Fragile Audio Watermark based on Empirical Mode Decomposition for Content Authentication

Dr. Matheel E. Abdulmunem  
Computer Science Department, University of Technology  
Baghdad, Iraq

Ameer A. Badr  
Computer Science Department, University of Technology  
Baghdad, Iraq

Abstract: Digital watermarking has become a passable technology for enabling multimedia protection schemes. Whilst most efforts focus on user authentication, lately attention in data authentication to assure data integrity has been growing. Fragile watermark algorithms are usually use in constructing content authentication systems. So, this paper propose a secure fragile adaptive blind audio watermarking algorithm based on Empirical Mode Decomposition (EMD). The audio signal is split into frames and each one is decomposed adaptively by EMD, into Intrinsic Mode Functions (IMFs). The watermark bits and the synchronization codes are embedded into the extrema of the first IMF, a high frequency mode sensitive to any small changes of audio signal. The experimental outcomes suggest that the method is fragile, imperceptible and having high capacity up to 3k pbs. The comparison analysis demonstrate that our method has superior performance than watermarking schemes reported recently.

Keywords: Fragile Audio Watermarking, Empirical Mode Decomposition, QR code.

I. INTRODUCTION

Digital audio watermarking has received a great deal of attention to provide efficient solutions for protection of digital media [1]. It is a process by which a watermark in the form of image, text, or audio is embedded or hidden into an original audio signal. These embedded data can be later extracted or detected from the marked signal for various applications such as content authentication, copyright protection, broadcast monitoring and fingerprinting [2]. Content authentication is one of the hottest topics of research recently, many real application need methodologies in order to assure that when delivering something to somewhere, it is delivered as is. The appropriate methodology should be simple and secure to assure the authenticity of the work [3]. Because of the sensitivity of Human Auditory System (HAS) over the Human Visual System (HVS) Watermarking a video or image sequence is quite easier than watermarking an audio signal [2].

Digital audio watermarking can be further divided into fragile watermark, semi-fragile watermark and robust watermark according to specific purpose. Fragile watermark is sensitive to any small changes of original multimedia file thus can be used to verify its integrity. Semi-fragile watermark can resist some common signal operations but is sensitive to malicious tampering. Robust watermark is used to copyright protection for it is resistant against various signal attacks [4].

Robustness, imperceptibility, and data capacity. Are main requirements of digital audio watermarking. More precisely, to preserve audio quality, the watermark should be inaudible within the host audio data. Finally, the watermark should be easy to extract to prove ownership [1].

Different watermarking techniques of varying complexities have been proposed, in [5] the watermarking bits are embedded into the peaks of the frames on which Discrete Fourier Transform (DFT) has been performed. The use of Fourier transformation is limited only to linear systems and stationary data series. In [6] Discrete Wavelet Transform (DWT) is used to decompose the host audio signal into several multi-resolution sub-bands. The highest resolution sub-band is chosen to embed the watermarking bits. This scheme proves to be promising considering the limitations of the Fourier transform, but yet poses a limitation that the basic functions of wavelet transform are fixed and do not necessarily match the shape of the considered data series in every instant in time [7].

To overcome this limitation, recently, a new signal decomposition method referred to as Empirical Mode Decomposition (EMD) has been introduced for analyzing non-stationary and nonlinear signals in totally adaptive way, as introduce in our previous work [8].

This paper proposes an efficient fragile audio watermarking that satisfies the requirement of inaudibility and security, based on EMD for audio content authentication. The rest of this paper is organized as follows. In Section II, EMD theory is reviewed. Section III, the Quick Response (QR) code was describe. Section IV, presents the synchronization code. Section V, present the prepressing, watermarking embedding and extracting algorithms are seen in section VI. Performance analysis and experimental results are shown in Section VII and VIII respectively. And providing concluding remarks in the final section.

II. EMPERICAL MODE DECOMPOSITION (EMD) FUNDAMENTAL

By applying EMD, the audio signal is decomposed into a set of Intrinsic mode functions (IMFs) and a final residual. The IMF defined by Huang [9], satisfies the following two conditions simultaneously [8]:

- In the entire data set, the extrema and zero crossing number have to similar or different at most by one.
- At each point, the envelope averaging value define by (local maxima, local minima) is zero.
A major advantage of EMD relies on a priori choice of filters or basis functions. Compared to classical kernel based approaches, EMD is fully data-driven method that recursively breaks down any signal into number of zero-mean components called IMFs.

Suppose the given signal $x(t)$ can be decomposed from finer scales to coarser ones as the summation of $n$ number of IMFs and a final residual as follows, as one can see in figure (1) [8]:

$$X(t) = \sum_{j=1}^{n} IMF(j) + r(t)$$

The IMFs are nearly orthogonal to each other, and all have nearly zero means. The number of extrema is decreased when going from one mode to the next, and the whole decomposition is guaranteed to be completed with a finite number of modes. The IMFs are fully described by their local extrema and thus can be recovered using these extrema [1].

Higher order IMFs such as low frequency mode are signal dominated, so, their modification can lead to signal degeneration. As result, these modes can be the best locations for robust watermark placement [1]. In contrast, watermarks embedded into high frequency mode such as lower order IMFs are most sensible to attacks. So, these modes can look to be the best position for fragile watermark placement as propose in this paper.

![Figure 1. Decomposition of an Audio Frame by EMD.](image)

III. THE QUICK RESPONSE (QR) CODE

QR Code is a two-dimensional bar code in the form of the matrix code that invented by Denso Wave in 1994. It has greater storage capacity, higher density, stronger error correction performance and safety over one-dimensional bar code, as see in figure (2-a) [10].

It can store large alphanumeric information and easily readable by scanner. A QR code is capable of being read in 360 degrees from any direction [11].

QR code is a matrix symbol that consists of an array of nominally square modules arranged in an overall square pattern. QR code includes unique finder pattern located at three corners of the symbol and intended to assist in easy location of its position, size and inclination. Structure of QR code is show in figure (2-b) [12].

![Figure 2. QR code; (a) A QR Code Image. (b) Structure of QR Code](image)

Figure 2-b shows the structure of the QR Code, which includes the following [13]:

- Version information: which denote the version of QR code from 1 to 40.
- Format information: is intended to store data, data type and data mask.
- Data area: is used to store data of QR code, which is the most space.
- Finder pattern: is used to detect the position of QR code for application to the decoder.
- Alignment pattern: if the images in the tilt. So, can be read correctly by decoder.
- Timing pattern: is detect the coordinates of the symbol for decoding.
- Quiet zone: is a region of the white space which helps to boost the finder pattern to detect quickly.

IV. SYNCHRONIZATION CODE (SC)

In most audio watermarking algorithms, the digital watermark bits are embedded into specific positions of the host audio signal. Therefore, to detect the hidden bits, the extracting process needs to know their positions. This is called the synchronization problem [15].

Synchronization is the key issue midst watermark extraction process. Any shift in the bit’s positions makes extracting schemes unable to succeed. So, find where the new shifted positions are, is the main goal of the synchronization schemes [15].

V. PREPROCESSING

The proposed watermarking method is based on EMD and without domain transform. Also the embedding and extracting process is done by using Quantization Index Modulation (QIM) due to its good robustness and blind nature [14]. Parameters of QIM are chosen to guarantee that the embedded watermark in the first IMF is inaudible.

The watermark is associated with a synchronization code to facilitate its location. An advantage to use the time domain approach, based on EMD, is the low cost in searching synchronization codes [1].
VI. PROPOSED FRAGILE AUDIO WATERMARKING ALGORITHM

The proposed watermarking technique idea is to hide in the time domain a mix of watermark data and a Synchronized Code (SC) into original audio signal. Firstly, the input audio signal is divided into equal frames and then EMD is conducted on every frame to extract the associated IMFs. As one can see in figure (1). Then bits sequence of watermark information and SCs, as seen in figure (3), is inserted in extrema points of a set of successive first-IMFs. A (1 or 0) bit is embedded per extrema.

Watermark and SCs are not all embedded in extrema of first IMF of only one frame. In general, the number of extrema per first-IMF of one frame is very small compared to length of the binary sequence to be embedded. Assume that L_1 and L_2 the numbers of bits of SC and watermark respectively. So, the length of binary sequence to be embedded is equal to 2L_1 + L_2. These bits are spread out on several first-IMFs (extrema) of the consecutive frame. Further, this sequence of bits is embedded N times.

Finally, the modified extrema of the watermarked signal are transformation back by using (EMD⁻¹), followed by frames concatenation.

As the embedding, in the extraction process, the watermarked audio signal is split into frames and EMD applied to each frame, as seen in figure (4). Binary data sequences are extracted from each first IMF by searching for SCs.

A. Using of SC

To locate the embedding position of the hidden watermark bits in the host signal a SC is used. Let A be the original SC and B be an unknown sequence of the same length. Sequence B is considered as a SC if only the difference between A and B, is less or equal than to a predefined threshold τ.

B. Encoding Watermark Information with QR Code

Considering the advantages of QR code, taking QR code image as the watermark image will give the watermarking system a certain degree of error correction ability and improve the effectiveness. Therefore, in the proposed approach, the text watermark information is firstly encoded with QR code encoding algorithm to generate the QR code image, which is then combining with SC for embedding in host signal.

C. Watermark Embedding

Before embedding, SCs are combined with QR watermark image bits to form a binary sequence denoted by W(i) ∈ \{0,1\}. Where (i) is the watermark bits, as seen in Figure (3). Algorithm (1) represent the watermark embedding as shown in Figure (5):

---

### Algorithm (1)

**Input:** Original audio signal, watermark bit sequence.

**Output:** Watermarked audio signal.

**Begin:**

1. Split original audio signal into frames.
2. Decompose each frame by EMD into IMFs.
3. Select the first IMFs (IMF1).
4. Detect the extreme points for IMF1.
5. Embed N times the binary sequence W(i) into extrema of the first IMF (one bits per extrema) by QIM as follow:
   - If W(i) equal to 1, then: \[ E^*(i) = \lfloor E(i)/S \rfloor + \frac{S}{2} (2) \]
   - Else if W(i) equal to 0, then: \[ E^*(i) = \lfloor E(i)/S \rfloor + \frac{S}{2} (3) \]
6. Reconstruct the frame using modified IMF1 and concatenate the watermarked frames to retrieve the watermarked signal.

**End.**

Where E(i) and E*(i) are the extrema of the host audio signal and the watermarked signal respectively, \( \lfloor \cdot \rfloor \) denotes the floor function, and S denotes the embedding strength chosen to maintain the inaudibility constraint.

---

**Figure 3:** Watermark Data Structure

**Figure 4:** Decomposition of the Watermarked Audio Frame by EMD.

**Figure 5:** Watermark Embedding Process
D. Watermark Extracting

For watermark extraction, watermark signal is split into frames and EMD is performed on each one as in embedding. First, one can extract binary data, then one can search for SCs in the extracted data. This is repeated by shifting the selected segment one sample at time until a SC is found. With the position of SC determined, we can then extract the hidden information bits, which follows the SC. Let $Y=M(i)$ denote the binary data to be extracted and $A$ denote the original SC. To locate the embedded watermark, we search the SCs in the sequence $M(i)$ bit by bit. The extraction is performed without using the original audio signal.

Algorithm (2) represent the watermarking extraction, as shown in Figure (6):

Input: Watermarked audio signal.

Output: QR code watermark image.

Begin:

Step 1: Split the watermarked signal into frames.

Step 2: Decompose each frame into IMFs.

Step 3: Extract the extrema $E(i)$ of IMF1.

Step 4: Extract $M(i)$ from $E(i)$ by QIM as follow:

Step 5: If: $E(i) \geq (S/2)$, then: $M(i) = 1$.

Step 6: Set the start index of the extracted data, $Y$, to $(I = 1)$ and select $(Len = L1)$ samples (sliding window size).

Step 7: Evaluate the similarity between the extracted segment $B = Y (1 : Len)$ and $A$ bit by bit.

Step 8: If the similarity value is $\geq \tau$, then: $B$ is taken as the SC and go to Step 10.

Step 9: Increase I by 1 and slide the window to the next $Len = L1$ samples and repeat Step 7.

Step 10: Evaluate the similarity between the second extracted segment, $B' = Y (I+L1+L2 : I+2L1+L2)$ and $A$ bit by bit.

Step 11: If: the similarity value is $\geq \tau$, then: $B$ is taken as the SC and go to Step 12.

Step 12: Extract the watermark bits from $(I+L1: I+L1+L2)$ as first candidate watermark image.

Step 13: Extract the N watermarks and make comparison bit by bit between these marks, for correction, and finally extract the desired watermark.

End.

VII. PERFORMANCE ANALYSIS

The performance of our method in terms of data payload, Signal to Noise Ratio (SNR) between original and the watermarked audio signals, Mean Opinion Score (MOS), Bit Error Rate (BER) and Normalized Correlation (NC) is evaluated. According to International Federation of the Photographic Industry (IFPI) recommendations, a watermark audio signal should maintain more than 20 dB SNR [1]. SNR calculated as [15]:

$$SNR(A,A') = 10 \log_{10} \left( \frac{\sum_{i=1}^{N} A(i)^2}{\sum_{i=1}^{N} (A(i)-A'(i))^2} \right) \text{ db}$$  \hspace{1cm} (6)

Five participants were selected to hear the original and watermarked audio signal and were asked to report the dissimilarities between the two. The output of this test is an average of the quality ratings called MOS. Table I shows the different MOS criterion [2].

<table>
<thead>
<tr>
<th>Score</th>
<th>Watermark Imperceptibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Imperceptible</td>
</tr>
<tr>
<td>4</td>
<td>Perceptible but not annoying</td>
</tr>
<tr>
<td>3</td>
<td>Slight annoying</td>
</tr>
<tr>
<td>2</td>
<td>Annoying</td>
</tr>
<tr>
<td>1</td>
<td>Very annoying</td>
</tr>
</tbody>
</table>

To evaluate the watermark image detection accuracy, we used the BER and the NC defined as follows [1]:

$$BER(W,W') = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} W(i,j) \oplus W'(i,j)}{M \times N}$$  \hspace{1cm} (7)

$$NC(W,W') = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} W(i,j) \ast W'(i,j)}{\sqrt{\sum_{i=1}^{M} \sum_{j=1}^{N} W^2(i,j)} \sqrt{\sum_{i=1}^{M} \sum_{j=1}^{N} W'^2(i,j)}}$$  \hspace{1cm} (8)

BER is used to estimate the accuracy of watermark detection after signal processing operations. Where $W$, $W'$ is the original and recovered watermark image respectively,
$N \times M$ are the sizes of watermark image. And $\oplus$ is the XOR operator. NC is used to evaluate the similarity between the extracted watermark and the original one. A low value of NC mention to the lack of watermark, while the large value mention to the presence of watermark.

The payload which quantifies the amount of information to be hidden can be used. More precisely, the data payload refers to the number of bits that are embedded into that audio signal within a unit of time and is measured in unit of bits per second (b/s).

### VIII. RESULT

To show the effectiveness of our scheme, emulation is performed on audio signals including Beethoven music, classic music, Latin music, pop song and slow song sampled at 44.1 kHz with 16-bit depth. The embedded watermark $W$ is a binary QR image of size $M \times N = 34 \times 34 = 1156$ bits, as see in figure (7). The 2D QR image was converted into 1D sequence for inserted it into the audio signal. A Barker sequence of 16-bit “1111100110101110” is used as SC. Each audio signal is divided into frames of size 64 samples. Also, the $S$ value is constant to 4 and the threshold $\tau$ is set to 5. These parameters have been chosen to have a good compromise between imperceptibility of the watermarked signal, payload and robustness. Also, to assure security of our proposed method, three parameters must be same in embedding and extracting process, there are: number of EMD iteration, locality between each extrema point and number of N times. Figure (8) shows the Beethoven music signal and its watermarked version. This figure shows that the watermarked signal is visually indistinguishable from the original one.

![Figure 7. QR Code Watermark Image](image7.png)

![Figure 8. A Beethoven Music Audio Signal and its Watermarked Version.](image8.png)

Perceptual quality rating can be done either by human acoustic perception by using subjective listening tests or using objective evaluation tests by measuring the MOS and SNR. One can see that the SNR values are not equal because the EMD is data dependent method. Also all the SNR values are above 20 dB showing the good choice of $S$ value and confirming to IFPI standard. All MOS values of the watermarked audio signals are 5, which demonstrates imperceptibility for the watermarked output, as see in table II.

<table>
<thead>
<tr>
<th>Audio File</th>
<th>SNR (db)</th>
<th>MOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Beethoven music</td>
<td>42.71</td>
<td>5</td>
</tr>
<tr>
<td>classic music</td>
<td>39.25</td>
<td>5</td>
</tr>
<tr>
<td>Latin music</td>
<td>42.60</td>
<td>5</td>
</tr>
<tr>
<td>pop song</td>
<td>37.38</td>
<td>5</td>
</tr>
<tr>
<td>slow song</td>
<td>33.60</td>
<td>5</td>
</tr>
</tbody>
</table>

Table II: SNR and MOS Between Original and Watermarked Audio.

<table>
<thead>
<tr>
<th>Audio file</th>
<th>BER %</th>
<th>NC</th>
<th>Extracted QR</th>
<th>Can be decoded ?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Beethoven music</td>
<td>0</td>
<td>0.9975</td>
<td><img src="image9.png" alt="QR Code" /></td>
<td>Yes</td>
</tr>
<tr>
<td>classic music</td>
<td>0</td>
<td>1</td>
<td><img src="image10.png" alt="QR Code" /></td>
<td>Yes</td>
</tr>
<tr>
<td>Latin music</td>
<td>0</td>
<td>0.9967</td>
<td><img src="image11.png" alt="QR Code" /></td>
<td>Yes</td>
</tr>
<tr>
<td>pop song</td>
<td>0</td>
<td>0.9992</td>
<td><img src="image12.png" alt="QR Code" /></td>
<td>Yes</td>
</tr>
<tr>
<td>slow song</td>
<td>0</td>
<td>0.9992</td>
<td><img src="image13.png" alt="QR Code" /></td>
<td>Yes</td>
</tr>
</tbody>
</table>

Table III: BER and NC of extracted watermark for Beethoven music audio signal given by proposed approach.

In order to evaluate the work performance of our fragile watermarking scheme, the authentication test is illustrated in the proposed watermarking algorithm to show the ability of content authentication. Since an attack changes the location of extrema in the watermark signal, the recovered watermark does not found in extrema point of the tampered signal. This results in the ability to detect any tampering in the signal.

Since the most common attacks are based on filtering, compression, cropping and resampling to the watermarked signal. So, to assess the authentication of our scheme, these attacks are performed:

- Filtering: Lowpass and highpass filtering was applied to the watermarked signal. A high pass filter removing all frequencies lower than a chosen
threshold, 50 Hz in our case. A low pass filter removing all frequencies higher than a chosen threshold, 15 kHz in our case.

- Cropping: Arbitrary samples of the watermarked signal are removed from begin, middle and end positions.
- Resampling: The watermarked signal, originally sampled at 44.1 kHz, is re-sampled at 22.05 kHz and restored back by sampling again at 44.1 kHz.
- Compression: A compressor is used to decrease the range of signal strength in audio signals, we have used the following settings: Attack time 1 ms, release time 1 ms, output gain -6 dB, threshold -15 dB and ratio 1:1.1.

Table IV shows the watermark signal authentication test; one can see the extracted watermarks with the associated BER values for different attacks on Beethoven music audio signal.

Table IV: Authentication test on Beethoven music audio signal.

<table>
<thead>
<tr>
<th>Attack type</th>
<th>Extracted QR</th>
<th>BER %</th>
<th>Can be decoded?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lowpass filter</td>
<td></td>
<td>49</td>
<td>No</td>
</tr>
<tr>
<td>(15 kHz)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Highpass filter</td>
<td></td>
<td>52</td>
<td>No</td>
</tr>
<tr>
<td>(50 kHz)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cropping</td>
<td></td>
<td>51</td>
<td>No</td>
</tr>
<tr>
<td>Resampling</td>
<td></td>
<td>51</td>
<td>No</td>
</tr>
<tr>
<td>Compression</td>
<td></td>
<td>55</td>
<td>No</td>
</tr>
</tbody>
</table>

Results of experiment demonstrate the algorithm is fragile to common signal process attack and is adaptive to tamper verify. This is mainly due to the insertion of the watermark into first IMF extrema. In fact, high frequency sub band has sensitive to any small changes of audio signal.

Also, the attack on classic music, Latin music, pop song and slow song gives similar results. Table V shows comparison results in terms of payload of our method to six recent watermarking schemes. The comparison is sorted by attempted data payload. It can be seen that our method achieves the highest payload.

Table V: Comparison of audio watermarking methods, sorted by attempted payload.

<table>
<thead>
<tr>
<th>Reference</th>
<th>Payload (pbs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proposed algorithm</td>
<td>2368 – 3423</td>
</tr>
<tr>
<td>Mehdi Fallahpur and David Megias [16]</td>
<td>683 – 3000</td>
</tr>
<tr>
<td>Kais Khaldi and Abdel-Ouahab Boudraa [1]</td>
<td>46.9 – 50.3</td>
</tr>
<tr>
<td>V. Bhat, K. I. Sengupta, and A. Das [17]</td>
<td>45.9</td>
</tr>
<tr>
<td>N. Cveic and T. Seppanen [18]</td>
<td>27.1</td>
</tr>
<tr>
<td>S. Xiang, H. J. Kim, and J. Huang [19]</td>
<td>2</td>
</tr>
</tbody>
</table>

IX. CONCLUSION

In this paper an adaptive fragile watermarking scheme based on the EMD is proposed. Watermark is embedded in high frequency mode (first IMF), thus achieving good sensitive against various attacks. The watermark image is a QR code, and is linked with synchronization codes to withstand cropping and shifting. Watermark bits are embedded in the extrema of the first IMF of the audio signal based on QIM. Outspread emulation over diverse audio signals indicate that the proposed watermarking scheme has better efficiency than six recently proposed algorithms. This scheme has much higher payload compared to these earlier audio watermarking methods. Also demonstrate that our algorithm is fragile to common signal process attack and is adaptive to tamper verify. In all audio test signals, the watermark introduced no audible distortion. Experiments demonstrate that the watermarked audio signals are indistinguishable from original ones. These performances take advantage of the self-adaptive decomposition of the audio signal provided by the EMD. Our watermarking method encompass easy calculations and does not use the original audio signal. In the conducted experiments the embedding strength $S$ is kept fixed for all audio files.

Suggestion for future work include the design of a solution method for adaptive embedding problem. Also as future research we plan to include the characteristics of the human auditory and psychoacoustic model in our watermarking scheme for much more improvement of the performance of the watermarking method. Finally, it should be interesting to investigate if the proposed method supports various sampling rates with the same payload.

X. REFERENCE


