Wavelet Transform for Denoising Audio Watermarking

W. Barkouti, A. Chabchoub, S. Alahmadi, A. Cherif

***Abstract*—Audio Watermarking is the process of embedding information into a signal in a way that is difficult to remove. If the signal is copied, then the information is also carried in the copy. Audio Watermarking has become increasingly important to enable copyright protection and ownership verification. This paper investigates the use of wavelet transform for denoising audio signals contaminated with noises.**

***Index Terms*— Wavelet transform, watermarking, attacks, de-noising.**

I. INTRODUCTION

With the proliferation of digital media such as images, audio, and video, robust digital watermarking and data hiding techniques are needed for copyright protection, copy control, annotation, and authentication. Based on the fact that noise and distortion are the main factors that limit the capacity of data transmission in telecommunications and that they also affect the accuracy of the results in the signal measurement systems, whereas, modeling and removing noise and distortions are at the core of theoretical and practical considerations in communications and signal processing. Another important issue here is that, noise reduction and distortion removal are major problems in applications such as; cellular mobile communication, speech recognition, image processing, medical signal processing, radar, sonar, and any other application where the desired signals cannot be isolated from noise and distortion[1]. The use of wavelets in the field of de-noising audio signals is relatively new, the use of this technique has been increasing over the past 20 years. One way to think about wavelets matches the way how our eyes perceive the world when they are faced to different distances. In the real world, a forest can be seen from many different perspectives; they are, in fact, different scales of resolution. From the window of an airplane, for instance, the forest cover appears as a solid green roof. From the window of a car, the green roof gets transformed into individual trees, and if we leave the car and approach to the forest, we can gradually see details such as the trees branches and leaves. If we had a magnifying glass, we could see a dew drop on the tip of a leaf. Audio watermarking techniques are still being developed, due to many applications, copyright protection, voice messages authentication, annotation of audio files, etc. [2].

Revised Version Manuscript Received on June 11, 2015.

Wahid Barkouti, Asst. Prof., in the Electronic Engineering Department, College of Technology, Meadinah, KSA.

Abdelkader Chabchoub, Asst. Prof., in the Electronic Engineering Department, College of Technology, Meadinah, KSA.

Salah Alahmadi, Asst. Prof., Faculty of Engineering - Electrical Engineering Department, Islamic University in Madinah, KSA.

Adnen Cherif, Professor, Faculty of Science Tunis FST - Electrical Engineering Department, School of Communications, University of Tunis El Manar Tunisia.

Recent developments in audio watermarking techniques have gone some way towards promoting an industry-wide acceptance of digital audio watermarking as a process that will eventually be used in all audio (and video) production. The predominant focus of such watermarking research has been in the area of content protection, because the prevention of illegal copying is an area of concern for content owners. Audio watermarking is the application on audio signals, a rather new field. Compared with images and video, inserting imperceptible, robust and secure watermark(s) into digital audio files presents special challenge. Since audio signals are represented by much less samples per time interval, the room for embedding is limited [3]. Moreover, the human auditory system (HAS) is much more sensitive than the human visual system (HVS), which means that inaudibility for audio is more difficult to achieve than invisibility for images [4]. Therefore, the advance of audio watermarking is slower than that of image or video watermarking. Specifically, our research is focused on embedding imperceptible, robust and secure watermarks for copyright protection. Different from cryptology for data security, watermarking techniques do not encrypt the host information to restrict the access to approach, but embed one or more watermarks with separately specific meanings into the host carrier [5]. These watermarks are permanent signs, hard to clear up without degrading the quality of the host media. When proprietorial disputes happen, the watermark(s) could be extracted as reliable proofs for assuring the authorship [6].

II. WATERMARKING DESIGN GOALS

Audio watermarking systems are design to meet three goals: maximizing the difficulty of removing the watermark without destroying the audio, minimizing the perceptual effect of the watermark, and maximizing the information which can be encoded per second of original audio. Designing a system that optimizes all of these goals is difficult because, for the most part, each of the goals work against the others. It has been claimed that phase coding is one of the most effective techniques in terms of SNR. Watermark should be also robust against resampling of the audio signal [7]. Watermarking is a technique through which the secure information is carried without degrading the quality of the original signal. The technique consists of two blocks:

(i) Embedding block
(ii) Extraction block

The embedded object is known as watermark, the watermark embedding medium is termed as the original signal or cover object and the modified object is termed as embedded signal or watermarked data [8]. The embedding block, shown in Figure 1consists of watermark, original signal (or cover object), and watermarking key as the inputs (creates the embedded signal or watermarked data) [8]. Whereas, the

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

inputs for the extraction block is embedded object, key and sometimes watermark as illustrated in Figure [8]. The watermarking technique that does not use the watermark during extraction process is termed as „blind watermarking.“ Blind watermarking is superior over other watermarking involving watermark for extraction as watermarked signal and key are sufficient to find the embedded secret information [9].

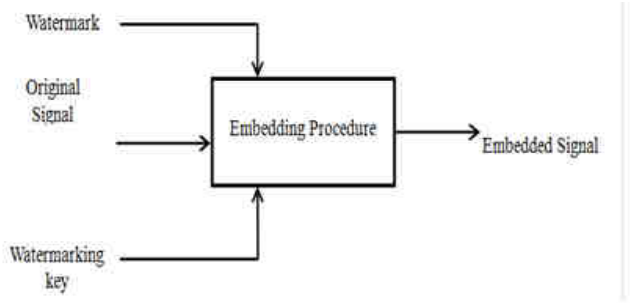

Figure 1. Digital watermarking embedding

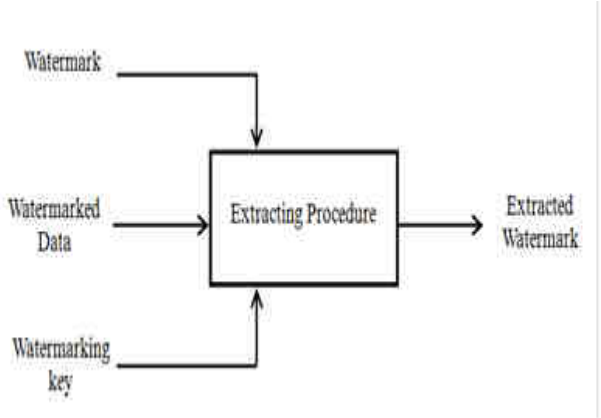

Figure 2. Digital watermarking extraction

III. Applications of Watermarking

A. Ownership protection and proof of ownership:

In ownership protection application, the watermark embedded contains a unique proof of ownership. The embedded information is robust and secure against attacks and can be demonstrated in a case of dispute of ownership. There can be the situations where some other person modifies the embedded watermark and claims that it is his own. In such cases the actual owner can use the watermark to show the actual proof of ownership [10] [11] [12].

B. Authentication and tampering detection:

In this application additional secondary information is embedded in the host signal and can be used to check if the host signal is tampered. This situation is important because it is necessary to know about the tampering caused to the media signal. The tampering is sometime a cause of forging of the watermark which has to be avoided [10] [11] [12].

C. Finger printing:

Additional data embedded by a watermark in the fingerprinting applications are used to trace the originator or recipients of a particular copy of a multimedia file. The usage of an audio file can be recorded by a fingerprinting system. When a file is accessed by a user, a watermark, or called fingerprint in this case, is embedded into the file thus creating a mark on the audio. The usage history can be traced by extracting all the watermarks that were embedded into the file [13].

D. Broadcast monitoring:

Watermarking is used in code identification information for an active broadcast monitoring. No separate broadcast channel is required as the data is embedded in the host signal itself which is one of the main advantages of the technique [12].

E. Copy control and access control:

A watermark detector is usually integrated in a recording or playback system, like in the DVD copy control algorithm [14] or during the development of Secure Digital Music Initiative (SDMI) [13]. The copy control and access control policy detects the watermark and it enforces the operation of particular hardware or software in the recording set [11].

F. Medical applications:

Watermarking can be used to write the unique name of the patient on the X-ray reports or MRI scan reports. This application is important because it is highly advisable to have the patients name entered on reports, and reduces the misplacements of reports which are very important during treatment [12].

G. Airline traffic monitoring:

Watermarking is used in air traffic monitoring. The pilot communicates with a ground monitoring system through voice at a particular frequency. However, it can be easily trapped and attacked, and is one of the causes of miss communication. To avoid such problems, the flight number is embedded into the voice communication between the ground operator and the flight pilot. As the flight numbers are unique the tracking of flights will become more secure and easy [15].

IV. Requirements of the Efficient Watermark Technique

According to IFPI (International Federation of the Phonographic Industry) [12], audio watermarking algorithms should meet certain requirements. The most significant requirements are perceptibility, reliability, capacity, and speed performance [16].

A. Perceptibility:

One of the important features of the watermarking technique is that the watermarked signal should not losethe quality of the original signal. The signal to noise ratio (SNR) of the watermarked signal to theoriginal signal should be maintained greater than 20dB [12]. In addition, the technique should make the modified signal not perceivable by human ear.

B. Reliability:

Reliability covers the features like the robustness of the signal against the malicious attacks and signal processing techniques. The watermark should be made in a way that they provide high robustness against attacks. In addition, the watermark detection rate should be high under any types of attacks in the situations of proving ownership. Some of the other attacks summarized by Secure Digital Music Initiative (SDMI), an online forum for digital music copyright protection, are digital-to-analog and analog-to-digital conversions, noise addition, band-pass filtering, time-scale modification, echo

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

addition, and sample rate conversion [17].

C. Capacity:

The efficient watermarking technique should be able to carry more information but should not degrade the quality of the audio signal. It is also important to know if the watermark is completely distributed over the host signal because, it is possible that near the extraction process a part of the signal is only available. Hence, capacity is also a primary concern in the real time situations [12].

D. Speed:

Speed of embedding is one of the criteria for efficient watermarking technique. The speed of embedding of watermark is important in real time applications where the embedding is done on continuous signals such as, speech of an official or conversation between airplane pilot and ground control staff. Some of the possible applications where speed is a constraint are audio streaming and airline traffic monitoring. Both embedding and extraction process need to be made as fast as possible with greater efficiency [12].

V. Problems and Attacks on Audio Watermarking

There is a trade-off between these two requirements; however, by testing the algorithm with the signal processing attacks that gap can be made minimal. Every application has its specific requirements, and provides an option to choose high robustness compensating with the quality of the signal. By performing perceptibility and robustness evaluations on each basic scheme, we find out their merits and demerits of withstanding some typical attacks. It is useful for preparing to develop an extra robust audio watermarking system for copyright protection.

A. Dynamics:

The amplitude modification and attenuation provide the dynamics of the attacks. Limiting, expansion and compressions are some sort of more complicated applications which are the non-linear modifications. Some of these types of attacks are re-quantization [18].

B. Filtering:

Filtering is common practice, which is used to amplify or attenuate some part of the signal. The basic low pass and high pass filters can be used to achieve these types of attacks.

C. Noise:

It is common practice to notice the presence of noise in a signal when transmitted. Hence, watermarking algorithm should make the technique robust against the noise attacks. It is recommended to check the algorithm for this type of noise by adding the host signal by an additive white Gaussian noise (AWGN) to check its robustness.

D. Time stretch and pitch shift:

These attacks change either the length of the signal without changing its pitch and vice versa. These are some de-synchronization attacks which are quite common in the data transmission.

VI. Experimental Results

We performed extensive experiments in order to test the imperceptibility and robustness characteristics of the proposed audio watermarking method. The compromises between audibility of watermarking artifacts and robustness requirements have been discussed in several papers [19, 20]. In the experiments we used audio signal sampled at 44.100 kHz rate. These signals are segmented into 11.5 ms frames, which are weighted with a hamming window, with 50% overlap between segments.

A. Embedding

The basic idea of the embedding method on time-frequency. In particulars, for every segment to be watermarked, the corresponding inaudible watermark signal is constructed in frequency domain and added to the host after transforming back to time domain.

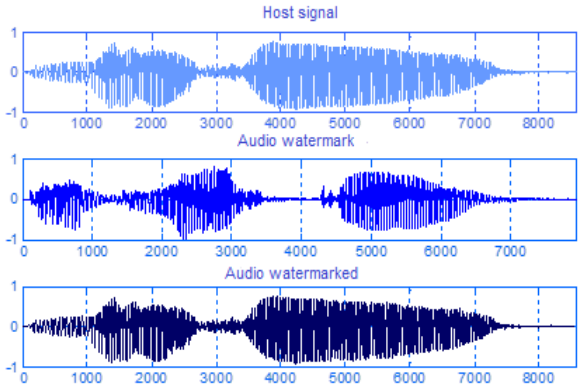

Figure 3. Embedding Audio watermark

Once the watermark is inserted, we make tests to avoid any audible distortion. If the quality of the host signal is modified after the dissimulation of the signature this has no explanation that the watermark is not well inserted. In our case, the results are perfected and distorted them are non-existent, thus we are going to move on to the next stage which is the disturbances met at the level of the channel.

B. Attacks

At the level of the channel, the watermarked signal can undergo damages (can be masked by the noise of the channel). For that reason and if our system is strong, the detection of the inserted mark (brand) will be completed. Indeed, having to insert our signature, we are going to add to watermarked signal a Gaussian white noise to SNR "signal to noise rate" variable. From point of view implementation, we make generate a random (unpredictable) noise of which the SNR is equal in 6db.

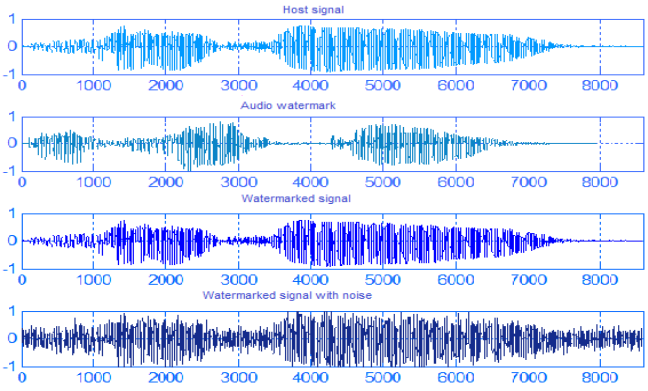

Figure 4. Audio watermark with noise

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

C. *Extraction*

Really the audio watermarked signal can have disturbances at the level of the channel.

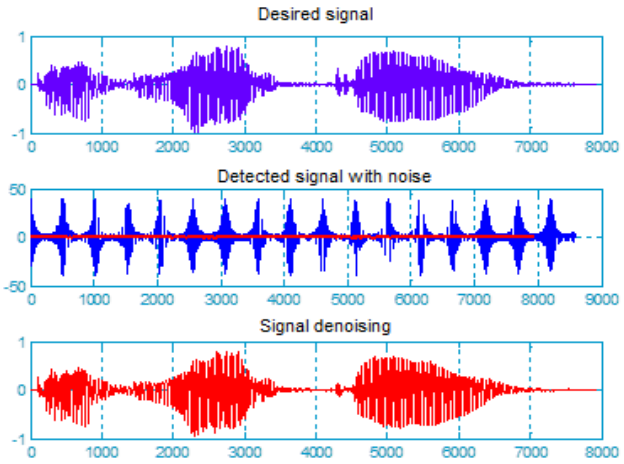

Figure 5. Denoising audio watermarked

At the level of detection, we can conclude that watermarked signal and the signal detected later denoising are identical, thus the detection is completed. It is verified that the WT technique is robust for most of the attacks.

VII. Conclusion

The proposed digital watermarking method for audio signals is based on a WT technique. The method retains the perceptual quality of the audio signal, while being resistant to diverse removal attacks. The digital watermarking is robust to malicious attacks, it is hard to detect and remove by an unauthorized person. It must be noted, that its robustness is confirmed on a rather small number of signal and further testing should be effectuated. Our watermarking system is imperceptible and resists attacks

Acknowledgments

I would like to express my gratitude and appreciation to all those who gave me the possibility to complete this paper. I would also like to acknowledge with much appreciation the crucial role of my parents.

References

[1] Abbate A, Decusatis C. M, Das P. K. “Wavelets and subbands: fundamentals and applications,” ISBN 0-8176-4136-X, Birkhauser, Boston, USA,2002.
[2] Przemysław Dymarski and Robert Markiewicz Robust Audio Watermarks in Frequency Domain 'journal of telecommunications and information technology,2014,2,pp 12-21.
[3] F. Hartung, M. Kutter, “Multimedia Watermarking Techniques”, in Proceedings of the IEEE, vol. 87, no.7, pp. 1079-1107, Jul. 1999.
[4] C.S. Xu, D.D. F, “Robust and Efficient Content-based Digital Audio Watermarking”, Multimedia Systems,vol. 8, pp. 353-368, 2002.
[5] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, “Techniques for Data Hiding,” IBM Systems Journal, vol.35, no. 3&4, pp. 313-336, 1996.
[6] Editors: B. Furht, D. Kirovski, Multimedia Watermaking Techniques and Applications, Auerbach Publications, Boca Raton, Fla., 2006.
[7] S. Xiang, “Audio watermarking robust against D/A and A/D conversions”,EURASIP J. Adv. Signal Proces., vol. 2011:3, 2011.
[8] M. Navneet Kumar, “Watermarking Using Decimal Sequences,” M.S. thesis, Louisiana State University, Baton Rouge, LA, USA, 2004.
[9] V. K. Bhat, I. Sengupta, and A. Das, “Audio Watermarking Based on Quantization in Wavelet Domain,” ICISS 2008, LNCS 5352, pp. 235 -242, 2008.
[10] S. Katzenbeisser, and F.A.P. Petitcolas, Information hiding techniques for steganography and digital watermarking, Artech House Publishers, 2000.
[11] C. Nedeljko , “Algorithms For Audio Watermarking And Steganography”, Academic Dissertation, University of Oulu, public discussion in Kuusamonsali (Auditorium YB210), Linnanmaa, Finland, 2004.
[12] Katzenbeisser, and F. A. P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Inc. 2000.
[13] S.A. Craver, B. Liu, and M. Wu, “What can we reasonably expect from watermarks? Applications of Signal Processing to Audio and Acoustics.” IEEE Workshop on 10/21/2001 -10/24/2001, pp. 223-226, 2001.
[14] J. Bloom, I. Cox, T. Kalker, J. Linnartz, M. Miller, and C. Traw. “Copy protection for DVD video,” Proceedings of the IEEE, vo. 7, Issue 87, pp. 1267- 1276, 1999.
[15] K. Hofbauer, and H. Hering, “Noise Robust Speech Watermarking with Bit Synchronisation for the Aeronautical Radio,” LNCS 4567, Springger-Verlag Berlin Heidelberg, pp. 252-266, 2007.
[16] F.A.P Petitcolas. “Watermarking schemes evaluation,” IEEE Signal Processing Magazine [Online], Volume 17, Issue 5, pp.58-64, 2000.
[17] SDMI. Call for Proposals for Phase II Screening Technology Version 1.0, 2000. [Online]. Available: http://www.sdmi.org/download/FRWG00033102-AMD1.htm [Accessed July 15. 2010].
[18] V. K. Bhat, I. Sengupta, and A. Das, “Audio Watermarking Based on Quantization in Wavelet Domain,” ICISS 2008, LNCS 5352, pp. 235 -242, 2008.
[19] X. Wang, and H. Zhao, “A Blind Audio Watermarking Robust Against Synchronization Attacks,” CIS 2005, Part II, LNAI 3802, pp. 617-622, 2005.
[20] E. Zwicker, and H. Fastl , Psychoacoustics. Springer Verlag, Berlin, Germany, 1999.

Wahid Barkouti is currently working as a Assistant Professor in the Electronic Engineering Department, college of technology Meadinah KSA, Researcher at Laboratory Innov'COM @ Sup'Com , School of Communications, University of Tunis El Manar Tunisia

Abdelkader Chabchoub is currently working as a Assistant Professor in the Electronic Engineering Department, college of technology Meadinah KSA, Researcher at Laboratory Innov'COM @ Sup'Com , School of Communications, University of Tunis El Manar Tunisia**.**

Salah Alahmadi is currently working as a Assistant Professor Faculty of Engineering - Electrical Engineering Department, Islamic University in Madinah KSA.

Adnen Cherif is currently working as a full Professor Faculty of Science Tunis FST - Electrical Engineering Department, Head of Unit Search at Laboratory Innov'COM @ Sup'Com, School of Communications, University of Tunis El Manar Tunisia**.**

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.