A Havoc Proof For Secure And Robust Audio Watermarking

K.Vaitheki email: vaidehi.balaji@gmail.com
Assistant professor, Department of Computer Science
Pondicherry University
Puducherry, India - 605014

R.Tamijetchelvy email:narendra_naren_lucky@yahoo.co.in
Assistant professor, Department of Electronics and communication
Perunthalaivar Kamarajar institute of Technology,Karaikal
Puducherry, India – 605107

Abstract

The audio watermarking involves the concealment of data within a discrete audio file. Audio watermarking technology affords an opportunity to generate copies of a recording which are perceived by listeners as identical to the original but which may differ from one another on the basis of the embedded information. A highly confidential audio watermarking scheme using multiple scrambling is presented Superior to other audio watermarking techniques; the proposed scheme is self-secured by integrating multiple scrambling operations into the embedding stage. To ensure that unauthorized detection without correct secret keys is nearly impossible, the watermark is encrypted by a coded-image; certain frames are randomly selected from the total frames of the audio signal for embedding and their order of coding is further randomized. Adaptive synchronization is improves the robustness against hazardous synchronization attacks, such as random samples cropping/inserting and pitch-invariant time stretching. The efficient watermarking schemes make it impossible to be detected and robust even though the watermarking algorithm is open to the public.

Keywords: Audio watermarking, Information hiding, Copyright protection, Multiple Scrambling.

1. INTRODUCTION

The digital media have opened the door to an information marketplace where the true value of the product (digital content) is dissociated from any particular physical medium. It also enables a greater degree of flexibility in its distribution and a lower cost, the commerce of disembodied information raises serious copyright issues. Indeed, digital data can be duplicated and re-distributed at virtually no cost, potentially turning piracy into a simple "click and drag" process. Cryptography has been clearly established as a technology of fundamental importance for securing digital transfers of data over unsecured channels. By providing encryption and authentication of digital data, cryptography enables trustworthy point-to-point information exchange and transactions to be achieved. Hence, once the recipient validates and decrypts the data, the product can be subsequently stripped from any content identification, proof-of-

ownership or other descriptive information and any further duplication and re-distribution can leave the rights holders powerless and royalty-less. While such re-distributions may not represent a serious threat when the content consists of proprietary information that has a short life span, such piracy could have catastrophic implications for the entertainment industry, whose content has a very long life span.

Cryptography provides an easy way to see how digital sub-codes and other proprietary digital formats can fail in similar ways, since they are only volatile representations of a medium. The true value of the product (the content) can still be transferred effortlessly onto different formats and media. Any attempt to secure the identities of content's rights holder's calls for a technology that enables some secure auxiliary information, or watermark, to travel with the content through any channel, format or medium where the content's value remains. A properly designed audio watermarking technology provides the means to do this in the context of audio content, while preserving the integrity of the original recording. Unlike sub-codes, encryption or audio compression, a watermark should not rely on any specific format. In order to travel along with the content it protects, the watermark must be carried by the content itself. Embedding a watermark is an active modification of the audio waveform. Subsequent to this process, the watermarked content becomes a message carrier regardless of the format of medium it lives on.

2. SCOPE OF AUDIO WATERMARKING

Digital watermarking is techniques of embedding information into a signal. The host signal that carries the watermark is also called a cover signal. When the cover signal is an audio signal, the embedding technique is called audio watermarking. The purposes, types and requirements of audio watermarking are presented after the research.

Purposes

There are various purposes for audio watermarking. The original intention of watermarking is for copyright protection. he most obvious purposes are the needs for proof of ownership and the enforcement of usage policy. In addition, watermarking can also be used for fingerprinting and additional features to a media

Proof of Ownership

A watermark can represent a code of information to identify the owner of a digital signal. This application is similar to the function of international standard book number (ISBN) for book identification. The watermark must be correctly presented to proof an ownership in a court of law.

Enforcement of Usage Policy

Watermark can be used to provide copyright information to consumer devices. The usage of audio information will be limited or stopped by the devices if certain requirement is not fulfilled by the user. However, this function of watermark has posted a difficulty in actual application. This is because in order for a consumer device to recognize a watermark, the watermark or the secret key for watermark generation has to be kept by the device. Attackers can use reverse engineering to obtain the watermark or disable the watermark verifying function in a device.

Fingerprinting

The usage of an audio file can be recorded by a fingerprinting system. When a file is accessed by a user, a watermark, or called fingerprint in this case, is embedded into the file. The usage history can be traced by extracting all the watermarks that were embedded into the file.

Additional Features

A watermark can also provide additional information to a file. For instance, the lyrics can be embedded into a song and extracted when it is played. Furthermore, the watermark can be a special label for convenient search function in databases.

3. REQUIREMENTS OF A WATERMARK

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

Perceptibility

The most important requirement is that the quality of the original signal has to be retained after the introduction of watermark. A watermark cannot be detected by listeners.

Reliability

Reliability involves 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 whether the watermarked signal has been attack or not. Otherwise, the watermark extracted is not useful for proof of ownership. Secure digital music initiative (SDMI), an online forum for digital music copyright protection, has summarized a list of possible attacks to evaluate the robustness of watermarking schemes. These attacks include digital-to-analog, analog-to-digital conversions, noise addition, band-pass filtering, time-scale modification, addition 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. An example can be seen in real-time application. If a watermark is spread across an audio signal, the complete signal has to be presented first. This is not possible in streaming over the Internet.

Speed

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

4. TYPES OF AUDIO WATERMARKS

Audio watermarks are special signals embedded into digital audio. These signals are extracted by detection mechanisms and decoded. Audio watermarking schemes rely on the imperfection of the human auditory system. However, human ear is much more sensitive than other sensory motors. Thus, good audio watermarking schemes are difficult to design. Even though the current watermarking techniques are far from perfect, during the last decade audio watermarking schemes have been applied widely. These schemes are sophisticated very much in terms of robustness and imperceptibility. Robustness and imperceptibility are important requirements of watermarking. There are two types of audio watermarks, Non-blind watermarking and blind watermarking

Non- blind watermarking

Non-blind watermarking schemes are theoretically interesting while they are conflicting each other. It requires double storage capacity and double communication bandwidth for watermark detection. These non-blind schemes may be useful as copyright verification mechanism in a copyright dispute.

Blind watermarking

The blind watermarking scheme can detect and extract watermarks without use of the unwatermarked audio. Hence it requires only a half storage capacity and half bandwidth compared with the non-blind watermarking scheme. Blind audio watermarking schemes are mostly used in practice. The blind watermarking methods need self detection mechanisms for detecting watermarks without unwatermarked audio.

5. REQUIREMENTS FOR AUDIO WATERMARKING ALGORITHMS

The relative importance of a particular property is application dependent, and in many cases the interpretation of a watermark property itself varies with the application.

Perceptual Transparency

The watermark-embedding algorithm has to insert additional data without affecting the perceptual quality of the audio host signal. The fidelity of the watermarking algorithm is usually defined as a perceptual similarity between the original and watermarked audio sequence. However, the quality of the watermarked audio is usually degraded, either intentionally by an adversary or unintentionally in the transmission process, before a person perceives it. It is more adequate to define the fidelity of a watermarking algorithm as a perceptual similarity between the watermarked audio and the original host audio at the point at which they are presented to a consumer.

Watermark Bit Rate

The bit rate of the embedded watermark is the number of the embedded bits within a unit of time and is usually given in bits per second (bps). Some audio watermarking applications, such as copy control, require the insertion of a serial number or author ID, with the average bit rate of up to 0.5 bps. For a broadcast monitoring watermark, the bit rate is higher, caused by the necessity of the embedding of an ID signature of a commercial within the first second at the start of the broadcast clip, with an average bit rate up to 15 bps. In some envisioned applications, for example hiding speech in audio or compressed audio stream in audio, algorithms have to be able to embed watermarks with the bit rate that is a significant fraction of the host audio bit rate, up to 150 kbps.

Robustness

The robustness of the algorithm is defined as an ability of the watermark detector to extract the embedded watermark after common signal processing procedures. Applications usually require robustness in the presence of a predefined set of signal processing modifications, so that watermark can be reliably extracted at the detection side. For example, in radio broadcast monitoring, an embedded watermark need only to survive distortions caused by the transmission process, including dynamic compression and low pass filtering, because the watermark is extracted directly from the broadcast signal. On the other hand, in some algorithms, robustness is completely undesirable and those algorithms are labelled *fragile audio watermarking* algorithms.

Blind or Informed Watermark Detection

A detection algorithm may use the original host audio to extract a watermark from the watermarked audio sequence (informed detection). It often significantly improves the detector performance, in that the original audio can be subtracted from the watermarked copy, resulting in the watermark sequence alone. However, if blind detection is used, the watermark detector does not have access to the original audio, which substantially decreases the amount of data that can be hidden in the host signal. The complete process of embedding and extracting of the watermark can be modelled as a communications channel where the watermark is distorted due to the presence of strong interference and channel effects. A strong interference is caused by the presence of the host audio, and channel effects correspond to signal processing operations.

5. WATERMARKING SCHEME EVALUATION

Digital watermarking has been presented as solutions for protection against illegal copying of multimedia objects and dozens algorithms. The requirements, tools and methodologies to assess the current technologies are al- most inexistent. The lack of benchmarking of current algorithms is blatant. This confuses rights holders as well as software and hardware manufacturers and prevents them from using the solution appropriate to their needs. Digital watermarking remains a largely untested field and only very few large industrial consortiums have published requirements against which watermarking algorithms should be tested. Even though number of claims has been made about robustness of watermarking, the growing number of attacks against such systems has shown that far more research is actually required to improve the quality of existing watermarking methods.
Using benchmarking authors and software providers would just need to provide a table of results which would give a reliable summary of the performances of the proposed scheme. So the users can check whether their requirements are satisfied the industry can properly evaluate risks associated to the use of a particular solution by knowing which level of reliability can be achieved by each contender. The idea to evaluate watermarking schemes is to implement an automated benchmark server for digital watermarking schemes and to allow users to send a binary library of their scheme to the server which in turns runs a series of tests on this library and keeps the results in a database accessible to the scheme owner or to all 'water-markers' through the Web.

The service has a simple interface with existing watermarking libraries (only three functions must be provided). It also takes into account the application of the watermarking scheme by proposing different evaluation profiles (sets of tests and images) and strengths.Each type of watermarking scheme needs different evaluation profiles without having to recompile the profile .Evaluation of profiles is not an easy task and the choice of these profiles does not affect the design of the evaluation service. The main function that should be done here is to evaluate the permeability of scheme, its capacity, its reliability (robustness to at- tacks and false alarm rate) and its performances (mainly the speed of execution). For each of these set of tests we have implemented ad-hoc libraries which are built easily on top of the core libraries. Perceptibility characterizes the amount of distortion introduced during by the watermarking scheme itself. The problem here is very similar to the evaluation of compression algorithms. The capacity of a scheme is the amount of information one can hide. In most applications the capacity will be a fixed constraint of the system so robustness test will be done with a random payload of given size. Our benchmark provide a test that help to analyze this trade-off by drawing different graphs.

The robustness can be assessed by measuring the detection probability of the mark and the bit error rate for a set of criteria that are relevant to the application, which is considered. Finally, related to speed our test just computes the average of the time required on a particular given platform to watermark and image depending on its size. The evaluation service only requires three functions to be exported from the watermarking library supplied by the user. All possible cases are captured and it ended up with a solution where several parameters are provided but not all of them are mandatory. They include the original medium, the watermarked medium, and the embedding key, the strength of the embedding, the payload, the maximum distortion tolerated and the certainty of extraction.

6. EXISTING SYSTEM

In an audio watermarking technology which is based on chaotic map and modified Patchwork algorithm, a chaotic sequence is introduced in the embedding process to ensure the security. And a novel Patchwork algorithm is projected in DWT domain. A portion of DWT coefficients in two patches have been modified in different ways according to bit code, thus, their statistical characteristics shift to opposite directions. But the disadvantage in this algorithm is degradation of host audio.

An algorithm based on Gammatone Filter bank which has remarkable resistance against common manipulations and attacks such as adding noise, low-pass filtering, resampling, lossy compression , random sampling etc. Gammatone filter bank (GTF) is a bank of overlapping band-pass filters, which mimics the characteristics of the human cochlea. Even though it has many merits, the demerit here is the values of SNR and BER are pretty high**.** A novel audio watermarking scheme based on the statistical feature manipulation in wavelet domain combined with error correction coding technique is used in this method. Here, a physical feature insensitive to attacks based on the idea of Invariant watermark is found and the watermark is embedded by modifying them directly. Robustness can be increased by using repetition codes and BCH codes. But only under the condition that BER is below 10%, the use of BCH codes makes sense. These attributes are overcome by a highly confidential audio watermarking scheme that is proposed.

7. PROPOSED WATERMARKING SCHEME

Audio watermarking is a promising solution to copyrights protection for digital audio and multimedia products. To achieve its objectives, a qualified audio watermarking scheme should possess excellent imperceptibility for transparent perception, high-level security for preventing authorized detection, and strong robustness against various attacks, such as noise addition, MPEG compression, reverberation, random samples cropping/inserting, time stretching and pitch shifting. Previously implemented audio watermarking schemes have excellent capabilities for the purpose of copyrights protection. In this system, performance on security is improved using multiple scrambling. Every scrambling operation has its independent secret key; a pseudorandom sequence, the detection can be only conducted properly when all the keys are known. This means that we can be able to revive the watermark even from the attacked audio files with loss of synchronization.The proposed system is a Havoc free multiple audio watermarking is a secure audio watermarking scheme which uses multiple scrambling. This new scheme is self-secured by integrating multiple scrambling operations into the embedding stage.

Firstly, a pre-selection is applied on the host audio signal to determine the embedding segments. Only the regions whose power exceeds a certain threshold will be chosen for watermarking. Before embedding the actual watermark in those embedding segments, the watermark is converted into the coded data because it can be identified visually, which is a kind of ownership stamp. Then the coded image is processed for encryption. The first scrambling operation is to encrypt the coded image watermark into incomprehensible ciphers, where one secret key is used. After the image is encrypted, the image bits are randomized in their order of encoding and then it is embedded in the host audio signal. Instead of using all the frames, we randomly select certain frames out of the total frames and randomize their orders of encoding. Since the secret keys are shared only between the embedder and authorized detectors, the goal of copyrights protection is really achieved. The proposed system uses DC watermarking scheme which hides watermark data in lower frequency components of the audio signal, that are below the perceptual threshold of the human auditory system. Security can be improved by using this multiple scrambling method. The proposed scheme can be further improved by embedding multiple watermarks. Multiple watermarks, each of which has different characteristics are embedded in an audio signal.

The characteristics of the various watermarks are chosen so that each of the watermarks will be affected in a different manner if the audio signal is subsequently copied and reproduced. Thus,

the audio watermarking is a promising solution to copyrights protection for digital audio and multimedia products. Thus its objectives can be achieved by using this havoc free multiple audio watermarking schemes. Audio watermarking involves the concealment of data within a discrete audio file. Audio watermarking technology thus affords an opportunity to generate copies of a recording which are perceived by listeners as identical to the original but which may differ from one another on the basis of the embedded information.

Multiple Scrambling

The proposed scheme is self-secured by integrating multiple scrambling operations into the embedding stage. Along with the random settings on the amount and positions of slots assigned to each watermark bit, anyone without all the secret keys rarely has the possibility to find out the watermark. Since the secret keys are shared only between the embedder and authorized detectors, the goal of copyrights protection is really achieved.

DC Watermarking Scheme

The DC watermarking scheme can be used to hide auxiliary information within a sound file. The watermarking scheme provides an overview of techniques which are common to all digital audio watermarking schemes. The DC watermarking scheme hides watermark data in lower frequency components that are perceptible to the human auditory system of the audio signal and that are below the perceptual threshold of the human auditory system. From the spectral analysis of each frame, the low frequency (DC) component F(1), can now be removed by subtraction from each frame using the following formula:

$$f(n) = \sum_{k=1}^{3969n} f(k) - F(1) \qquad n = 1, 2, \ldots, N$$

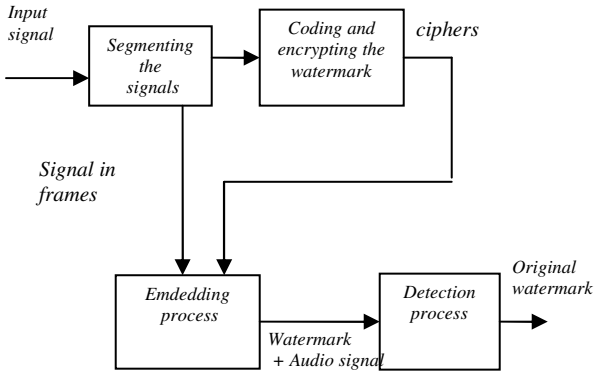

FIGURE 1. Multiple Scrambling Operations of Audio watermarking Scheme

Segmenting The Audio Signal

The audio file is portioned into frames which are 90 milliseconds in duration. This frame size is chosen so that the embedded watermark does not introduce any audible distortion into the file. With a 90 ms frame size, our bit rate for watermarked data is equal to 1 / 0.09 = 11.1 bits per second.

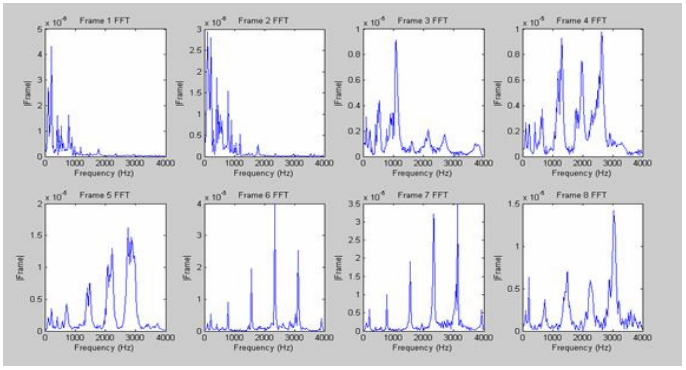

FIGURE 2. Sample spectrum of signal frames

Coding And Encrypting The Watermark

The image to be embedded is converted into a coded binary image with bits '1' and '0' as visual watermark, instead of meaningless pseudorandom or chaotic sequence. Not only because coded binary image can be identified visually, which is a kind of ownership stamp indeed, but also post processing on the extracted watermark could be done to enhance the binary image and consequently the detection accuracy will increase. Image de-noising and pattern recognition are examples of post processing techniques for automatic character recognition. Thus, on top of the bit error rate, coded binary image provides a semantic meaning for reliable verification. Next the coded binary image is encrypted for the security purpose, which involves a secret key.

Watermark Embedding Process

Multiple Scrambling

To increase the level of security, multiple scrambling can be used in the embedding. The first scrambling operation is to encrypt the coded image watermark into incomprehensible ciphers, where one secret key is used. Furthermore, instead of using all the subbands, we randomly select some frames out of total frames and randomize their orders of encoding, where two secret keys are employed. Along with the random settings on the amount and positions of frames assigned to each watermark bit, anyone without all the secret keys rarely has the possibility to find out the watermark. Since the secret keys are shared only between the embedder and authorized detectors, the goal of copyrights protection is really achieved.

Embedding Process

The process of embedding a watermark into an audio file is divided into four main processes. An original audio file in wave format is fed into the system, where it is subsequently framed, analyzed, and processed, to attach the inaudible watermark to the output signal.

Framing

As with the insertion process, the audio file is partitioned into frames which are 90 milliseconds in duration. With a 90 ms frame size, we expect an extracted watermark data rate equal to 11.1 bits per second.

Spectral Analysis

Subsequent to the framing of the unprocessed audio signal, spectral analysis is performed on the host audio signal, consisting of a fast Fourier transform (FFT), which allows us to calculate the low frequency components of each frame, as well as the overall frame power. The FFT processing is accomplished in Mat lab, using the following equation:

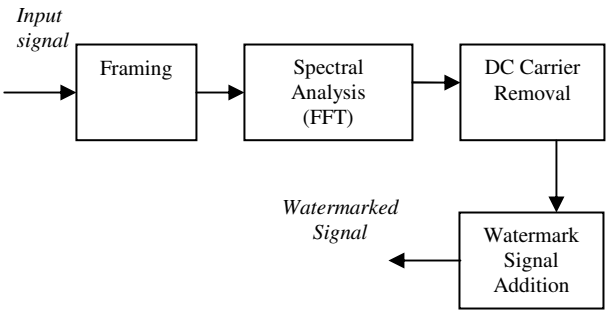

FIGURE 3- Watermark Embedding Process

$F(k) = \sum_{n=1}^{N} f(n) e^{\frac{-j2\pi(n-1)(k-1)}{N}}$ $k = 1, 2, \ldots, N$, N denotes the last frame in the audio file.

With a standard 16 bit CD quality audio file having a sampling rate, Fs = 44,100 samples per second, a frame consists of 3969 samples. If we perform a FFT on a frame of this size

with N = 3969, we end up with a frequency resolution as follows:

$$\frac{44{,}100\ Hz}{2 \times \frac{3969}{2}\ samples} = 5.6\ Hz\ resolution$$

From the FFT, we are now able to determine the low frequency (DC) component of the frame F(1), as well as the frame spectral power. To calculate the frame power, we use the sum of amplitude spectrum squared:

$$P_{Frame}(n) = \frac{1}{\left(\frac{3969}{2}+1\right)} \sum_{k=1}^{3969+1} F(k)^2 \quad n = 1, 2, \ldots, N$$

DC Removal

From the above spectral analysis of each frame, the low frequency (DC)

$$P_{Frame}(n) = \frac{1}{\left(\frac{3969}{2}+1\right)} \sum_{k=1}^{3969+1} F(k)^2 \quad n = 1, 2, \ldots, N$$

From the above spectral analysis of each frame, the low frequency (DC) component F(1) is calculated, which can now be removed by subtraction from each frame using the following formula:

$$f(n) = \sum_{k=1}^{3969n} f(k) - F(1) \qquad n = 1, 2, .., N$$

Watermark Signal Addition

From the spectral analysis completed previously, we calculated the spectral power for each frame, which is now utilized 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. The magnitude of the watermark is added according to the formula:

$$f(n) = \sum_{k=1}^{3969n} f(k) + K_s \times w(n) \times P_{frame}(n) \qquad n = 1, 2, ..., N$$

Where Ks is the scaling factor, which ensures the watermark is embedded below the audibility threshold, and w(n) represents the watermark signal data, which is binary, having a value of 1, or -1.The f (n) function has now been watermarked with the above process, and is ready for storage, testing, and watermark extraction.

Watermark Detection Process

Watermark Extraction

The process of extracting the digital watermark from the audio file is similar to the technique for inserting the watermark. The computer processing requirements for extraction are slightly lower. A marked audio file in wave format is fed into the system, where it is subsequently framed, analysed, and processed, to remove the embedded data which exists as a digital watermark.

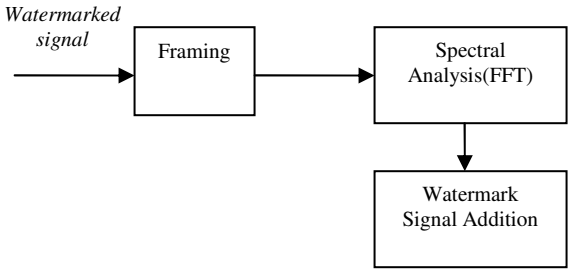

FIGURE 4 - Watermark Extraction Process

Watermark Signal Extraction

From the spectral analysis completed previously, we calculated the spectral power for each frame, which allows us to examine the low frequency power in each frame and subsequently extract the watermark, according to the following formula:

$$w(n) = \begin{cases} 1 & if\ F_x(1) \geq 0 \\ 0 & if\ F_x(1) \leq 0 \end{cases} \qquad n = 1, 2, \ldots, N$$

where, N denotes the last frame in the audio file.

The extracted watermark signal, w (n), should be an exact replica of the original watermark, providing the original audio file has enough power per frame to embed information below the audible threshold, and above the quantization floor.

8. EXPERIMENTAL RESULTS

The implementation phase begins with the process of dividing the audio signal into a certain number of frames such that each frame is 90 milliseconds in duration. This frame size is chosen so that the embedded watermark does not introduce any audible distortion into the file.

FIGURE 5. Input Audio Signal

The sample spectrum of the original audio signal is shown below .

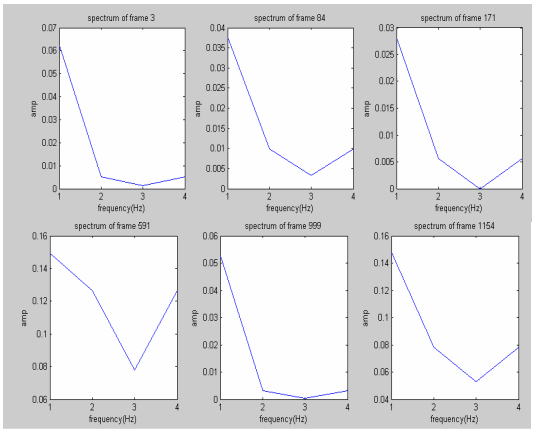

FIGURE 6 Sample Spectrum Of the Original Audio Signal

The image to be watermarked is chosen and is binary coded as shown in figure 7.

FIGURE 7 Image to be watermarked

After coding the image watermark, it is embedded using Multiple Scrambling and DC watermarking scheme. Following the process of embedding, the original audio signal now consists of the image watermark. It is shown as in figure 8. The embedded watermark is then detected from the watermarked signal in the detection process.

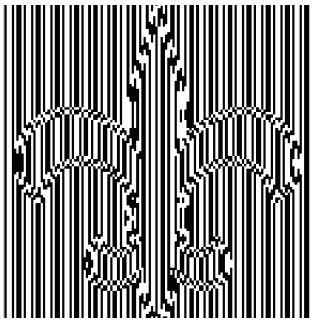

FIGURE 8. Encrypted image

After encrypting the image watermark, it is embedded using Multiple Scrambling and DC watermarking scheme. Following the process of embedding, the original audio signal now consists of the image watermark. The sound is played using the sound viewer.

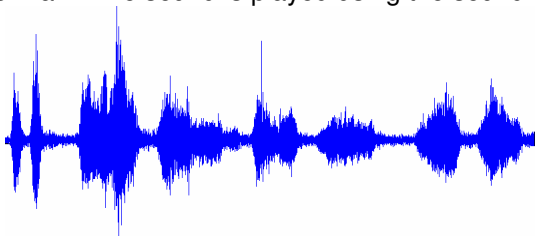

FIGURE 9 Watermarked Audio Signal

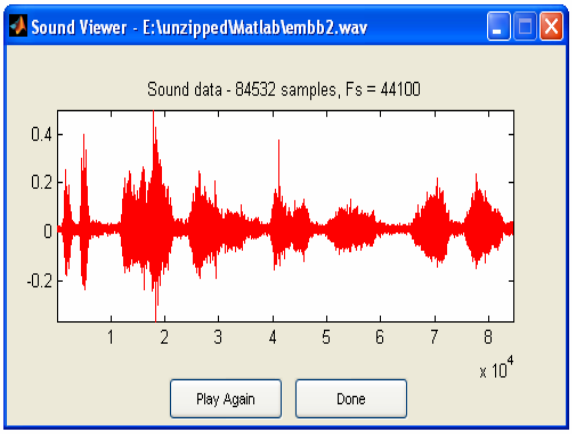

FIGURE 10 Sound Viewer

9. CONCLUSION AND FUTURE WORK

Audio watermarking can also be used for fingerprinting and additional features to audio contents besides the functions as copyright protection. a secure and robust audio watermarking scheme using coded-image watermark, multiple scrambling and adaptive synchronization is proposed .The report has also found that in order to achieve these functionalities, a watermarking scheme has to meet the requirements of perceptibility, reliability, capacity and speed. The coded image can further improve the watermark detection by using image processing techniques and pattern matching analysis Compared with digital image and video watermarking technologies, audio watermarking technology provides a special challenge because the human auditory system is extremely more sensitive than human visual system. Audio watermarking is a persistent data communication channel within an audio stream. It should survive through various format changes. Watermarked Audio Signal and manipulations (either legitimate or not) of the audio material, as long as the content retains some commercial potential. Additionally, it should do so without introducing any perceivable audio artifacts. Most of the audio watermarking technology includes many demerits such as degradation of host audio signal, high Bit Error Ratio and Signal to Noise Ratio of the host signal, less security and etc. which can be completely overcome by the proposed audio watermarking technology. Also with the help of multiple scrambling, the scheme is strictly self-protected and any attacker without all the secret keys is impossible to ascertain or destroy the watermark embedded without noticeably degrading the signal. The experimental results prove that the system is secure and robust. The work can be extended for security against collusion attacks.

ACKNOWLEDGMENT

We would like to acknowledge all the persons who have contributed to a great extent towards the initialization, development and success of this paper. With great respect and obedience, We would like to thank our parents who were the backbone behind our deeds.

REFERENCES

[1] F.A.P. Petitcolas, "Watermarking schemes evaluation", IEEE Signal Processing Magazine, vol. 17, no. 5, pp. 58-64, 2000.

[2] Rangding Wang, Qian Li and Diqun Yan ," A High Robust Audio Watermarking Algorithm", CKC Software Lab, University of Ningbo,2006.

[3] R. Tachibana, "Improving audio watermarking robustness using stretched patterns against geometric distortion", IEEE Pacific-Rim Conference on Multimedia (PCM'02), pp. 647-654, 2002.

[4] Tong Won Seok and Jin Woo Hong, "Audio watermarking for copyright protection of digital audio data", Electronics Letters, Vol. 37, No. 1,2001.

[5] Y.Q. Lin, W.H. Abdulla, "Robust audio watermarking for copyrights protection", Technical Report (No. 650), Dept. of Electrical & Computer Engineering, The University of Auckland, 2006. http://www.ece.auckland.ac.nz/~wabd002/Publications.

[6] Y.Q. Lin, W.H. Abdulla, "Robust audio watermarking technique based on Gammatone filterbank and coded image", International Symposium on Signal Processing and Its Application (ISSPA'07), 2007.

[7] Eric Metois, Ph.D. "Audio Watermarking and Applications", ARIS Technologies, Inc. – September 1999.

[8] A. Gurijala, J.R. Jr. Deller, "Robust algorithm for watermark recovery from cropped speech",IEEE International Conference on Acoustic, Speech and Signal Processing (ICASSP'01), vol. 3, pp. 1357-1360, 2001.

[9] W. Li, X. Xue, "An audio watermarking technique that is robust against random cropping", Computer Music Journal, vol. 27, no. 4, pp. 58-68, 2003.

[10]http://www.ece.uvic.ca/~aupward/w/watermarking.htm.

[11] Yiqing Lin Waleed H. Abdulla "A Secure and Robust Audio Watermarking Scheme Using Multiple Scrambling and Adaptive Synchronization" International Symposium on Signal Processing and Its Application, 2007

[12] W. Li, X. Xue, "An audio watermarking technique that is robust against random cropping", Computer Music Journal, vol. 27, no. 4, pp. 58-68, 2003.

[13] EBU, "SQAM - Sound Quality Assessment Material", http://sound.media.mit.edu/ mpeg4/ audio/ sqam/

[14] Essaouabi Abdessamad ,E.Ibneihaj, F.Regragui," A Wavelet- based object watermarking system for MPEG4 Video ", International journal of Image Processing,(IJIP),volume (3): issue(6).