ISSN: 2278-0181
ICONECT-2015 Conference Proceedings

Secure Watermarking for Audio Files

Devendra Negi, Venkatesh Guntuk, Akshay Revadekar
B.E.Computer
K.C.C.O.E.M.S.R
Mumbai University

Abstract:- **Digital watermarking has been proposed as a new, alternative method to enforce intellectualproperty rights and protect digital media from tampering. Digital watermarking is defined as imperceptible, robust and secure communication of data related to the host signal, which includes embedding into and extraction from the host signal. The main challenge in digital audio watermarking is that if the perceptual transparency parameter is fixed, the design of a watermark system cannot obtain high robustness and a high watermark data rate at the same time.In our thesis 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. Relying on exhaustive simulations, we show the robustness of the hidden watermark for various types of attacks and different types of noises such as additive noise, Gaussian noise, Salt and pepper noise.**

General Terms
Empherical mode decomposition, Intrinsic mode function, audio watermarking, Quantization, Segmentation, Embedding, Extraction.

Keywords :- Sync code, EMD, Digital Image Watermarking, Modulation, IMF

1. INTRODUCTION

By virtue of the new advancements in computer and telecommunication networks, multimedia files are produced, stored and distributed easily across the globe. However, the ownership and copyright of multimedia files are not usually protected. Digital audio watermarking has been proposed in recent years as a means of protecting multimedia contents from intellectual piracy. This is achieved by modifying the original content, by inserting a signature which can be extracted, when necessary, as a proof of ownership. Indeed, many effective digital image and video watermarking algorithms have been proposed and implemented at a commercial scale.

2. LITERATURE SURVEY

The zero-watermarking idea is introduced into the design of robust watermarking algorithm to ensure the transparency and to avoid the interference between the robust watermark and the semi-fragile watermark.ICA(Independent component analysis) is a very general-purpose statistical technique to recover the independent sources given only sensor observations that are linear mixtures of independent source signals[1].In this paper,PCM (Pulse Code Modulation) is used.In this paper an information hiding method as a real-time watermarking technique in musical acoustic signals **.**Watermark is inserted in the wavetable of a sound synthesizer separately, and the watermarked waveform was generated automatically with a selective output of the instruments in real-time[2].This paper considers desired properties such as security properties such as robustness, mathematical formulation, coding procedure and possible applications of audio watermarking algorithms such as copyright protection, monitoring, fingerprints, indication of content manipulation. Special attention is given to statistical methods working in the Fourier domain. It will present a solution of robust watermarking of audio data and reflect the security properties of the techniques[3].

The proposed method enables us to embed digital watermarks in a near-optimum manner for each audio file. In addition, the security of the watermarked audio is improved by using a characteristic secret key to embed and extract digital watermark[4]. In this paper, several novel mechanisms for effective encoding and detection of direct-sequence spread-spectrum watermarks in audio signals**.** Information modulation is usually carried out using Spread Spectrum or quantization index modulation (QIM).In this paper spread spectrum sequences are hidden inside the audio signal by using modulated complex lapped transform (MCLT) and Psycho-Acoustic Frequency Maskinghigher robustness to frame dropping and limited geometric distortions[5].

In this paper, a robust audio watermarking scheme based on singular value decomposition (SVD) and differential evolution (DE) using dither modulation (DM) quantization algorithm is proposed. LWT\DWT is first applied to decompose the host signal and obtain the corresponding approximate coefficients followed by DCT to take advantage of “energy compaction” property. SVD is further performed to acquire the singular values and enhance the robustness of the scheme [6].The RASE

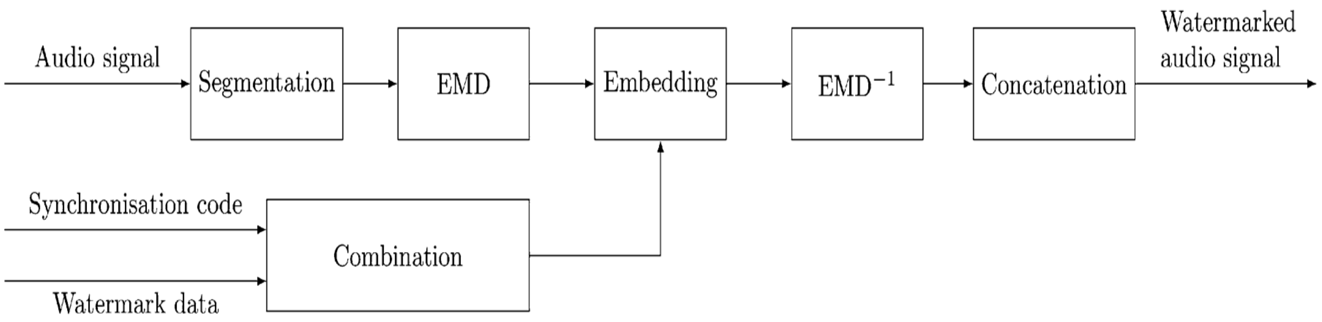

Fig 1.Watermark Embedding

(Robust Audio Segment Extractor) is proposed to extract reliable segments for watermarking. The watermark is embedded in the approximation coefficients of SWT (Stationary Wavelet Transform) decomposition. The spread spectrum communication technique is adopted to embed the watermark[7].

Robust patchwork-based watermarking method for audio signals, which is specifically designed to resist de-synchronization attacks. In the paper, watermarks are embedded into the audio signal by modifying its DCT coefficients. In order to tackle de-synchronization attacks, a number of synchronization bits are added into the watermarked signal in the LDCT domain at the embedding stage [8].

The DWT transform decomposes the host audio signal into several multi-resolution sub-bands, enabling algorithm developers to locate the most appropriate sub-bands for embedding the watermark bits. In the proposed algorithm, the watermark bits are embedded in the high-resolution sub-bands of the audio signal, so that satisfactory robustness and imperceptibility (inaudibility) performances are obtained [9].

The use of antipodal binary random binning has several advantages, including the possibility of relying on simple and effective binary code constructions and the ease with which this kind of schemes can cope with amplitude scaling. By relying on a novel binning strategy,we derive a lower bound of the Gelfand–Pinsker capacity of the watermark channel when the encoder is forced to use an antipodal binary auxiliary random variable, showing that forlow to moderate bit-rates, the bound coincides with Costa's capacity[10].

3. METHODOLOGY

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

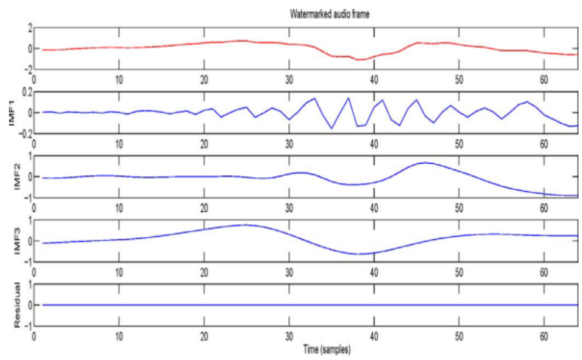

Fig. 2. Decomposition of the watermarked audio frame by EMD.

3.2 WATERMARK EMBEDDING

Before embedding, SCs are combined with watermark bits to form a binary sequence denoted by mi€ {0, 1},
i-th bit of watermark. Basics of our watermark embedding are shown in Fig. 1 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 ofthe last IMF by QIM:

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

where and are the extrema of the host audio signal and the watermarked signal respectively. sgn function is equal to "+" if is a maxima, and "-" if it is a minimal. Denotes the floor function, and S denotes the embedding strength chosen to maintain the inaudibility constraint.

Step 4: Reconstruct the frame using modified and concatenate the watermarked frames to retrieve the watermarked signal.

3.2. Watermark Extraction

For watermark extraction, host signal is splitted into frames andEMDis performed on each one as in embedding.We extract binary datausing rule given by Step 4 of watermark extraction. We then search for SCs in the extracted data.This procedure is repeated by shifting the selected segment (window).

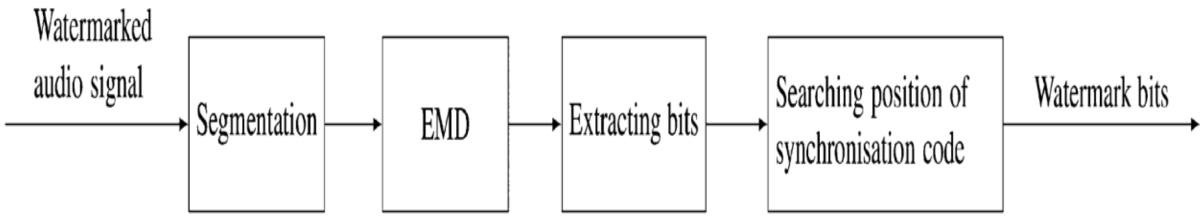

Fig 3. Watermark extraction

The segment window is shifted one sample at time until a SC is found. With the position of SC determined,we can then extract the hidden information bits, which followsthe SC. Let denote the binary data to be extracted anddenote the original SC. To locate the embedded watermark we searchthe SCs in the sequence bit by bit. The extraction is performedwithout using the original audio signal. Basic steps involved in the watermarkingextraction, shown in Fig. 3, are given as follows:

Step 1: Split the watermarked signal into frames.

Step 2: Decompose each frame into IMFs.

Step 3: Extract the extrema of Fig. 6. Last IMF of an audio frame before and after watermarking.

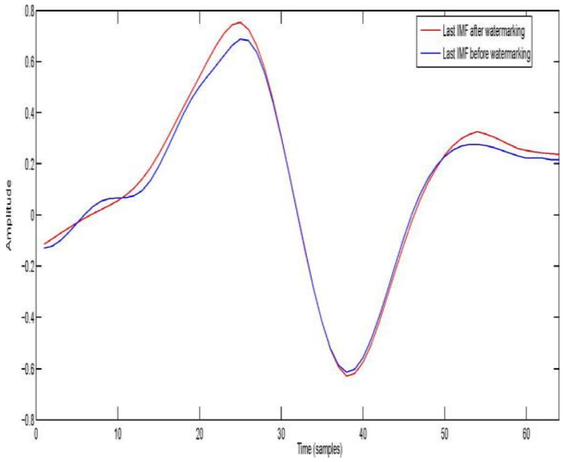

Fig 4. Last IMF of an audio frame before and after watermarking.

Step 4: Extract mi* from ei* using the following rule

$$m_i^* = \begin{cases} 1 & \text{if } e_i^* - \lfloor e_i^*/S \rfloor \cdot S \geq \text{sgn}(S/2) \\ 0 & \text{if} e_i^* - \lfloor e_i^*/S \rfloor \cdot S < \text{sgn}(S/2) \end{cases} \quad (3)$$

Step 5: Set the start index of the extracted data, Y, to I=1 and Select L=N1 samples (sliding window size).
Step 6: Evaluate the similarity between the extracted segment V=Y (1: L) and bit by bit. If the similarity value is.≥ T, then is taken as the SC and go to Step 8. Otherwise proceed to the next step.
Step 7: Increase by 1 and slide the window to the next L=N1 samples and repeat Step 6.

Step 8: Evaluate the similarity between the second extracted segment'=Y (I+ N1+ N2;I+2 N1+ N2) and U bit by bit.
Step 9: I<-I+N1+N2, of the new value is equal to sequence length of bits, go to Step 10 else repeat Step 7.
Step 10: Extract the watermarks and make comparison bit by bit between thesemarks, for correction,and finally extract the desired watermark.Watermarking embedding and extraction processes are summarize.

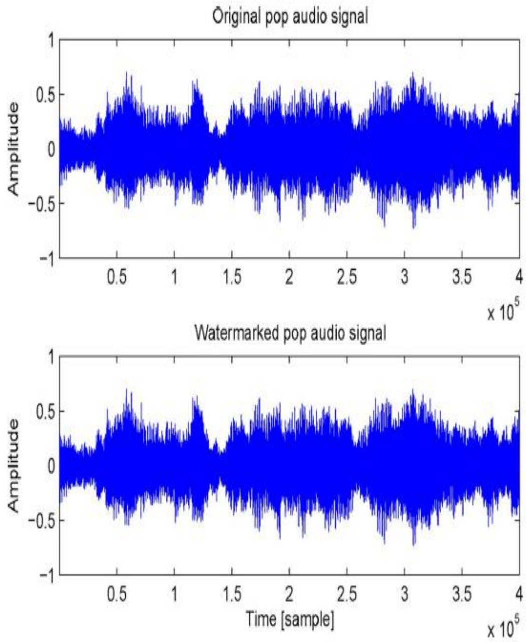

Fig.5. A portion of the pop audio signal and its watermarked version

RESULTS

Research and various experiments are being carried out in this subject to get the best possible results as mentioned in the below tables, simulations are performed on audio signals which include various types of music such as pop, jazz, rock and classic at the sampling rate of 44.1 kHz. The embedded watermark, is a binary logo image of size MXN=34X48=1632 bits .We convert this 2D binary image into a gray scale and then 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 T is set to 4. The 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. 5 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. The SNR values are above 20 dB showing the good choice of S value and confirming to IFPI standard.

A. Robustness Test

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

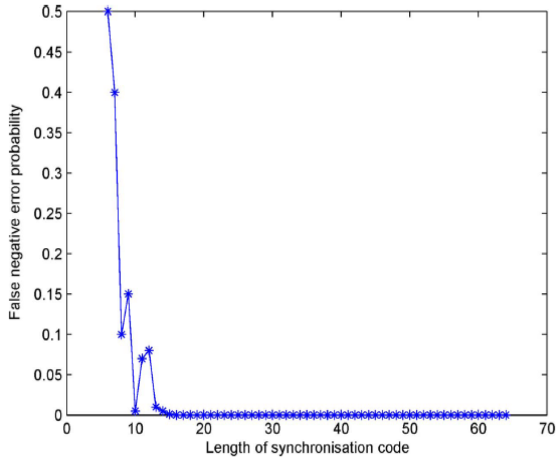

Fig 6. Synchronization code length

—**Noise**: White Gaussian Noise (WGN) is added to the watermarked signal until the resulting signal has an SNR of 20dB.
—**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.

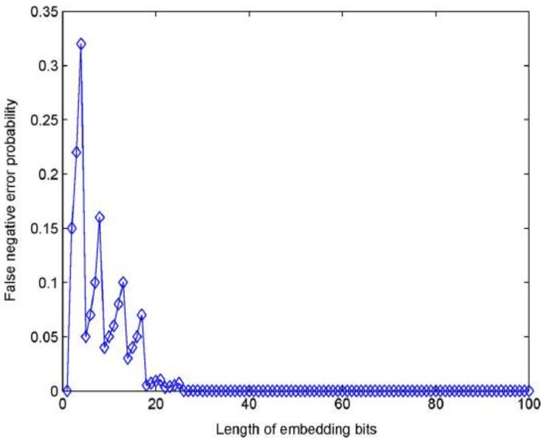

Fig. 7. Length of embedding bits

—**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) UsingMP3, 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 I shows the extracted watermarks with the associated NC and BER values for different attacks on pop audio signal. NC values are all above 0.9482 and most BER values are all below 3%. The extracted watermark is visually similar to the original watermark. These results show 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 detect any error. This is mainly due to the insertion of the watermark into IMFC extrema. In fact low frequency sub band has high robustness against noise addition. Table II reports similar results for classic, jazz and rock audio files.NC values are all above 0.9964 and BER values are all below 3%, demonstrating the good performance robustness of our method on these audio files. This is robustness is due to the fact that even the perceptual characteristics of individual audio files vary, the EMD decomposition adapts to each one.

Table I. Extracted Watermark For Pop Audio Signal By Proposed Approach

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

Table II. Extracted Watermark For Different Audio Signals (Classic, Jazz, Rock) By Our Approach

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

6.1 CONCLUSION

In this paper, we have given a glance of how the watermarking of audio will be done along with the possible results which will try to achieve which is far much better than any other watermarking scheme. A new water marking 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. EMD 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. Our watermarking method involves easy calculations and does not use the original audio signal. The experiments which will be conducted by us will have an embedding strength of S which will be kept constant for all audio files. To further improve the performance of the method, the 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. Moreover, the rapid growth of digital multimedia usage has resulted in serious concerns about the copy control and intellectual property protection. Thus, the goal is to make watermarking systems as secure as possible as well as maintaining the robustness of the watermarking schemes.

6.2 REFERENCES

1. Multipurpose audio watermarking algorithm Ning CHEN, Jie ZHU 2008
2. Audio Watermarking Based on PCM Technique Ranjeeta Yadav, Sachin Yadav, Jyotsna Singh 2010
3. Audio Watermarking: Features Applications and Algorithms Michael Arnold 2008
4. Audio Watermarking Using Wavelet Transform and Genetic Algorithm for Realizing High Tolerance to MP3 Compression 2011
5. Spread Spectrum Watermarking of Audio Signals 2003
6. Robust SVD-Based Audio Watermarking Scheme With Differential Evolution Optimization 2013
7. Robust Segments Detector for De-Synchronization Resilient Audio Watermarking 2012
8. Patchwork-Based Audio Watermarking Method Robust to De-synchronisation Attacks 2012
9. Discrete Wave Transform-Based Audio Watermarking 2011
10. A New Watermarking Scheme Based on Antipodal Binary Dirty Paper Coding 2011