Chapter 20
Audio Watermarking With Reduced Number of Random Samples

Rohit Anand
G. B. Pant Engineering College, India

Gulshan Shrivastava
National Institute of Technology Patna, India

Sachin Gupta
Vivekananda Institute of Professional Studies, India

Sheng-Lung Peng
National Dong Hwa University, Taiwan

Nidhi Sindhwani
Amity School of Engineering and Technology, India

ABSTRACT

Digital signal watermarking is an indiscernible and safe transmission of freehold data through host signal that includes immersing into and extrication from the actual host. Some algorithms have been investigated for the strong and secure embedding and extraction of watermarks within the host audio files but they do not yet yield good results in compression and re-sampling. In this chapter, an excellent method is suggested for the compressed wave files that uses random carrier to immerse the watermark in the sequence of an audio signal. The watermark is embedded lucently in audio stream after adaptive differential pulse code modulation (ADPCM) before quantization. The proposed scheme has been implemented and its parameters are compared with the finest auditory watermarking method known. A tool has been used to measure the parameters to produce the results and tabular values. The larger PSNR and smaller BER prove that the suggested scheme is robust.

DOI: 10.4018/978-1-5225-4100-4.ch020

INTRODUCTION

A drastic number of changes in the world have been because of the evolution of the online networks and the digital content uprising. The different kinds of wideband transmission webworks/ networks and interactive media information present in a binary format (text, pictures, audio, and video) have unlocked so many challenges and possibilities for modernization and novelty. Easy-to-use as well as versatile software and the shrinking prices of the different kinds of digital devices (for example, compact and movable mp3 players and CD players, camcorders, digital scanners, digital cameras, DVD players, CD and DVD recorders, laptops etc.) have created the possibility for the customers from the different regions of the world to design, modify and interchange the different types of data related to multimedia. Different high-speed internet connections and near-accurate transmission of data ease the people to share the heavy kinds of multimedia files and create their homogeneous digital reprints. Digital interactive media files do not undergo any loss of the superiority due to repetitive processes of copying such as analog audio and Video Home System tapes. Further, recording medium and transportation networks for different kinds of analog media are very uneconomical. These benefits of digital means over the analog means may shift to the drawbacks as far as cerebral copyright supervision is concerned because of the likelihood for boundless replication without a loss of precision results in a large economic loss for the holders of possession rights. The effortlessness of the alteration of the matter and exact replication in the digital sphere have encouraged the safekeeping of phrenic possession and the avoidance of illicit dabbling of the different kinds of mixed media data to become a crucial specialized and inspecting issue (Adya, 2007).

A large usage of the audio-visual data along with a speedy transportation of mixed media to the different customers having gadgets with a very good quality of service is growing into a huge challenge. Copy protection systems based on the hardware have now been sidestepped for the analog media. The digital media are very easier to hack because of the possibilities of the different kinds of mixed media processing platforms. Simple protection mechanisms are obsolete now as header information can be easily be eliminated by a simple format of the data that does not affect the correctness of data.

Applying the coding technique to the mixed media avoids ingress to the different mixed media details to a human without a genuine deciphers key. So, detail providers are rewarded for the carriage of recognizable multimedia and each consumer who has paid the royalties should have a proper decipher key so as to unravel the file that has been received. After the decoding of the mixed media file, it can easily be duplicated and dispensed in a repetitive manner with no hurdles. Present-day software and high-speed internet present the aid to accomplish it with very least amount of skills and awareness needed. A very usual example is the hacking of a system based on digital rights management as well as encryption for digital versatile disks. So, existing protocols related to security remain tend to guard the medium of communication between the user and the person who can provide the data for a mixed media. These protocols are totally insignificant if transaction item is digitally designated.

The type of watermarking discussed above can be used to make the digital media safe and secure from the process of tampering. Digital watermarking refers to the embedding of a lucent digital signature (containing a data useful in the applications like broadcast monitoring, anti-tampering etc.) into a host signal. A watermark embedder has one input as watermark message (i.e. a binary sequence along with a secret key) and second input as host signal (like image, audio or video etc.) while the product of a watermark implanter is a very safe watermarked signal that may be broadcasted later to the watermark detector. The function of watermark detector is to find out whether there is any watermark in the multimedia signal and if there is such a watermark, what kind of message is encoded in that. Watermarking is very much