In phase coding technique the watermark is embedded having phase shift into phase spectrum of audio [6]. This type of technique is more effective because phase shift cannot be audible by ear.

In echo-hiding technique, the watermark is embedded into audio signal by introducing an echo.
Spread-spectrum technique is a technique in which a signal is transmitted on a bandwidth considerably larger than the frequency of the original information. In this technique, the bit of secret information spreads over the audio frequency spectrum [7]. It requires different code for encoding as well as decoding of hidden information [5]. It is more immune to noise. It also has improved BER (Bit Error Rate) [8]. Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum and Chirp Spread Spectrum (CSS) techniques are used in this. CSS technique is most advantageous in terms of power consumption, speed, security and robustness [9]. Patchwork is a data hiding technique developed by Bender et alii and published on IBM Systems Journal, 1996. It is based on a pseudorandom, statistical model. It works by invisibly embedding a specific statistic, with a Gaussian distribution, into the host audio. Two sets of patches, of the audio. Patchwork has an extremely low bit rate. Patchwork is its resistance to cropping.

Transform domain uses several frequency transforms i.e. Fast Frequency Transform (FFT), Discrete Cosine Transforms and Discrete Wavelet Transforms and others. In transform domain watermarking information (watermark) embedded into the coefficients of audio signal. It is more robust against signal processing operations (Low pass filtering, sampling, quantization, compression). Transform domain technique has large capacity for watermark insertion. In contrast of robustness DWT technique is most effective [10]. Compressed domain watermarking a type of lossy or lossless compression in which the amount of data in a recorded waveform is reduced to differing extents for transmission respectively with or without some loss of quality, used in CD and MP3 encoding, Internet radio, and the like. In this technique the watermark is embedded into bit steam of host audio. No coding and decoding is required [11] [12]. The distortion becomes inaudible to ear.

Overview of watermarking system:

![Diagram](image)

Fig: 1. General audio watermarking system

An encoder is used to insert watermark into original signal. The watermark may be any text or PN sequence noise signal.

In decoding process, decoder checks for the presence of a watermark. The extracted watermark is compared with the original watermark.

Audio Watermarking Characteristics:
Data Hiding in Audio Using Matlab Software

- **Robustness**: Robustness defines the ability of hidden information against attacks. Common attacks include A/D conversion, D/A conversion, sampling, quantization, cropping, low pass filtering [20].

- **Capacity**: It measures the amount of watermark information to which the watermark is embedded without distortion.

- **Perceptual Transparency**: This characteristic defines the similarity between original and extracted message during signal processing and attacks.

Designing and Implementation

Step 1: Reads an mp3-encoded audio file. Length of sound: 1281071 samples

![Original audio Signal](image)

Fig: 2. Original audio signal

Step 2: Watermark Insertion:

SNR of original input sound after watermark insertion = 15.956572401889506
Step: 3 Corrupt watermarked signal
SNR of watermarked, corrupted sound = 8.878974600361559

Step: 4 Watermark Detection:
Data Hiding in Audio Using Matlab Software

Fig: 5. Detected watermark

Dynamic source code:

Introduction Window for watermark embedding (Fig: 6)

Fig: 6. Select audio file for watermark insertion (fig: 7)
Fig: 7

Inserted watermark (fig: 8)

Fig: 8
Recover Watermark, select file (fig: 9)
CONCLUSION

Many methods have been proposed for audio watermarking, the robustness of a watermark depends on the technique used, audio and the signal processing operations. The different schemes have advantages and disadvantages. There are two main issues in audio watermarking: First is robustness and other is capacity. The watermarking scheme depends on the type of application. We have presented an overview about different audio watermarking techniques and applications for Audio Watermarking.

REFERENCES


16) HIMEUR Yassine and BOUDRAA Bachir, “Secure and robust audio watermarking system for copyright protection” 24th International Conference on Microelectronics (ICM), 16-20 Dec. 2012, pp. 1-4


