Science Arts & Métiers (SAM)
is an open access repository that collects the work of Arts et Métiers ParisTech researchers and makes it freely available over the web where possible.

This is an author-deposited version published in: https://sam.ensam.eu
Handle ID: http://hdl.handle.net/10985/8985

To cite this version:
Kais KHALDI, Abdel-Ouahab BOUDRAA - Audio watermarking via EMD - IEEE Transactions on Audio, Speech and Language Processing - Vol. 21, n°3, p.675-680 - 2013

Any correspondence concerning this service should be sent to the repository Administrator: archiveouverte@ensam.eu
Audio Watermarking Via EMD

Kais Khaldi and Abdel-Ouahab Boudraa, Senior Member, IEEE

Abstract—In this paper a new adaptive audio watermarking algorithm based on Empirical Mode Decomposition (EMD) is introduced. The audio signal is divided into frames and each one is decomposed adaptively, by EMD, into intrinsic oscillatory components called Intrinsic Mode Functions (IMFs). The watermark and the synchronization codes are embedded into the extrema of the last IMF, a low frequency mode stable under different attacks and preserving audio perceptual quality of the host signal. The data embedding rate of the proposed algorithm is 46.9–50.3 b/s. Relying on exhaustive simulations, we show the robustness of the hidden watermark for additive noise, MP3 compression, re-quantization, filtering, cropping and resampling. The comparison analysis shows that our method has better performance than watermarking schemes reported recently.

Index Terms—Empirical mode decomposition, intrinsic mode function, audio watermarking, quantization index modulation, synchronization code.

I. INTRODUCTION

Digital audio watermarking has received a great deal of attention in the literature to provide efficient solutions for copyright protection of digital media by embedding a watermark in the original audio signal [1]–[5]. Main requirements of digital audio watermarking are imperceptibility, robustness and data capacity. More precisely, the watermark must be inaudible within the host audio data to maintain audio quality and robust to signal distortions applied to the host data. Finally, the watermark must be easy to extract to prove ownership. To achieve these requirements, seeking new watermarking schemes is a very challenging problem [5]. Different watermarking techniques of varying complexities have been proposed [2]–[5]. In [5] a robust watermarking scheme to different attacks is proposed but with a limited transmission bit rate. To improve the bit rate, watermarked schemes performed in the wavelets domain have been proposed [3], [4]. A limit of wavelet approach is that the basis functions are fixed, and thus they do not necessarily match all real signals. To overcome this limitation, recently, a new signal decomposition method referred to as Empirical Mode Decomposition (EMD) has been introduced for analyzing non-stationary signals derived or not from linear systems in totally adaptive way [6].

A major advantage of EMD relies on no 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 a reduced number of zero-mean with symmetric envelopes AM-FM components called Intrinsic Mode Functions (IMFs). The decomposition starts from finer scales to coarser ones. Any signal $x(t)$ is expanded by EMD as follows:

$$x(t) = \sum_{j=1}^{C} \text{IMF}_j(t) + r_C(t)$$  \hspace{1cm} (1)$$

where $C$ is the number of IMFs and $r_C(t)$ denotes the final residual. 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 [7], [8]. Low frequency components such as higher order IMFs are signal dominated [9] and thus their alteration can lead to degradation of the signal. As result, these modes can be considered to be good locations for watermark placement. Some preliminary results have appeared recently in [10], [11] showing the interest of EMD for audio watermarking. In [10], the EMD is combined with Pulse Code Modulation (PCM) and the watermark is inserted in the final residual of the subbands in the transform domain. This method supposes that mean value of PCM audio signal may no longer be zero. As stated by the authors, the method is not robust to attacks such as band-pass filtering and cropping, and no comparison to watermarking schemes reported recently in literature is presented. Another strategy is presented in [11] where the EMD is associated with Hilbert transform and the watermark is embedded into the IMF containing highest energy. However, why the IMF carrying the highest amount of energy is the best candidate mode to hide the watermark has not been addressed. Further, in practice an IMF with highest energy can be a high frequency mode and thus it is not robust to attacks.

Watermarks inserted into lower order IMFs (high frequency) are most vulnerable to attacks. It has been argued that for watermarking robustness, the watermark bits are usually embedded in the perceptually important components, mostly, the low frequency components of the host signal [12]. Compared to [10], [11], to simultaneously have better resistance against attacks and imperceptibility, we embed the watermark in the extrema of the last IMF. Further, unlike the schemes introduced in [10], [11], the proposed watermarking is only based on EMD and without domain transform. We choose in our method a watermarking technique in the category of Quantization Index Modulation (QIM) due to its good robustness and blind nature [13]. Parameters of QIM are chosen to guarantee that the embedded watermark in the last 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. Audio signal is first segmented into frames where each one is decomposed adaptively into IMFs. Bits are inserted into the extrema of the last IMF such that the watermarked signal inaudibility is guaranteed. Experimental results demonstrate that the hidden data are robust against

Fig. 1. Decomposition of an audio frame by EMD.

Fig. 2. Data structure $(m_i)$.
attacks such as additive noise, MP3 compression, requantization, cropping and filtering. Our method has high data payload and performance against MP3 compression compared to audio watermarking approaches reported recently in the literature.

II. PROPOSED WATERMARKING ALGORITHM

The idea of the proposed watermarking method is to hide into the original audio signal a watermark together with a Synchronized Code (SC) in the time domain. The input signal is first segmented into frames and EMD is conducted on every frame to extract the associated IMFs (Fig. 1). Then a binary data sequence consisted of SCs and informative watermark bits (Fig. 2) is embedded in the extrema of a set of consecutive last-IMFs. A bit (0 or 1) is inserted per extrema.

Since the number of IMFs and then their number of extrema depend on the amount of data of each frame, the number of bits to be embedded varies from last-IMF of one frame to the following. Watermark and SCs are not all embedded in extrema of last IMF of only one frame. In general the number of extrema per last-IMF (one frame) is very small compared to length of the binary sequence to be embedded. This also depends on the length of the frame. If we design by $N_1$ and $N_2$ the numbers of bits of SC and watermark respectively, the length of binary sequence to be embedded is equal to $2N_1 + N_2$. Thus, these $2N_1 + N_2$ bits are spread out on several last-IMFs (extrema) of the consecutive frames. Further, this sequence of $2N_1 + N_2$ bits is embedded $P$ times. Finally, inverse transformation (EMD$^{-1}$) is applied to the modified extrema to recover the watermarked audio signal by superposition of the IMFs of each frame followed by the concatenation of the frames (Fig. 3). For data extraction, the watermarked audio signal is split into frames and EMD applied to each frame (Fig. 4). Binary data sequences are extracted from each last IMF by searching for SCs (Fig. 5). We show in Fig. 6 the last IMF before and after watermarking. This figure shows that there is little difference in terms of amplitudes between the two modes. EMD being fully data adaptive, thus it is important to guarantee that the number of IMFs will be same before and after embedding the watermark (Figs. 1, 4). In fact, if the numbers of IMFs are different, there is no guarantee that the last IMF always contains the watermark information to be extracted. To overcome this problem, the sifting of the watermarked signal is forced to extract the same number of IMFs as before watermarking. The proposed watermarking scheme is blind, that is, the host signal is not required for watermark extraction. Overview of the proposed method is detailed as follows:

A. Synchronization Code

To locate the embedding position of the hidden watermark bits in the host signal a SC is used. This code is unaffected by cropping and shifting attacks [4].

Let $U$ be the original SC and $V$ be an unknown sequence of the same length. Sequence $V$ is considered as a SC if only the number of different bits between $U$ and $V$, when compared bit by bit, is less or equal than to a predefined threshold $\tau$ [3].

B. Watermark Embedding

Before embedding, SCs are combined with watermark bits to form a binary sequence denoted by $m_i \in \{0,1\}$, $i$-th bit of watermark (Fig. 2). Basics of our watermark embedding are shown in Fig. 3 and detailed as follows:

Step 1: Split original audio signal into frames.
Step 2: Decompose each frame into IMFs.
Step 3: Embed $P$ times the binary sequence $\{m_i\}$ into extrema of the last IMF (IMF$_C$) by QIM [13]:

$$e^*_i = \begin{cases} \lfloor e_i/S \rfloor \cdot S + \text{sgn}(3S/4) \cdot \text{sgn}(S) & \text{if } m_i = 1 \\ \lfloor e_i/S \rfloor \cdot S + \text{sgn}(S/4) & \text{if } m_i = 0 \end{cases}$$

where $e_i$ and $e^*_i$ are the extrema of IMF$_C$ of the host audio signal and the watermarked signal respectively. $\text{sgn}$ function is equal to “+” if $e_i$ is a maxima, and “−” if it is a minima. $\lfloor \cdot \rfloor$ denotes the floor function, and $S$ denotes the embedding strength chosen to maintain the inaudibility constraint.

Step 4: Reconstruct the frame (EMD$^{-1}$) using modified IMF$_C$ and concatenate the watermarked frames to retrieve the watermarked signal.

C. Watermark Extraction

For watermark extraction, host signal is split into frames and EMD is performed on each one as in embedding. We extract binary data using rule given by (3). We then search for SCs in the extracted data. This procedure is repeated by shifting the selected segment (window) 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 $U$ 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. Basic steps involved in the watermarking extraction, shown in Fig. 5, are given as follows:

Step 1: Split the watermarked signal into frames.
Step 2: Decompose each frame into IMFs.
Step 3: Extract the extrema $\{e^*_i\}$ of IMF$_C$.
Step 4: Extract $m_i^*$ from $e_i^*$ using the following rule [3]:

$$m_i^* = \begin{cases} 1 & : \left| e_i^* - \frac{e_i^*}{S} \right| \geq \text{sgn}(S/2) \\ 0 & : \left| e_i^* - \frac{e_i^*}{S} \right| < \text{sgn}(S/2) \end{cases}$$  \hspace{1cm} (3)$$

Step 5: Set the start index of the extracted data, $y$, to $I = 1$ and select $L = N_1$ samples (sliding window size).

Step 6: Evaluate the similarity between the extracted segment $V = y(I + 1 : L)$ and $U$ bit by bit. If the similarity value is $\geq \tau$, then $V$ is taken as the SC and go to Step 8. Otherwise proceed to the next step.

Step 7: Increase $I$ by 1 and slide the window to the next $L = N_1$ samples and repeat Step 6.

Step 8: Evaluate the similarity between the second extracted segment, $V' = y(I + N_1 + N_2 : I + 2N_1 + N_2)$ and $U$ bit by bit.

Step 9: If $I = I + N_1 + N_2$, then the new $I$ value is equal to sequence length of bits, go to Step 10 else repeat Step 7.

Step 10: Extract the $P$ watermarks and make comparison bit by bit between these marks, for correction, and finally extract the desired watermark.

Watermarking embedding and extraction processes are summarized in Fig. 7.

III. Performance Analysis

We evaluate the performance of our method in terms of data payload, error probability of SC, Signal to Noise Ratio (SNR) between original and the watermarked audio signals, Bit Error Rate and Normalized cross-Correlation. According to International Federation of the Photographic Industry (IFPI) recommendations, a watermark audio signal should maintain more than 20 dB SNR. To evaluate the watermark detection accuracy after attacks, we use the $\mathcal{XC}$ measure defined as follows [4]:

$$\mathcal{XC}(W, \hat{W}) = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} W(i, j) \otimes \hat{W}(i, j)}{M \times N}$$  \hspace{1cm} (5)$$

A large $\mathcal{XC}$ indicates the presence of watermark while a low value suggests the lack of watermark. Two types of errors may occur while searching the SCs: the False Positive Error (FPE) and the False Negative Error (FNE). These errors are very harmful because they impair the credibility of the watermarking system. The associated probabilities of these errors are given by [3], [4]:

$$P_{\text{FPE}} = \frac{1}{2^p} \sum_{k=p+1}^{C_p^k} C_p^k \quad \text{and} \quad P_{\text{FNE}} = \frac{1}{2^p} \sum_{k=p+1}^{C_p^k} C_p^k (\text{BER})^k (1 - \text{BER})^{p-k}$$  \hspace{1cm} (6)$$

where $p$ is the SC length and $\tau$ is the threshold. $P_{\text{FPE}}$ is the probability that a SC is detected in false location while $P_{\text{FNE}}$ is the probability that a watermarked signal is declared as unwatermarked by the decoder. We also use as performance measure the payload which quantifies the amount of information to be hidden. 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).
To show the effectiveness of our scheme, simulations are performed on audio signals including pop, jazz, rock and classic sampled at 44.1 kHz. The embedded watermark, $W$, is a binary logo image of size $M \times N = 34 \times 48 = 1632$ bits (Fig. 8). We convert this 2D binary image into 1D sequence in order to embed it into the audio signal. The SC used is a 16 bit Barker sequence $1111100110101110$. Each audio signal is divided into frames of size 64 samples and the threshold $\tau$ is set to 4. The $S$ value is fixed to 0.98. These parameters have been chosen to have a good compromise between imperceptibility of the watermarked signal, payload and robustness. Fig. 9 shows a portion of the pop signal and its watermarked version. This figure shows that the watermarked signal is visually indistinguishable from the original one.

Perceptual quality assessment can be performed using subjective listening tests by human acoustic perception or using objective evaluation tests by measuring the SNR and Objective Difference Grade (ODG). In this work we use the second approach. ODG and SNR values of the four watermarked signals are reported in Table I. The SNR values are above 20 dB showing the good choice of $S$ value and confirming to IFPI standard. All ODG values of the watermarked audio signals are between $-1$ and 0 which demonstrates their good quality.

### IV. Results

#### A. Robustness Test

To assess the robustness of our approach, different attacks are performed:

- **Noise**: White Gaussian Noise (WGN) is added to the watermarked signal until the resulting signal has an SNR of 20 dB.
- **Filtering**: Filter the watermarked audio signal using Wiener filter.
- **Cropping**: Segments of 512 samples are removed from the watermarked signal at thirteen positions and subsequently replaced by segments of the watermarked signal contaminated with WGN.
- **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**: (64 kb/s and 32 kb/s) Using MP3, the watermarked signal is compressed and then decompressed.
- **Requantization**: The watermarked signal is re-quantized down to 8 bits/sample and then back to 16 bits/sample.

Table II shows the extracted watermarks with the associated $\text{NC}$ and $\text{BER}$ values for different attacks on pop audio signal. $\text{NC}$ values are all above 0.9482 and most $\text{BER}$ values are all below 3%. The extracted watermark are visually similar to the original watermark. These results shows the robustness of watermarking method for pop audio signal. Even in the case of WGN attack with SNR of 20 dB, our approach does not detects any error. This is mainly due to the insertion of the watermark into IMFs extrema. In fact low frequency subband has high robustness against noise addition [3], [4]. Table III reports similar results for classic, jazz and rock audio files. $\text{NC}$ values are all above 0.9964 and $\text{BER}$ values are all below 3%, demonstrating the good performance robustness of our method on these audio files. This robustness is due to the fact that even the perceptual characteristics of individual audio files vary, the EMD decomposition adapts to each one. Table IV shows comparison results in terms of payload and robustness to MP3 compression attack of our method to nine recent watermarking schemes.
TABLE II
BER AND NC OF EXTRACTED WATERMARK FOR POP AUDIO SIGNAL BY PROPOSED APPROACH

<table>
<thead>
<tr>
<th>Attack type</th>
<th>BER %</th>
<th>NC</th>
<th>Extracted watermark</th>
</tr>
</thead>
<tbody>
<tr>
<td>No attack</td>
<td>0</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>AWGN (20 dB)</td>
<td>0</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Filtering</td>
<td>6</td>
<td>0.9482</td>
<td></td>
</tr>
<tr>
<td>Cropping</td>
<td>0</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Resampling</td>
<td>3</td>
<td>0.9783</td>
<td></td>
</tr>
<tr>
<td>MP3 (64 Kb/s)</td>
<td>0</td>
<td>0.9996</td>
<td></td>
</tr>
<tr>
<td>MP3 (32 Kb/s)</td>
<td>1</td>
<td>0.9876</td>
<td></td>
</tr>
<tr>
<td>Requantization</td>
<td>0</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

TABLE III
BER AND NC OF EXTRACTED WATERMARK FOR DIFFERENT AUDIO SIGNALS (CLASSIC, JAZZ, ROCK) BY OUR APPROACH

<table>
<thead>
<tr>
<th>Audio signal</th>
<th>Attack type</th>
<th>BER %</th>
<th>NC</th>
</tr>
</thead>
<tbody>
<tr>
<td>classic</td>
<td>No attack</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>AWGN</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Filtering</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Cropping</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Resampling</td>
<td>2</td>
<td>0.9986</td>
</tr>
<tr>
<td></td>
<td>MP3 (64 kb/s)</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>MP3 (32 kb/s)</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Requantization</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>jazz</td>
<td>No attack</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>AWGN</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Filtering</td>
<td>3</td>
<td>0.9964</td>
</tr>
<tr>
<td></td>
<td>Cropping</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Resampling</td>
<td>2</td>
<td>0.9983</td>
</tr>
<tr>
<td></td>
<td>MP3 (64 kb/s)</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>MP3 (32 kb/s)</td>
<td>1</td>
<td>0.9973</td>
</tr>
<tr>
<td></td>
<td>Requantization</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>rock</td>
<td>No attack</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>AWGN</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Filtering</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Cropping</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Resampling</td>
<td>1</td>
<td>0.9989</td>
</tr>
<tr>
<td></td>
<td>MP3 (64 kb/s)</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>MP3 (32 kb/s)</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Requantization</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

V. CONCLUSION

In this paper a new adaptive watermarking scheme based on the EMD is proposed. Watermark is embedded in very low frequency mode (last IMF), thus achieving good performance against various attacks. Watermark is associated with synchronization codes and thus the synchronized watermark has the ability to resist shifting and cropping. Data bits of the synchronized watermark are embedded in the extrema of the last IMF of the audio signal based on QIM. Extensive simulations over different audio signals indicate that the proposed watermarking scheme has greater robustness against common attacks than nine recently proposed algorithms. This scheme has higher payload and better performance against MP3 compression compared to these earlier audio watermarking methods. 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. The proposed scheme achieves very low false positive and false negative error probability rates. Our watermarking method involves easy calculations and does not use the original audio signal. In the conducted experiments the embedding strength S is kept constant for all audio files. To further improve the performance of the method, the S parameter should be adapted to the type and magnitudes of the original audio signal. Our future works 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 and robustness and also if in real applications the method can handle D/A-A/D conversion problems.

REFERENCES


