A ROBUST WAVELET BASED WATERMARKING SCHEME FOR DIGITAL AUDIO

Ayad Ibrahim Abdulsada

Dept. of Computer Science, College of Education, University of Basrah, Basrah, Iraq.

Emile: ***mraiadibraheem@yahoo.com***

Abstract─ In this paper, a robust wavelet based watermarking scheme has been proposed for digital audio. A single bit is embedded in the approximation part of each frame. The watermark bits are embedded in two subsets of indexes randomly generated by using two keys for security purpose. The embedding process is done in adaptively fashion according to the mean of each approximation part. The detection of watermark does not depend on the original audio. To measure the robustness of the algorithm, different signal processing operations have been applied on the watermarked audio. Several experimental results have been conducted to illustrate the robustness and efficiency of the proposed watermarked audio scheme.

Keywords: *Audio, Wavelet, Fidelity, Robust, Blind watermark, MSE.*

منهج علامة مائية قوي معتمد على التحويل المويجي للأصوات الرقمية

أياد إبراهيم عبد السادة

قسم علوم الحاسبات, كلية التربية, جامعة البصرة, البصرة, العراق.

الخلاصة: في هذا البحث, تم تقديم منهج علامة مائية قوي يعتمد على التحويل المويجي للأصوات الرقمية. ثنائية منفردة يتم تضمينها في جزء التقريب لكل إطار. ثنائيات العلامة المائية يتم تضمينها في مجموعتين من المواقع المولدة عشوائيا بالاعتماد على مفتاحين وذلك لغرض الأمنية. عملية التضمين تتم بطريقة متكيفة بالاعتماد على معدل جزء التقريب. الكشف عن العلامة المائية يتم بدون الحاجة إلى الصوت الأصلي. لقياس متانة الخوارزمية, عدة عمليات لمعالجة الإشارة تم تطبيقها على الصوت الذي يحتوي على العلامة المائية. النتائج أظهرت أن الخوارزمية قوية و نقية

1. Introduction

Digital documents that are exchanged over the Internet can be accessed or modified by a malicious user with relative ease. This creates an important security concern while exchanging multimedia data over the Internet. Multimedia data contains information in the form of audio, video, still images, etc. Large amounts of multimedia data are being made available in many digital repositories such as newspaper and television web sites and museum databases, which archive historic documents. This increases the need for authentication and verification of document integrity for users of such data. One of the well-known methods used for authentication of digital documents is the public key encryption-based authentication [1]. However, the encryption-based method is not suitable for widespread distribution of a document since it needs to be decrypted by each recipient before using it or additional data should be tagged along with the document. An alternate approach uses digital watermarking [2] to ascertain the source/origin of the document, where a signature string is embedded in the document in such a way that the contents of the document are not altered. Watermarking can also be used in conjunction with encryption-based authentication techniques to provide an additional level of security in document authentication.

2. Watermarking Applications and Properties

Digital watermarking can be use for the following purposes [3, 4, 5]:

Broadcast monitoring: By putting a unique watermark in each video or sound clip prior to broadcast watermarks can be use for broadcast monitoring. Automated monitoring stations can then receive broadcasts and look for these watermarks, identifying when and where each clip appears. This is desired by content owners who wish to ensure that their material is not being illegally distributed, or who wish to determine royalty payments. It is also desired by advertisers who wish to ensure that their commercials are being broadcast at the times and locations they have purchased. Several commercial systems already exist which make use of this technology.

Owner identification: The watermark identifies the owner of the content. This information can be used by a potential use to obtain legal rights to copy or publish the content from the contact owner.

Fingerprinting: Watermarks can assist in tracing the source of illegal copies. In this case, the owner can embed different watermarks in the copies of the data that are supplied to different customers. Fingerprinting can be compared to embedding a serial number that is related to the customer's identity in the data. It enables the intellectual property owner to

identify customers who have broken their license agreement by supplying the data to third parties.

***Authentication*:** Here, the watermark encodes information required to determine that the content is authentic. It must be designed in such a way that any alteration of the content either destroys the watermark, or creates a mismatch between the content and the watermark that can be easily detected. If the watermark is present, and properly matches the content, the user of the content can be assured that it has not been altered since the watermark was inserted.

Copy control: The information stored in a watermark can directly control digital recording devices for copy protection purposes. In this case, the watermark represents a copy-prohibit bit and watermark detectors in the recorder determine whether the data offered to the recorder may be stored or not These are some of the major applications for which watermarks are currently being considered or used, but several others are likely to appear A digital watermark should possess certain properties. The relative importance of these properties depends on the application.

Some general properties can be given for most of the applications mentioned above [4, 5, 6, 7]:

Perceptual transparency: The modifications caused by watermark embedding, should not degraded the perceived media quality. A watermark-embedding procedure is truly imperceptible if humans cannot distinguish the original data from the data with the inserted watermark. However, even hardly visible differences may become apparent when the original data is compared directly with the watermarked data. Since users of watermarked data normally do not have access to the original data, they cannot perform this comparison. Therefore, it may be sufficient that the modifications in the watermarked data go unnoticed as long as the data are not compared with the original data.

Robustness: A watermarks is said to be robust if it survives signal processing operation that intentionally or unintentionally attempt to remove or alter the watermark information. Examples of unintentional operations are lossy compression techniques, filtering, re-sampling, digital-analog (D/A) and analog-digital (A/D) conversion, and geometric distortions. On the other hand, a watermark can also be subjected to processing solely intended to remove the watermark. In general, there should be no way in which the watermark can be removed or altered without sufficient degradation of the perceptual quality of the host data so as to render it unusable.

Capacity: It refers to the payload or the amount of watermark information that can be reliably hidden and recovered with low probability of error. The amount of information that can be stored in a watermark depends on the application. For copy control purposes, a payload of one bit is usually sufficient.

Security: The security of watermarking techniques can be interpreted in the same way as the security of encryption techniques. Secure data-embedding procedures cannot be broken unless the unauthorized user has access to a secret key that controls the insertion of the data

in the host signal. Hence a watermarking technique is truly secure if knowing the exact algorithms for embedding and extracting the watermark does not help an unauthorized party to detect the presence of the watermark.

Blind watermarking: In some applications extraction algorithms can use the original un watermarked data to find the watermark. This is called watermarking with informed detection or non-blind watermarking. Non-blind watermarking methods are usually more robust since the availability of the original data in the recovery process allows the detection and inversion of the applied distortion. However, access to the original un watermarked data is not possible in all cases, for example, in applications like broadcast monitoring. For other applications, like copy control, it may be impractical to use the original data because of the large data volume, even if it is available. This renders the watermark extraction more difficult. Most recent methods do not require the original for watermark recovery. Watermarking algorithms of this kind are referred to as blind or oblivious watermarking algorithms.

False positive rate: A false positive is a detection of a watermark in a piece of media that does not actually contain that watermark.

Computational cost: As with any technology intended for commercial use, the computational costs of inserting and detecting watermarks are important. This is particularly true when watermarks need to be inserted or detected in real-time video or audio.

3. Digital Audio Watermarking

Digital audio watermarking is the process of embedding a watermark signal into audio signal. Audio watermarking is a difficult job because of the sensitivity of *Human Auditory System* (HAS). Digital audio watermarking techniques can be classified according to the domain where the watermark takes place. there are four domains in digital audio watermarking [8, 9, 10]: frequency domain, time domain, compressed domain, and wavelet domain. In next section, we will present a robust algorithm for embedding a watermark in the wavelet domain of an audio signal.

4. The Proposed Audio Watermarking Algorithm

Wavelet transform can be used to decompose a signal into two parts, high frequencies (details D) and low frequencies (approximation A). The low frequencies part is decomposed again into two parts of high and low frequencies. The number of decompositions in this process is usually determined by application and length of original signal. The data obtained from the above decomposition are called the Discrete Wavelet Transform (DWT) coefficients. The original signal can be reconstructed from these coefficients. This reconstruction is called the inverse DWT [11].

In this paper, we embed a string of bits (watermark) in an audio signal by using the approximation coefficients of wavelet domain. Our algorithm consists of two parts: The embedding part and the detection part.

a. The Embedding Part:

The algorithm of embedding the watermark *W* in the audio signal *S* of length *L* consist of the following steps :

1. Determine the watermark $W=w_1, w_2, ..., w_N$. w_i is 0 or 1. N is the length of the watermark *W*.
2. Set the control of robustness, alpha.
3. Indexes Generation: Generate two subsets (A_{index}, B_{index}) of indexes randomly of length *R* by using two keys (key_1, key_2), respectively, for security purposes.
4. Divide the signal *S* into frames of the length *P* samples. The output of this step is: $Frame_1, Frame_2, ..., Frame_{L/P}$
5. **for** *i=1 to N*

Wavelet decomposition: in this step, we decompose the $Frame_i$ by using wavelet transform in two levels as shown in Figure (1).

Compute the mean of absoulute A_2 coefficients. $m=mean(abs(A_2))$.

If $w_i = 1$ **then**

$A_2(A_{index})=A_2(A_{index})+(m*alpha);$

$A_2(B_{index})=A_2(B_{index})-(m*alpha);$

Else

$A_2(A_{index})=A_2(A_{index})-(m*alpha);$

$A_2(B_{index})=A_2(B_{index})+(m*alpha);$

End

Wavelet reonstruction: Reconstruct the $Frame_i$ to construct the watermarked frame.

6. Collect all the watermarked frames and the remained frames to constuct the watermarked signal *WS*.

b. The Detection Part:

The algorithm used to detect the watermark from the watermarked signal WS consist of the following steps:

1. Generate the same subsets (A_{index}, B_{index}) of indexes using the same keys (key_1, key_2) which are used in the embedding part.

2. **For** *i=1 to N*

2.1 Decompose the $Frame_i$ as in Figure (1).

2.2 Compute: $Sum_A=sum(A_2(A_{index}))$, $Sum_B=sum(A_2(B_{index}))$.

2.3 **If** $Sum_A>Sum_B$

$w_i=1$

Else

$w_i=0$

End

5. Experimental Results

6. Figure (2) explain the digital audio signal that has been used as a cover to embed the string of watermark bits in it. In this paper we use frame size $P=100$ sample, $R=10$, and $alpha=0.7$.

7. Experiment (1):

8. In this experiment, we test the ***transparency*** **or** ***fidelity*** of the audio watermarked. We compute the difference between the original signal and the watermarked signal by using the Mean

Square Error (MSE) measure, which is explained in equation (1).

$$MSE = 1/L\sum_{i=1}^{L}(x_i - y_i)^2 \qquad \ldots(1)$$

where x_i, y_i are the original and watermarked signals, respectively, L is the signal length. Table (1) explains the MSE by using watermarks of different lengths N.

Experiment (2):

In this experiment, we test the ***robust*** of the proposed algorithm. Different signal processing operatoins has been tested. In all the following tests we embed the watermark, *W=[0 0 0 0 0 1 1 1 1 1], N=10*.

a. ***Noise:*** We add noise to the watermarked signal, Figure (2) explain the noised signal. Table (2) explain the effect of noise on the detected watermark.

b. ***Low Pass Filter:*** Figure (3) explain the filtered signal. Table (3) explains the effect of the low pass filter on the detection of the watermark from the watermarked signal. We use different cutoff frequencies.

c. ***Invert:*** when we invert the watermarked audio we notice that the watermark was inverted also. So, the retrieved watermark after invert the signal is *W=[1 1 1 1 1 0 0 0 0 0]*.

d. Resample: the watermarked signal sampled at 8000 sample/second. Table (4) explain the effect of resampling the watermarked signal.

e. ***Echo***: Adding echo to the watermarked audio does not affect on the watermark. So, the retrieved watermark *W=[0 0 0 0 0 1 1 1 1 1]*.

f. ***Compression:*** Figure (4) explain the effect of compression on the watermarked audio. Table (5) explains the effect of compression operation on the detected watermark. A compression ratio of 25% has been used for different thresholds.

6. Conclusions

1. The watermarked audio has more ***fidelity*** according to the MSE measure of Table (1). So, human ear cannot distinguish the original audio from the audio with the inserted watermark.
2. From experiment (2) we notice that the proposed algorithm have a ***robust*** property.
3. A ***security*** property is added to the proposed algorithm by using two keys to generate two subsets of indexes randomly.
4. In this paper a ***blind watermarking*** algorithm has been proposed. It does not require the original audio for watermark recovery.
5. In the embedding part an ***adaptive watermark*** has been used. Since it depend on the mean for each frame.

References

[1] B. Schneier, "Applied Cryptography". John Wiley & Sons, 1996.

[2] M. Wu and B. Liu, "Multimedia Data Hiding". Springer, 2002.

[3] Cox, M. Miller and J. Bloom, "Watermarking applications and their properties," *Int. Conf. on Information Technology'2000*, Las Vegas, 2000.

[4] Cox, M. Miller, and J. Bloom, "*Digital Watermarking*," Morgan Kaufmann Publishers, Inc., San Francisco, 2001.

[5] G. Langelaar, I. Setyawan, R. Legendijk, "Watermarking digital image and video data – A stateof- the-art overview," *IEEE Signal Processing Magazine,* vol. 17, no. 5, pp. 20-46, September 2000.

[6] F. Hartung and M. Kutter, "Multimedia watermarking techniques," *Proceeding of the IEEE, Special Issue on Protection of Multimedia Content*, vol. 87, pp. 1097- 1107, July 1999.

[7] M. Swanson, M. Kobayashi, A. Tewfik, "Multimedia Data-Embedding and Watermarking Technologies," *Proceedings of the IEEE*, vol. 86, no. 6, June 1998.

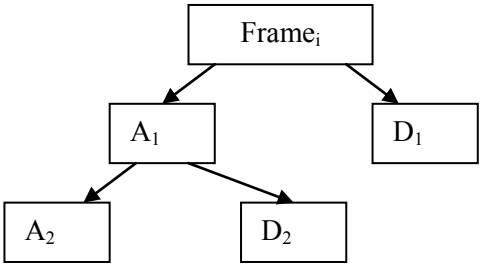

Figure (1): Wavelet Decomposition

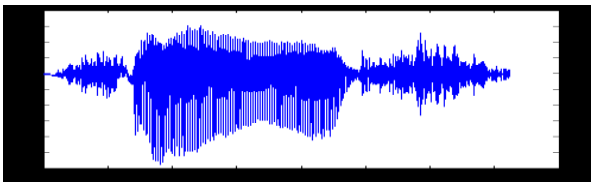

Figure (2): Digital audio

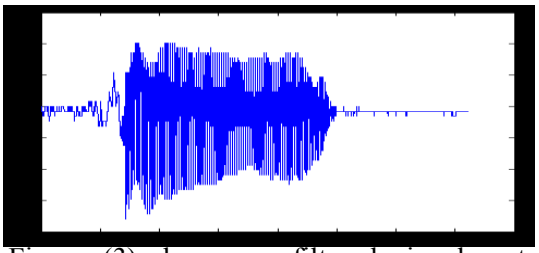

Figure (3): low pass filtered signal, cutoff freq. 500.

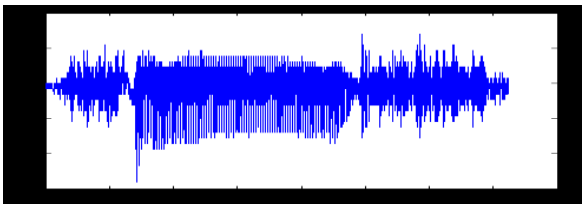

Figure (4): Compressed signal.

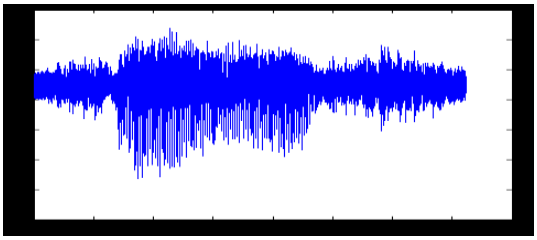

Figure (5): Noised signal, noise

Table(1): MSE of watermarks of different lengths.

N	MSE
10	2.0896e-005
20	0.0023
30	0.0058
40	0.0084

Table (2): Noise effect

Noise Rate	Detected watermark	No. of Correct bits
0.1	0 0 0 0 0 1 1 1 1 1	10
0.2	0 0 0 0 0 1 1 1 0 1	9
0.3	1 0 1 1 0 1 1 1 0 1	6
0.4	1 0 1 1 0 1 1 1 0 1	6
0.5	1 0 1 1 0 0 1 1 0 1	5

Table (3): Low Pass filter effect.

	Detected watermark	No. of Correct bits
100	1 0 0 0 1 0 1 1 0 1	6
200	1 1 1 0 1 1 0 0 0 0	2
300	1 1 1 0 0 1 1 1 1 1	7
400	0 0 0 0 0 1 1 1 1 1	10
500	0 0 0 0 0 1 1 1 1 1	10

Table (4): Resampling effect.

Samples	Detected watermark	No. of Correct bits
5500	0 1 0 1 1 0 1 0 1 1	5
6000	0 1 0 0 0 1 1 0 01	7
8300	0 0 0 0 0 1 1 1 1 1	10
9000	0 0 0 1 1 1 0 0 1 1	6
10000	0 1 1 1 1 0 1 0 0 1	3

Table (5): Compression effect

Threshold	Detected watermark	No. of Correct bits
0.001	0 0 0 0 0 1 1 1 1 1	10
0.005	0 0 0 0 0 1 1 1 1 1	10
0.01	0 0 0 0 0 1 1 1 1 1	10
0.05	0 0 0 0 0 1 1 1 1 1	10
0.02	0 0 0 0 0 1 1 1 1 1	10