PCM Encoding and a Spread Spectrum Modulation in the Watermarking System

W. Barkouti, S. Oueslati and A. Cherif
Department of Physics, Faculty of science, Manar University, Tunis, Tunisia.

Abstract-In the recent years, a huge amount of digital information is circuiting through all over the world by means of the World-Wide Web. Most of this data is exposed and can be easily forged or corrupted. Digital watermarking has been proposed as one of the possible ways to deal with this problem, to keep information safe. We propose to study in this paper the PCM coding technique and the contribution of different spread spectrum modulation on the performance of a watermarking system.

Keywords- PCM, Digital watermarking, modulation.

I. INTRODUCTION

The watermarking of digital data has become very popular approach for intellectual property rights protection. Several watermarking techniques were developed and a large amount of methods were proposed, but still the most of known ways to protect data are far from ideal. The digital data of the various types such as text, images, audio, and video can be processed by the watermarking procedure. In general, all types of data watermarking techniques have similar simple ideas – to hide a set of owner’s data within the materials, which should published, with the purpose to be able to prove his ownership. The requirements for watermarked data quality and safety for all types are also the same. Watermark should be imperceptible for unauthorized user, should not affect an original data quality and should be robust against various types of attacks [1].

Audio watermarking is concerned with the insertion of a signal of known information or characteristics in an audio signal in an imperceptible way. Detection of the embedded watermark helps in authenticating the audio, identifying illegal copies of the audio, and detecting unauthorized changes made to the audio. While data embedding in an audio signal, or audio steganography, resembles audio watermarking in many ways, the former has applications in covert and/or secure communication of battlefield information, confidential financial transactions, etc., requiring a large payload capacity. Watermarking, on the other hand, is primarily used for copyright protection of digital products that require embedding a small amount of information [2].

To be effective in the general application of copyright protection, a watermarking technique must satisfy three major criteria, namely, the watermarked audio is perceptually indistinguishable from the original audio, the watermark is robust so that a user is unable to extract the watermark without destroying the audio, and the watermark is unambiguously retrieved by the copyright owner to establish ownership. These requirements, which are also common to data embedding and steganography, cannot all be met simultaneously for any practical application. Because of this challenge, a large body of work has been reported over the past decade with varying degrees of success for steganography and watermarking applications [2].

In this paper, we discuss two techniques for inserting a speech signal in a musical signal, the first is the PCM coding technique and the second is based on spread spectrum modulation.

II. AUDIO WATERMARKING FOR COPYRIGHT PROTECTION

The watermark embedded in the audio media must be imperceptible, robust against attacks and self-secured. Moreover, capacity of embedding and speed of watermarking are also worthy of notice. In addition to these main requirements, the watermark also should be spread throughout the entire host audio [3].

The most significant requirements are perceptibility, reliability, capacity and speed performance.

Perceptibility
The most important requirement is that the quality of the original signal has to be retained after the introduction of watermark. A watermark cannot be detected by listeners [4].

Security
Since copyright protection is the main application for watermarking, security is an issue of high priority. The removal or modification of the watermark has to be prohibited or only made possible at the cost of severe degradation of the host signal[5]. Security is usually related with the ability of a data hiding scheme to protect some secret parameter, so that an attacker can not use it to access the watermark contents[6].

Capacity
The amount of information that can be embedded into a signal is also an important issue. A user has to be able to change the amount embedded to suit different applications. An example can be seen in real-time application. If a watermark is spread across an audio signal, the complete signal has to be presented first. This is not possible in streaming over the Internet [4].

Speed
Speed is important in practical; for real-time and low-delay processing is hot currently. The complexity of each watermarking scheme determines the speed. The watermark

Reference Number: WI1-0061
embedding and extracting processes have to be fast enough to suit these applications.

III. AUDIO WATERMARKING SEEN AS A DIGITAL COMMUNICATION

The process of watermarking is viewed as a transmission channel through which the watermark message is being sent, with the host signal being a part of that channel. In Figure 1, a general mapping of a watermarking system into a communications model is given. After the watermark is embedded, the watermarked work is usually distorted after watermark attacks. The distortions of the watermarked signal are, similarly to the data communications model, modeled as additive noise [7].

![Watermarking system](image)

Figure (1): Watermarking system

Watermarking in an audio signal can be seen as a means of transmitting a sequence of bits (“1”s and “0”s) through a very particular noisy communication channel, whose “noise” contribution is the audio signal (host signal) itself. With this view in mind, creating an audio watermarking system amounts to designing an emitter and a receiver adapted to the specificities of the channel; the emitter has to insert the watermark in the audio signal in such a way that the watermark cannot be heard, and the receiver must extract this hidden information from the watermarked audio signal.

The problem therefore looks very similar to that of sending information bits through the Internet; one has to maximize the bit rate while minimizing the bit error rate, even in the presence of communication noise and distortion. However, watermarking techniques are very specific in terms of bit rate, error rate, and signal-to-noise ratio. SNR is typically made very low so as to make the watermark inaudible.

IV. PULSE CODE MODULATION

Since the introduction of the Compact Disc (CD) in 1982, Pulse Code Modulation (PCM) has been the dominant technique for digital music recording. In essence, PCM involves sampling the analog signal (conforming to the Nyquist criteria) and coding the signal into a finite sequence of numbers. Therefore, the quality of the output signal depends on the sampling frequency, $sF$ and the number of bits or quantization levels. For digital audio, signal levels are represented by binary numbers [8].

An analog signal is sampled at regular time intervals. An amplitude measurement that could take on an infinite number of values exists at regularly spaced sample times; the sampling time is fixed. The next step is to approximate each amplitude by selecting the nearest of two digital approximations according to the $2^n$ levels available, with $n$ being the number of bits chosen in the system (for example, $n=16$ for compact disc storage). The amplitude is said to be “quantized”, and the audio signal will now contain what is called “quantization noise” – noise added to the signal due to the process of quantizing the amplitude at each sample position. The final step in PCM conversion is to convert the quantized amplitude into a binary format using only 1’s and 0’s to transmit the information [9].

V. APPLICATION OF PCM ON WATERMARKING SYSTEMS

This is a digital representation of an analog signal where the height of the signal is sampled regularly at uniform intervals of duration $T$. Each sample was quantified on a series of symbols in a digital code, which is usually a binary code.

The PCM is used in digital telephone systems. This is also the standard format for digital audio as wav sounds and words. Figures (2) and (3) show the original signal and the coded signal to PCM.

![Original signal](image)

Figure (2): Original signal

![PCM coding of the transmitted signal](image)

Figure (3): PCM coding of the transmitted signal
Converting the speech signal in binary is given by the following figure.

![Figure 4: converting the speech signal into binary](image)

The speech signal is converted in binary from 16 bits per sample, and sampling frequencies of 44.1 KHz.

VI. SPREAD SPECTRUM MODULATION

Spread spectrum was originally developed for military use (radar and communications) in several countries. Since its declassification, it has found civilian application, particularly in code-division multiple-access (CDMA) communications, the system used for cellular telephony.

In spread spectrum, a narrowband signal (the message to be transmitted) is modulated by a broadband carrier signal, which broadens (spreads) the original, narrowband spectrum; hence the term "spread spectrum".

Rather than embedding watermark in narrow bands of the host signal, it is more difficult to intercept and remove the watermark carried in spread spectrum watermarking scheme. In a spread spectrum scheme, the watermark message is first shaped according to psychoacoustic model and then modulated by a pseudorandom sequence called the key.

Some spreading sequence (also called spreading code or pseudo-noise) is used to create the wide-band spread spectrum signal from the information bits to send. This code must be shared by the emitter and the receiver, which makes spread spectrum signals hard to intercept. In the 1990s, spread spectrum techniques have found a major application in code division multiple accesses (CDMA), now used in satellite positioning systems (GPS), and for wireless digital phone communications systems. Spread spectrum techniques also make it possible to hide information in communication noise.

The audio signal \( x(n) \), sampled at \( F_s \) Hz, is added to a spread spectrum watermark signal \( v(n) \) obtained bymodulating a watermark sequence of \( M \) bits \( b_m \) (in \{0,1\}) with a spreading signal \( d(n) \) composed of \( N_b \) samples (and shown in figure (5), as a vector \( d = (d(0), d(1), \ldots, d(N_b - 1)) \)).

![Figure 5: Emitter](image)

Vector \( \mathbf{d} \) is synthesized by a pseudo-random sequence generator as a Walsh–Hadamard sequence or a Gold sequence with values in \([-1, +1]\).

The spread spectrum signal \( v(n) \) is given by

\[
v(n) = \sum_{m=0}^{M-1} a_m d(n - mN_b)
\]

(1)

Where \( m \) is a symbol in \([-1, +1]\) given by

\[
a_m = 2b_m - 1
\]

(2)

We can also see this signal as a concatenation of vectors:

\[
v(n) = a_m \mathbf{d} = \begin{cases}
+1 & \text{if } a_m = 1 \\
0 & \text{otherwise}
\end{cases}
\]

(3)

Finally it is amplified by some gain \( g \), which makes it possible to control the signal-to-noise ratio (SNR) between the watermarked signal \( v(n) \) and the audio signal \( x(n) \). Since 1 bit is emitted every \( N_b \) samples, the bit rate is simply given by \( R = F_s - N_b \) (bits/s), where \( F_s \) is the sampling frequency (typically 44.1 kHz). The watermarked signal \( v(n) \) is given by the following figure:

![Figure 6: Modulated signal](image)

VII. CONCLUSION

A new technique for the application of a PCM encoding and a spread spectrum modulation that designed for watermarked system has been presented in this paper. The proposed PCM is designed to convert an analog signal into binary format that draws thereafter to apply the spread spectrum modulation.
REFERENCES


