Chapter 6
Audio Watermarking:
State-of-the-Art

Dejan Drajic
Ericsson d.o.o., Serbia

Nedeljko Cvejic
University of Cambridge, UK

ABSTRACT

In this chapter, the authors recapitulate the background and the state-of-the-art of digital audio watermarking, including descriptions of audio watermarking algorithms and malicious attacks against these algorithms. The areas in which audio watermarking has been implemented and the possible future applications are outlined. The three requirements of the “magic triangle” in audio watermarking are described as well, with characterized by a number of defining properties, including robustness, watermark bit rate and perceptual transparency. The chapter also provides a comprehensive list of attacks used by adversaries to interfere with the embedded watermark and to prevent its detection.

1. INTRODUCTION

Although the number of published articles on watermarking and information hiding increased sharply from 1992, the watermarking algorithms were primarily developed for digital images and video sequences (Bender, Gruhl, Morimoto, & Lu, 1996; Cox, & Miller, 2001), whereas the interest and research in audio watermarking started later (Hartung, & Kutter, 1999; Swanson, Zhu, & Tewfik, 1999). In the past few years, several algorithms for embedding and extraction of watermarks in audio sequences have been published. It is clear that audio watermarking initially started as a sub-discipline of digital signal processing, focusing mainly on convenient signal processing techniques to embed additional information to audio sequences. This included the investigation of suitable transform domain for watermark embedding and schemes for imperceptible modification of the host audio. Digital watermarking has only recently been provided with a stronger theoretical foundation, becoming a more mature discipline, with a proper foundation in both communication modelling and information theory.

Section 2 presents application areas for the audio watermarking algorithms and in Section 3
the three most important requirements in audio watermarking are highlighted (Arnold, Wolthusen, & Schmucker, 2003). For example, amount of data that can be embedded transparently into an audio sequence is considerably lower than the amount that can be hidden in images as audio signal has a dimension less than two-dimensional image files.

When the perceptual transparency requirement has been fulfilled, design objective is to increase robustness and achieve a practical watermark bit rate. Section 4 gives a general framework of the audio watermark systems performance in the presence of attacks. Many attacks that are malicious against image watermarking algorithms (e.g., geometrical distortions, spatial scaling etc.) cannot be implemented against audio watermarking schemes, whereas some of the signal modifications are specific for audio watermarking, such as time desynchronisation and echo addition.

A literature survey of audio watermarking algorithms that form the mainstream research is presented in Section 5. The algorithms are categorized by the statistical method used for detection and extraction of watermark bits, with references to specific algorithms using different signal domains for watermark embedding. Section 6 gives an overview of the publications describing for the latest developments in the area of audio watermarking.

2. AUDIO WATERMARKING APPLICATIONS

2.1 Ownership Protection

In the ownership protection applications, a watermark containing ownership information is embedded to the multimedia host signal. The watermark, known only to the copyright holder, is expected to be very robust and secure (i.e., to survive common signal processing modifications and intentional attacks), enabling the owner to demonstrate the presence of this watermark in case of dispute to demonstrate his ownership. Watermark detection must have a very small false alarm probability. On the other hand, ownership protection applications require a small embedding data rate of the system, because the number of embedded bits that can be subsequently extracted does not have to be large, as long as the watermark robustness is preserved.

2.2 Authentication and Tampering Detection

In the content authentication applications, a set of secondary data is embedded in the host multimedia signal and is later used to determine whether the host signal was tampered. The robustness against removing the watermark or making it undetectable is not a concern as there is no such motivation from attacker’s point of view. However, forging a valid authentication watermark in an unauthorized or tampered host signal must be prevented. In practical applications it is also desirable to locate (in time or spatial dimension) and to discriminate the unintentional modifications (e.g. distortions incurred due to moderate MPEG compression (Noll, 1993; Wu, 2004)) from content tampering itself. In general, the watermark embedding capacity has to be high to satisfy the need for more additional data than in ownership protection applications. The detection must be performed without the original host signal because either the original is unavailable or its integrity has yet to be established. This kind of watermark detection is usually called a blind detection.

2.3 Proof of Ownership

It is even more demanding to use watermarks not only in the identification of the copyright ownership, but as an actual proof of ownership. The problem arises when adversary uses editing software to replace the original copyright notice with his own one and then claims to own the copyright himself. In the case of early watermark systems,
Related Content

Object-of-Interest Retrieval in Social Media Image Databases for e-Crime Forum Detection
www.igi-global.com/article/object-of-interest-retrieval-in-social-media-image-databases-for-e-crime-forum-detection/132686?camid=4v1a

Future Directions of Multimedia Technologies in E-Learning
www.igi-global.com/chapter/future-directions-multimedia-technologies-learning/27183?camid=4v1a

Evaluating Learning Management Systems: Leveraging Learned Experiences from Interactive Multimedia
www.igi-global.com/chapter/evaluating-learning-management-systems/27073?camid=4v1a

Correlation-Based Ranking for Large-Scale Video Concept Retrieval
www.igi-global.com/article/correlation-based-ranking-large-scale/49150?camid=4v1a