

Performance Analysis and Study of Audio Watermarking Algorithms

Seethal Paul¹, Sreelakshmi T.G²

¹Adishankara Institute of Engineering and Technology, Mahatma Gandhi University,
kalady, kerala, India
seethu.paul@gmail.com

²Adishankara Institute of Engineering and Technology, Mahatma Gandhi University,
kalady, kerala, India
sreelakshmitg98@gmail.com

Abstract: Audio Watermark is a signature, embedded within the original signal, which should be inaudible to the human ear and resistant to any attempts to remove it. All audio watermarking schemes contain various parameters in common, in particular robustness, security, transparency, complexity, and capacity. This research work aims to devise a watermarking algorithm that improves the robustness, imperceptibility and speed without affecting the quality of the original host signal. In Echo hiding, the Signal to noise ratio obtained after watermark embedding is 15.3521 and the BER is 6.25%. For LSB coding, the SNR obtained for the watermarked signal is 33.8329 and the BER is obtained as 6.25%. For Chirp spread spectrum, the SNR obtained from simulation results is 32.9604 and the error rate obtained is 2.50%.

Keywords: - Audio watermarking , Chirp spread spectrum,
Robustness, Transparency, Performance analysis

1. Introduction

The rapid growth of the internet has greatly lead to the unauthorized distribution and hacking of digital media. The hacking of the digital systems is easier due to the availability of several processing platforms. As a result, the music industry suffers a multibillion dollar annual revenue loss due to piracy[1]. Thus a technique is needed for the security and protection of the digital data. Watermarking is a descendent of a technique known as steganography, which has been in existence since 1490. Steganography is a technique which is used for concealed communication. In contrast to cryptography where the content of the message is a secret, in steganography the very existence of the message is a secret and only parties involved in the communication know its presence. Steganography is a technique where a secret message is hidden within another unrelated message and then communicated to the other party[2]. The secret communication between the transmitter and the receiver plays a major role in militaries, radar and wireless communication .

Watermarking provides secrecy to the communication between them. Watermarking can be considered as a special technique of steganography where one message is embedded in another and the two messages are related to each other in some way[2]. The most common examples of watermarking are the presence of specific patterns found in currency notes, which are visible only when the note is held to light, and logos in the background

of printed text documents. The watermarking techniques prevent forgery and unauthorized replication of physical objects.

In digital watermarking a low energy signal is imperceptibly embedded in another signal. The low energy signal is called the watermark and it depicts some information like security or rights information about the main signal[3]. The main signal in which the watermark is embedded is referred to as the cover signal since it covers the watermark. The cover signal can be generally a still image, audio clip, video sequence or a text document in digital format.

The digital watermarking system essentially consists of a watermark embedder and a watermark detector. The watermark embedder inserts a watermark into the cover signal and the watermark detector detects the presence of watermark signal. An entity called the watermark key is used during the process of embedding and detection of watermarks. The watermark key has a one-to-one correspondence with the watermark signal which means that there exists a unique watermark key for every watermark signal[4]. The watermark key will be known only to the authorized parties and thus it ensures that only the authorized parties can detect the watermark. The communication channel can be noisy and hostile and may be prone to attacks and hence the digital watermarking techniques should be resistant to both noise as well as security attacks.

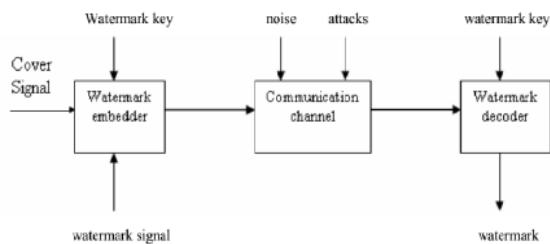


Figure 1: Block Diagram of Digital watermarking system

Security is defined as the degree of protection against danger, damage, loss, and criminal activity. When a sensitive message is to be delivered to a destination, authentication and confidentiality are required. Providing security for electronic documents is a major issue. Digital watermarking has to embed pieces of information into a digital media for protecting it against copyright infringements and other unauthorized applications.

A lot of works has been done on digital watermarking of various media such as image and video, but this particular work will focus on digital watermarking of audio file. Inaudible watermarks are made possible by exploiting characteristics of the Human Auditory System (HAS). Audio watermarking is especially challenging as compared to image watermarking because the HAS is far more sensitive than the visual system. Human ear is much more sensitive than other sensory organs [16]. If a signal is maintained below the threshold of sensitivity, then the watermark will be inaudible. Above 2 kHz, the HAS focuses more on the temporal envelope of an audio signal than the actual structure [17]. Thus, small changes in the spectrum above 2 kHz are less likely to be noticed by a human listener.

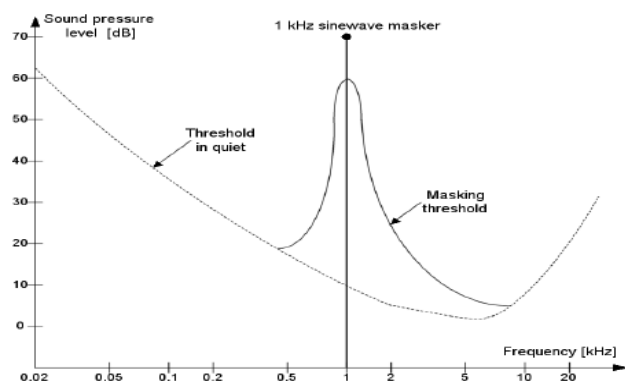


Figure 2: Frequency masking in the human auditory system (HAS), reference sound pressure level is $p_0 = 2 \times 10^5 \text{Pa}$:

2. Literature Survey

There are three main stages in the watermarking process :

- Generation and Embedding :
- Attacks :
- Detection :

The generation of watermarks is an important stage of the watermarking process. The information contained within the watermark must be unique otherwise the owner cannot be identified uniquely [4]. In embedding process, an algorithm accepts the host audio signal and the information to be embedded and finally produces the watermarked signal. In the watermark embedding block, a private key is used to create an inaudible watermark on the audio file [2]. This private key is used to encode the digital watermark into the original

file. Later, the owner can examine whether a given audio file, which is suspected for being illegally copied, contains his or her own watermark and can use it as a legal proof. In the watermark detector block, the same key is used.

2.1 Watermark Insertion and Extraction

- Watermark Insertion:

There are four main steps for inserting a digital watermark into an audio file. First an original audio file is fed into the system in wave format which is then subsequently framed, analysed and processed to attach the inaudible watermark into the output signal.

- Framing

The original host audio signal is partitioned into frames. The frame size is chosen so that the watermark that is embedded does not introduce any audible distortion into the file.

- Spectral Analysis

After the framing of the unprocessed audio signal, the spectral analysis of the signal is performed consisting of a Fast Fourier Transform (FFT) which allows the calculation of low frequency components of each frame as well as the overall frame power.

- DC Removal

From the above spectral analysis of each frame, the low frequency (DC) component $F(1)$, is calculated which can be removed by subtraction from each frame.

- Watermark Signal Addition

From the spectral analysis completed, the spectral power for each frame is calculated, which is now utilised for embedding the watermark signal data. The power in each frame determines the amplitude of the watermark which can be added to the low frequency spectrum.

- Watermark Extraction

The process of extracting the digital watermark from the audio file is similar to the technique for inserting the watermark. A marked audio file in wave format is fed into the system, where it is then framed, analysed, and processed, to remove the embedded data which exists as a digital watermark in the signal.

2.2 Characteristics of Audio Watermarking

A number of requirements have to be satisfied for a scheme to fulfill the purposes of watermark. The most important requirements are perceptibility, reliability, capacity and speed performance.

Perceptibility

The quality of the original signal has to be retained after the introduction of watermark [2]. This is meant by perceptibility of the system. The watermark cannot be detected by listeners.

Robustness

A digital watermark is called robust if it resists a designated class of transformations. Robust watermarks may be used in copy protection applications.

Reliability

Reliability is determined by the robustness and detection rate of the watermark. A watermark has to be robust against intentional and unintentional attacks. The detection rate of watermark should be perfect to determine if the watermarked signal has been attacked or not [4]. The attacks on the audio files include digital-to-analog, analog-to-digital conversions, noise addition, band-pass filtering, time-scale modification, addition of echo and sample rate conversion. If the quality of the watermarked signal after the attacks is not significantly

distorted, the watermark should not be removed by these attacks.

Capacity

The amount of information that can be embedded into a signal is also an important issue. A user has to be able to change the amount embedded to suit different applications.

Speed

Watermarking may be used in real-time applications, such as audio streaming. The watermark embedding and extracting processes have to be fast enough to suit these applications.

Secret keys

Secret keys are essential for security issues and are included in many watermarking systems to protect the watermark information from undesirable alterations or even removal. There are two kinds of secret keys: unrestricted-keys and restricted keys. Unrestricted-keys are those in which the same key is known and used in different watermarks, whereas restricted-keys are used only in a specific watermark [4].

3 Applications of Digital Watermarking

Digital watermarking techniques have wide range of applications. Some of the applications are listed below:

Copy protection:

Digital content can be watermarked to indicate that the content be illegally replicated. Devices capable of replication can then detect such watermarks and prevent unauthorized replication of the content.

Tracking:

Digital watermarks can be used to track the usage of digital content. Each copy of digital content can be uniquely watermarked with metadata specifying the authorized users of the content [3]. Such watermarks can be used to detect illegal replication of content by identifying the users who replicated the content illegally. The watermarking techniques used for tracking is called fingerprinting.

Broadcast monitoring:

Digital watermarks can be used to monitor broadcasted content like television and broadcast radio signals. Advertising companies can use systems that can detect the broadcast of advertisements for billing purposes by identifying the watermarks broadcast along with the content [1].

Tamper proofing:

Digital watermarks, that are fragile, can be used for tamper proofing. Digital content can be embedded with fragile watermarks that get destroyed when any sort of modification is made to the content. Such watermarks can be used to authenticate the content.

4 Attacks on the watermarked signal

4.1 Synchronization

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. Synchronization is the key issue during watermark extraction process especially when the host audio is manipulated by desynchronizing attack [6].

4.2 Noising and de-noising

Noising attacks are usually performed by white gaussian noise addition on vertex coordinates. De-noising is usually performed by Laplacian smoothing.

4.3 Topological attacks

Topological attacks are complex attacks which may change the topological features of the audio signal. (topological refers to shape topology). Cropping is the most well-known attack of this class. Most cropping attacks significantly degrade the shape but some of them preserve important parts of the shape that should also be protected.

4.4 Resampling

In the resampling attack, the original sampling frequency of the watermarked audio is changed to a lower frequency. This results in a decrease in the bandwidth of the audio signal. Therefore, if the watermark is already embedded in the high frequency components of the audio signal, the watermark can be destroyed. The original audio signals were sampled with a sampling rate of 44.1 kHz [5]. The sampling rate of the watermarked audio data was reduced to 22.05 kHz and resampled to the original rate of 44.1 kHz. This causes audible distortions especially in audio tracks carrying high frequencies.

4.5 Low Pass Filtering

Low pass filtering, one of the most common attacks performed on watermarked audio files, removes the high frequency component of the audio signal.

4.6 AWGN Attack

Information Theory states that the Gaussian noise [5] is the worst-case additive noise in point to-point channels, means that, for a fixed noise variance, the Gaussian noise minimizes the capacity of an additive noise channel. The Gaussian noise is the worst-case noise in wireless networks.

4.7 Requantization

The standard quantization bit length for CD quality of audio (music) is 16 bit. In requantization attack, the quantization bit length of audio is decreased to values as small as 8 bit. Requantization process decreases the dynamic range of the audio samples without modifying the overall shape and the frequency specification of the audio signal. Audio tracks sampled at 8-bit are often used in games and multimedia applications. We therefore tested the process of requantization of a 16-bit watermarked audio signal to 8-bit and back to 16-bit. This increases the incoherent background noise of the audio track due to the rounding errors during the processing.

4.8 Cropping:

A portion of the audio file is undergone cutting and this may destroy the watermark and sometimes this may create distortions in the audio file. In audio watermarking this is one of the serious issues which must be taken into consideration.

5 Performance And Evaluation Criteria

Performance of the audio watermarking algorithm is evaluated with respect to the robustness and the imperceptibility (inaudibility/clearness).

5.1 Robustness

A digital watermark is called robust if it resists a designated class of transformations. Robust watermarks may be used in copy protection applications to carry copy and no access control information.

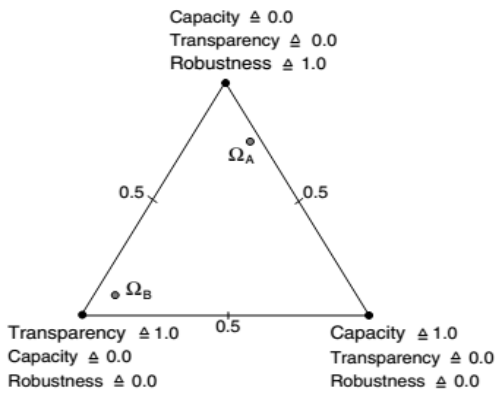


Figure 3: Performance Parameters of Watermark [7]

5.2 Bit Error Rate

Bit error rate can be defined as the percentage of bits corrupted in the transmission of digital information due to the effects of noise, interference and distortion. For example, the bits to be transmitted are 11001100 and the received bits are 10000100. Comparing the number of bits transmitted to received, two bits are affected by transmission. Hence, the BER in this example is $2/8 \times 100 = 25$

$$BER = E/P \times Q \text{ } 100\% \quad (1)$$

E is the number of erroneous bits of the watermark (picture) during the retrieval process. BER expresses the difference between the watermark bits embedded in the host audio signal, and the watermark bits extracted at the receiver side. P x Q is the binary watermark size.

$$BER = 100/B \sum_{b=0}^{B-1} \{ \text{if } 1, w(\sim n) \neq w(n); \text{ if } 0, w(\sim n) = w(n) \} \quad (2)$$

5.3 Imperceptibility

In any audio watermarking method, inserting watermark information introduces a small amount of distortion to the host audio signal. Therefore, the quality (clearness) of the watermarked audio can be used as another criterion for evaluating the performance of audio watermarking algorithms[5]. This can be evaluated by listening test and calculating the PSNR of the watermarked signal.

5.4 Signal to Noise Ratio

Signal to noise ratio is a parameter used to know the amount by which the signal is corrupted by the noise. It is defined as the ratio of the signal power to the noise power. Alternatively, it represents the ratio of desired signal (say a music file) to the background noise level[6]. SNR can be calculated by equation below.

$$SNR = \text{Signal power} / \text{Noise power}$$

refers to the amount of noise that the algorithm adds to the audio signal. In this A represents an N -sample audio signal while A is the watermarked version of that signal.

5.5 Bit Rate

The amount of watermark data that maybe reliably embedded within a host signal per unit of time .A higher bit rate may be desirable in some applications in order to embed more copyright information. Reliability is measured as the bit error rate (BER) of extracted watermark data.

5.6 Perceptual Quality

In most applications, it is important that the watermark is undetectable to a listener This ensures that the quality of the host signal is not perceptibly distorted, and does not indicate the presence or location of a watermark. In this study, the signal-to-noise ratio (SNR) of the watermarked signal versus the host signal was used as a quality measure or viewer.

5.7 Computational Complexity

Computational complexity refers to the processing required to embed watermark data into a host signal, or to extract the data from the signal. It may influence the choice of implementation structure or DSP architecture.

5.8 Transparency of the attacked signals

Given a reference object Sref and a test object Stest the transparency function T provides a measure of the perceptible distortion between Sref and Stest[7]. Without loss of generality, such a function may take values in the closed interval [0,1] where 0 provides the worst case. The signals Sref and Stest are so different that Stest cannot be recognized as a version of Sref and 1 is the best case (an observer does not perceive any significant difference between Sref and Stest):

$$T(\text{Sref}; \text{Stest}) \longrightarrow [0; 1]$$

In case of signal to noise ratio (SNR) measures, the transparency function can be chosen as follows[7]:

$$SNR(\text{Sref}, \text{Stest}) = \max(0, 10 \log_{10} SNR(\text{Sref}, \text{Stest})) \quad (3)$$

The transparency can be obtained from SNR as the following equation:

$$T_{SNR}(\text{Sref}, \text{Stest}) = 1 - \exp(-k \times SNR(\text{Sref}, \text{Stest})) \quad (4)$$

where k is some positive constant which can be chosen to provide an appropriate scale. choose k =0.075 [7].

6. Study and Analysis of Existing Systems-Audio Watermarking Algorithms

There are several audio watermarking techniques based on their applications. The main difference among them depends on the purpose they are created for. The main challenge that the audio watermarking systems face is that the human auditory system has a very wide range and it is very sensitive to noise. The watermark should be inserted in such a manner that it should be undetectable. In order to accomplish this various watermarking algorithms are proposed and these algorithms consist of two crucial processes-watermark embedding and its detection.

6.1 Lowbit Encoding [8]

This technique is one of the earliest techniques in the area of audio watermarking. Data hiding in the least significant bits (LSBs) of audio samples in the time domain is one of the simplest algorithms with very high data rate of additional information. The LSB watermark encoder usually selects a subset of all available host audio samples chosen by a secret key[8]. The substitution operation on the LSBs is performed on this subset, where the bits to be hidden substitute the original bit values. Extraction process simply retrieves the watermark by reading the value of these bits from the audio. LSB watermarked signal is extremely sensitive to signal

manipulations. Also, the random selection of the samples used for embedding introduces low power additive white Gaussian noise (AWGN).

6.2 Echo hiding [9]

This algorithm adds an echo on continuous blocks of the cover medium to embed a secret bit, i.e., adding a delayed version with d_1 samples of the original audio, this is to embed a binary '1' and to add a delayed version with d_2 samples of the original audio this is to embed a binary '0'. The original audio is partitioned into blocks of size 'N', where 'N' is the number of bits of the watermark [9]. Each block is subjected to a comparison with the bit you want to hide, if it is '1' is adhered to a delayed version of d_1 samples from the same block and with an amplitude, but if that bit is a '0' is adhering a delayed version of d_2 samples of the same block and an amplitude.

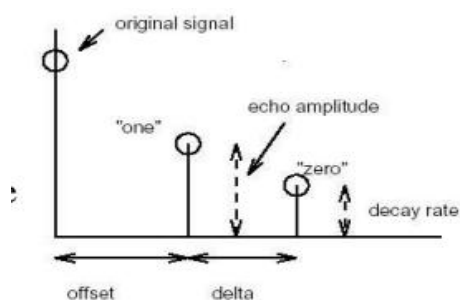


Figure 4: Kernals for Echo hiding [9]

6.3 Phase Coding [8]

Phase Coding watermarking works by substituting the phase of an initial audio segment with a reference phase, this phase represents the hidden data. The phase of subsequent segments is adjusted in order to preserve the relative phase between segments.

The major advantage of Phase Coding is that it is more robust technique than LSB. The major disadvantage is that the method is, Phase coding method is a low payload technique because the watermark embedding can be only done on the first block. The watermark is not dispersed over the entire data set available, but is implicitly localized and can thus be removed easily by the attackers.

6.4 DWT Based Audio Watermarking [10]

This algorithm is based on applying the Discrete Wavelet Transform (DWT) on the digital audio signal in which a watermark is to be embedded. The algorithm consists of two procedures; watermarking embedding procedure and watermarking extraction procedure. Wavelets are special functions which, in a form analogous to sines and cosines in Fourier analysis, are used as basal functions for representing signals [10]. They provide powerful multi resolution tool for the analysis of non-stationary signals with good time localization information. The embedding procedure performs three major operations; watermark pre-processing, DWT based frequency decomposition of the audio signal, and watermark embedding in the DWT-transformed audio signal. The watermark extraction procedure enables the owner of the audio clip to extract the embedded watermark. The procedure requires knowledge of the original audio file, the watermark intensity, and the size of the watermark, in order to extract the watermark. The watermark extraction steps are a direct reversal of steps carried out in the embedding procedure.

6.5 Audio watermarking via Empirical Mode Decomposition [13]

Empirical Mode Decomposition (EMD) is a new adaptive audio watermarking algorithm for non-linear and non-stationary time series data. The audio signal is divided into frames and each one is decomposed adaptively, by EMD, into Intrinsic Mode Functions (IMFs) and finally there will be residual [13]. IMFs are intrinsic oscillatory components. The watermark and the synchronization codes are embedded into the extrema of the last IMF, a low frequency component which will be stable under different attacks and preserving the quality of the host signal. Low frequency components such as higher order IMFs are signal dominated. Watermarks inserted into high frequency IMFs are most vulnerable to attacks.

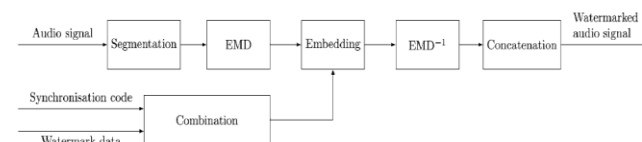


Figure 5: watermark embedding [13]



Figure 6: watermark extraction [13]

6.7 Spread Spectrum Technique [11]

The main idea is to embed a narrow-band signal (the watermark) into a wideband channel (the audio file). Spread spectrum techniques protect the watermark privacy by using a secret key to control the pseudorandom sequence generator. Spread spectrum techniques allow the frequency bands to be matched before embedding the message. Spread Spectrum is a technique in which a signal is transmitted on a bandwidth considerably larger than the frequency of the original information. In this technique, the bit of secret information spreads over the audio frequency spectrum. It requires different code for encoding as well as decoding of hidden information. It is more immune to noise [12].

6.8 Chirp Spread Spectrum Audio Watermarking [14]

In this technique a CHIRP signal is used instead of a pseudo random noise producer. Chirp, is one of spread spectrum techniques which embed CHIRP signal in an audio signal and CHIRP signal can be used as a common key between the sender and the receiver. High robustness and imperceptibility of created watermark by this method will lower the possibility to recognize and identify the original signal [15]. This method has significant qualities in comparison with other methods, hence we use this method to embed the audio files. These qualities are like: low power consumption, low delay, high security, imperceptibility and etc., which can be used in military applications. The watermarked signal is transferred all over the canal so that the adversary is not able to identify the audio signal which is being transferred between the sender and the receiver.

7. Existing System-Simulation Results

A. Echo hiding:

The basic idea is to embed a watermark by adding an echo to the original sample. And the watermark is hidden within the echo produced. The watermark is embedded by generating an echo of

the original audio sample. The signal is sampled at 44.1 kHz, represented by 16 bits per sample, and ten seconds in length. The watermarked signal is written into another file. When that watermarked signal is undergone listening test, we hear a noisy signal which means the quality of the echo hidden watermarked signal is very low. Steps: First the original audio file is read as a wave file. The watermark used here is a binary signal ie, [1 1 1 1 0 0 0 0] which is the information that is hidden within the echo. Now the length of both the audio file and the watermark is determined. Echo is generated from the input signal and is added along with the input if it is 1. And if it is 0, then nothing is added with the input signal. Now the marked signal is written into another file. Attacks on watermarked signal: The watermarked signal is undergone attacks like filtering, cropping, resampling, requantisation and addition of noise. But, resampling and addition of noise fails. Only the filtered signal survives and we can extract the watermark from the filtered signal.

Table 1: The watermark detection after attacks

Types of attacks	Retrieved watermark
Filtering	1 1 1 1 0 0 0 0
Addition of noise	1 1 1 1 1 1 1 1
Resampling-downsampling	1 1 1 1 0 0 0 0
Resampling- upsampling	0 0 0 0 0 0 0 0
Requantisation	1 1 1 1 1 1 1 1
Cropping	1 1 1 1 1 1 1 1

The Signal to noise ratio obtained before attacks is 15.3521 and the BER is 6.25%. After attacks the average SNR obtained is 14.123 and the average error rate is 7.63%.

B. LSB coding

LSB coding is one of the earliest techniques studied in the information hiding and watermarking area of digital audio. Data hiding in the least significant bits (LSBs) of audio samples in the time domain is one of the simplest algorithms with very high data rate of additional information. The LSB watermark encoder usually selects a subset of all available host audio samples chosen by a secret key. The substitution operation on the LSBs is performed on this subset, where the bits to be hidden substitute the original bit values. Extraction process simply retrieves the watermark by reading the value of these bits from the audio. Therefore, the decoder needs all the samples of the audio that were used during the embedding process. In LSB coding, the following steps are done to embed the watermark: 1) Get the audio source wav 2) Divide the audio source into pieces for 256 points per pieces. 3) Quantized all points 5) DCT transfer 6) Produced watermark 7) embedded watermark.

Several attacks like Filtering, Resampling, Requantisation, Noise Addition, and Cropping are performed and corresponding SNR, BER and Transparency in each case is calculated. In literature the SNR obtained is 67.90 and the BER is 4.90% and the SNR obtained for the watermarked signal is 33.8329 and the BER is obtained as 6.25%

Table 2: Attacks on LSB coding

ATTACKS	SNR	BER
Requantisation	0.5295	0.0925
Filtering	33.8329	0.0875
Addition of noise	9.0678	0.0975

Cropping	0.5295	0.0975
Resampling	0.5295	0.0975

C. Chirp coding, Decoding and Watermarking

The coding process is compounded in the following basic steps:

- 1) Read a .wav file.
- 2) Extract a section of a single vector of the data (note that a .wav contains stereo data, i.e. two vectors arrays).
- 3) Apply wavelet decomposition using Daubechies wavelets with 7 levels. Note that in addition to wavelet decomposition, the approximation coefficients for the input signal are computed to provide a measure on the global effect of introducing the watermark into the signal. Thus, 8 decomposition vectors in total are generated.
- 4) Compute the (percentage) energy values.
- 5) Round to the nearest integer and convert to binary form.
- 6) Concatenate both the decimal and binary integer arrays.
- 7) Chirp code the binary sequence
- 8) Scale the output and add to the original input signal.
- 9) Re-scale the watermarked signal.

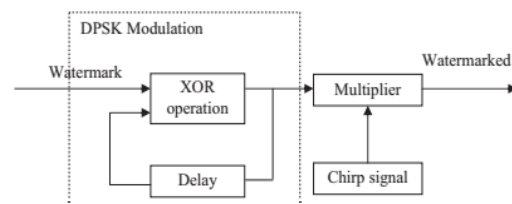


Figure 7: Block diagram of chirp spread spectrum audio watermarking transmitter.

The decoding process is as follows:

- 1) Steps 1-6 in the coding processes are repeated
- 2) Correlate the data with a chirp identical to that used for chirp coding.
- 3) Extract the binary sequence
- 4) Convert from binary to decimal.
- 5) Display the original and reconstructed decimal sequence
- 6) Display the error.

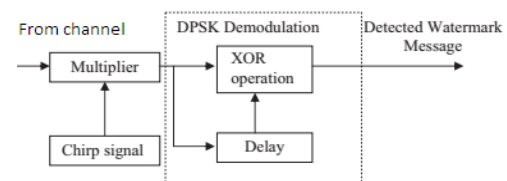


Figure 8: Block diagram of chirp spread spectrum audio watermarking receiver

Performance analysis of the audio watermarking using CSS: Here we have chosen four types of attacks, like: requantisation, filtering, noise addition and cropping. It is obvious that BER is less than 4% and SNR more than 30. The SNR obtained from simulation results is 32.9604 and the error rate obtained is 2.50% which is also very less. The average SNR after attacks is obtained as 21.925 and the average error rate obtained after attacks is 8.06%.

Table 3: Attacks on CSS watermarking

ATTACKS	SNR	BER
Requantisation	32.1819	0.02
Filtering	32.9064	0.090
Addition of noise	8.6044	0.25
Cropping	0.5295	0.02

Resampling	35.8837	0.023
------------	---------	-------

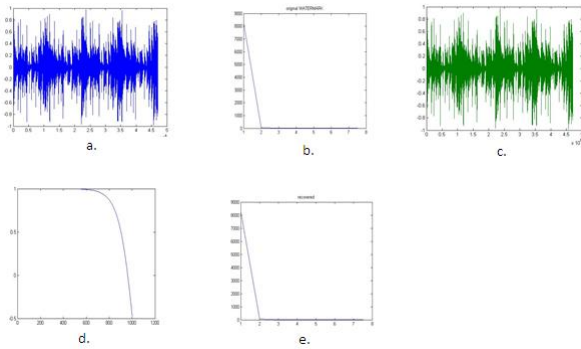


Figure 9. a. The original audio signal b. The watermark c. The watermarked signal d. The chirp signal

8. Performance Analysis of the Algorithms

Performance of the audio watermarking algorithm is evaluated with respect to the robustness and the imperceptibility[7] (inaudibility/clearness). There is a trade off between transparency, capacity and robustness. Transparency ranges between two values 0 and 1. A digital watermark is called robust if it resists a designated class of transformations. Bit error rate can be defined as the percentage of bits corrupted in the transmission of digital information due to the effects of noise, interference and distortion.

Table 4. CPU timings of the three algorithms

Algorithm	Total Time(sec)
Echo hiding	0.236
LSB Coding	4.8945
CSS	1.805

Table 5: consolidated summary of the simulation results

Algorithm	Robustness	Imperceptibility	Transparency
Echo hiding	15.3521	0.625	0.0638
LSB Coding	33.8329	0.625	0.9209
CSS	32.9064	0.002	0.9152

Table 6. SNR values of the three algorithms for various attacks

ATTACKS	Echohiding(SNR)	LSB(SNR)	CSS(SNR)
Requantisation	15.3211	0.5295	32.1819
Filtering	15.3521	33.8329	32.9064
Addition of noise	9.0745	9.0678	8.6044
Cropping	15.5152	0.5295	0.5295
Resampling	15.3521	0.5295	35.8837

Table 7. Transparency of the attacked signals

ATTACKS	Echohiding (Transparency)	LSB (Transparency)	CSS (Transparency)
Requantisation	0.6831	0.0389	0.9105
Filtering	0.6838	0.9209	0.9152
Addition of noise	0.4937	0.4934	0.4755
Cropping	0.6877	0.0389	0.0389
Resampling	0.6838	0.0389	0.9322

9. Proposed System

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[13]. A major advantage of EMD relies on no a priori choice of filters or basis functions and can be used instead of Discrete wavelet transform in the CSS algorithm so that external modifications can be corrected automatically within the system.

10. Conclusion

The audio watermarking is a domain of very vast research. Here three algorithms Echo hiding, LSB coding and Chirp spread spectrum are tested for watermarking of the audio signal. In Echo hiding, the Signal to noise ratio obtained after watermark embedding is 15.3521 and the BER is 6.25% and average transparency is 64.64%. For LSB coding, the SNR obtained for the watermarked signal is 33.8329 and the BER is obtained as 6.25% and average transparency is 30.62%. For Chirp spread spectrum, the SNR obtained from simulation results is 32.9604 and the error rate obtained is 2.50% and average transparency is 65.44%. But the problem is that, the algorithms don't meet the tradeoffs i.e., though the LSB algorithm meets transparency and capacity, it doesn't meet robustness. Echo hiding meets transparency but it doesn't meet capacity and robustness. And, Chirp spread spectrum meets robustness and transparency but it doesn't meet capacity. So this system can be enhanced if the decomposition method is replaced by Empirical mode decomposition.

ACKNOWLEDGMENT

First of all, I thank Almighty for His enlightening presence and blessings throughout my life and for helping me to complete this project work successfully. I would like to take this opportunity to thank all those who have contributed to this project.

References

- [1] Michael Arnold, "Audio watermarking: features, applications and algorithms" and Expo., ICME 2000 IEEE International Conference vol. 51, 2000
- [2] Paraskevi Bassia, Ioannis Pitas, Senior Member, IEEE, and Nikos Nikolaidis, Associate Member, "Robust audio watermarking in time domain" Can. J. Elect. Comput. Eng Vol. 33, No. 3/4, Summer/Fall 2008.

- [3] Goenka and M.P.K Patil "Overview of audio watermarking techniques" International Journal of Emerging Technology and Advanced Engineering Website: www. ijetae.com (ISSN) 2250-2459., p. 353, February 2012
- [4] K.JaralaneKirubavathy,"Copyright protection using digital audio watermarking- an overview,"International Journal of Computer Science And Applications, vol. 6, Apr 2013
- [5] J. D. Gordy and L. T. Bruton "Performance evaluation of digital audio watermarking algorithms" Circuits and Systems, 2000. Proceedings of. 43rd IEEE Midwest Symposium, vol. 28, 2010
- [6] J.E.Vila-Forcen,"Quantization- based method Additive attacks performance analysis", Transactions on DHMS III, LNCS 4920.
- [7] Jana Dittmann,David Megas, Andreas Lang,andJordi Herrera- JoancomartI, "Theoretical framework for a practical evaluation and comparison of audio watermarking schemes in the triangle of robustness, transparency and capacity",Vol. 26, No. 3/4 IEEE transactions on medical imaging march 2007.
- [8] G. Prof .Samir Kumar, Bandyopadhyay Barnali, "Lsb modification and phase encoding technique of audio steganography revisited," International Journal of Advanced Research in Computer and communication Engineering, 2012.
- [9] Dolores Z. Saavedra Juan A. R. Chvez, Carlos A . Ruiz," Programmable logic implementation of echo hiding for Audio watermarking ," Journal of Theoretical Applied Information Technology,pp. 135 - 138 January 2013.
- [10] A. Mohammad and L. Bata," DWT based audio watermarking" Int. Arab J Inf. Technol., - idc-online .com 2011.
- [11] A. Nedeljko Cvejic, Tapio Sepp"Spread spectrum Audio Watermarking using frequency hopping and attack characterization",journal,signal processing archive,January 2004
- [12] D . Kirovski and I. Henrique S. Malvar, Fellow, " Spread-spectrum watermarking of audio signals " IEEE Transactions on signal processing vol.51, APRIL 2003
- [13] K. Khaldi and I. Abdel - Ouahab Boudraa Senior Member " Audio watermarking via EMD ," IEEE Transactions on audio, speech, and language processing, vol. 21, MARCH.
- [14] Jonathan M Blackledge Fellow ,IET,"Digital watermarking and self authentication using chirp coding" Transactions on electronics and signal processing, 2007
- [15] Karthigaikumar ,P.Baskaran,K. Kirubavathy, K.J." Hard Ware implementation of audio watermarking communication"IEEE Transaction on Medical Imaging vol.24nov
- [16] S. Kuo et al., "Covert Audio Watermarking Using Perceptually Tuned Signal Independent Multiband Phase Modulation," IEEE International Conference on Acoustics, Speech, and Signal Processing, vol. 2, pp. 1753-1756, May 2002.
- [17] P. Noll, "MPEG Digital Audio Coding," IEEE Signal Processing Magazine, vol. 14(5), pp. 59-81, Sep. 1997

Author Profile

1. SEETHAL PAUL



PG Scholar at Adishankara Institute of Engineering and Technology, Kerala,India specialised in VLSI and Embedded System in the year 2012-2014.Done Graduation at METS School of Engineering,Kerala,India, specialised in Electronics and Communication from 2008-2012 .

2. SREELAKSHMI.T.G



PG Scholar at Adishankara Institute of Engineering and Technology,Kerala,India specialised in VLSI and Embedded System in the year 2012-2014.Done Graduation at Matha College of Technology,Kerala,India specialised in Electronics and Communication from 2008-2012.

