DIGITAL WATERMARKING OF AUDIO SIGNALS FOR ENHANCED SIGNAL PROTECTION

Gautam Nag

Electrical and Electronics Engineering, SRM University, 603203

Email: gn8732@srmist.edu.in

Shruti Srivastava

Electrical and Electronics Engineering, SRM University, 603203

Email: ss1750@srmist.edu.in

ABSTRACT

In today's world we know the importance of encryption and privacy and with data being the most prized possession it is more important than ever to protect that data. Therefore, for our project we are aiming at using this as our principal objective for protecting signal and audio during transmission. To do this will use digital watermarking and using a digital image/unique code superimposing the signal and then transposing that image as a watermark on the audio signal. Watermarking is a technique used to label digital media by hiding copyright or other information into the underlying data. The aim is to create a watermark that must be imperceptible or undetectable by the user and should be robust to attacks and other types of distortion. In our method, the watermark is kept as a digital image or if contingency arises a masked signal copy. With advantages we also have disadvantages of everything switching to an online mode of working. This would augment cyber-attacks like phishing, malware, cross site scripting, sql injection and so on. In order to reduce the disadvantages and protect the data watermarking becomes mandatory. We believe that doing so will uniquely enhance security of the audio signal.

1. Introduction

Digital/Audio Watermarking is the intriguing field of research that is in the growth phase. As mentioned earlier in this report, all the services have switched to online mode which makes it essential to maintain the confidentiality and security of a large dataset. Our objective in conducting the literature survey was to identify the gaps in previous research and try to bridge them through our project proposal. In order to accomplish our goal, we have referred to six literature papers and reviewed them to gain insights and draw inferences to proceed with our research. Having leveraged the gap between the problem and the proposed solutions related to

Audio Watermarking of Audio signals, we performed experiments to determine which method of encrypting the signals was reliable and efficient. In order to carry out the execution, we used the Audacity, an open-source software platform to watermark the host file and thereby generated a white noise using the waveform of Tone (Overlapping method) but a major disadvantage of using the waveform signal of Tone was a noise that was detected and therefore made the quality of host file (original audio) bad due to this the original content could not be recognized. Encrypting data though necessary is a challenge and according to the reports there are five reasons why encryptions doesn't work. The reasons are listed below.

1. Encryptions don't work for systems.
2. Encryptions cannot be audited
3. Encryptions does not work against the insider threat

Therefore, the experiment performed by us was using a digital image (png or jpeg) to watermark the audio signals which became successful. To carry out this a MATLAB software was used and with the help of coding we accomplished our goal to encrypt the audio signals through digital watermarking. Not only this method is unique compared to other proposed methods by various researchers but also this opens up a way for many to do advanced research in this field.

The pandemic not only has brought destruction to us but also has changed our way of living and working. Since the majority of the population has switched to work from home and this has led to the majority of information being interchanged and transactions taking place online. This does not stop here as the pandemic has also paved the way for digital innovation, from shopping to medical check-ups that are taking place through online, it becomes essential to maintain the security and confidentiality of big data therefore Watermarking/encrypting plays a vital role in present and in the future. With advantages we also have disadvantages of everything switching to an online mode of working. This would augment cyber-attacks like phishing, malware, cross site scripting, sql injection and so on.

In order to reduce the disadvantages and protect the data watermarking becomes mandatory. Digital Watermarking is the method of using a digital form of media to hide valuable information inside another media to enhance its security. One of the features of watermarking is that it does not affect the data usage. Furthermore, this technology often protects copyright of multimedia data and protects databases and text files from unauthorized access and being corroded. One of the applications of Watermarking that explains it best and stresses its importance is its use in money and stamps to assist in identifying counterfeiting. This technique has its similarities to steganography. Hence basically the idea behind creating a watermark is to create a translucent image on the paper to provide authenticity.

In this era of digitization and digitalization it is very difficult to claim 99.999% protection of data after embedding a watermark in the media since there are chances of web scraping, cropping, editing and redistributing but this does not claim the inefficiency of watermarking

rather to be on the safer side it is recommended to create a copy of the data with watermark embedded in it. The ideal watermark is 30-70% transparent and covers a significant portion of the asset. Hence adding a digital watermark is basically adding bits of pattern which are unnoticeable to the human eye in the picture/ video that is to be protected and authenticated. Furthermore, since the watermarks are easy to create, applicable in seconds, it is considered to be one of the most effective methods of safeguarding images from theft and unauthorized use. Therefore, these are the reasons why Watermarking is the need of the hour and why one should go for watermarking the data.

2. Methodology

2.1 Algorithmic Approach

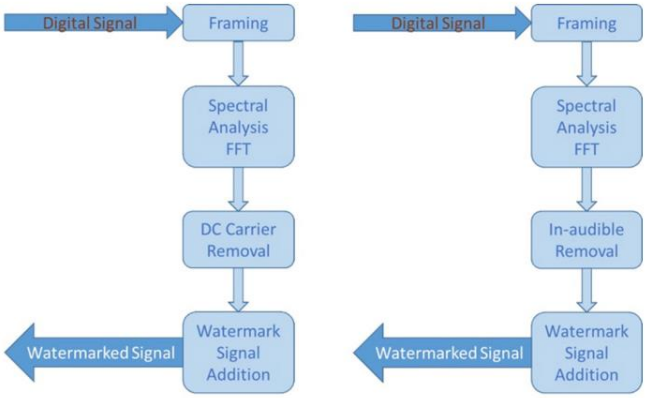

Figure 2.1.1 Algorithmic Implementation

A Watermark is embedded into the digital signal at each point of distribution which is unnoticeable to the human eye. If the data is copied the watermark is carried with the data and the watermark can be retrieved from the copy and the source of distribution is known. Digital Watermarking is a technology that embeds machine readable information within the content of a digital media file that could be image, audio or video. The information is encoded through subtle changes to the image, audio, or video. In other words, the watermarking is a practice of modifying the digital data (software program, photos, songs, videos) without causing destruction to it to embed a message about that work. Multimedia watermarking is the practice of imperceptibly altering a work. The watermarking is a technique related to steganography which means keeping the existence of messages secret by hiding them within objects, media, or other messages.

We started with the classification of the audio signal and dividing it into things such as bandwidth, nominal level, power level in decibels (dB), and voltage level. The attachment between P-V is the impedance of the signal path. Signal paths may be 1 ended or balanced. 15 For our work we will be using MATLAB and Audacity which is an open source - multi platform software. This is an inhouse project for which the minimum specifications required to run the project are as follows:

Table 2.1.1 System Parameters

Parameter	**Minimum Specifications Needed**
Operating System (OS)	Windows 7
Processing power	1.8 GHz
Random Access Memory (RAM)	2 GB

We started with using Audacity to test the form of audio signal and the Waveform Audio File Format in the preliminary stages. We used a file that contained audio recordings with different sampling rates and bit rates but were saved in a 44.1 kHz, 16-bit format on Audacity. These files were divided into host and port WAV's and sampled onto Audacity and was mapped using the Microsoft sound mapper at the following specifications:

Table 2.1.2 Parameter Value Set

Parameter Name	**Value Set**
Audio Channel	Mono
Frequency	44100 Hz
Bit point (floating)	32 bit
Mapping (range)	- 1.0 - 1.0
Time Sampled	Duration = 60 seconds

3. Working

3.1 Code Approach

A Watermark is embedded into the digital signal at each point of distribution which is unnoticeable to the human eye. If the data is copied the watermark is carried with the data and the watermark can be retrieved from the copy and the source of distribution is known. Digital Watermarking is a technology that embeds machine readable information within the content of a digital media file that could be image, audio or video. The information is encoded through subtle changes to the image, audio, or video. In other words, the watermarking is a practice of modifying the digital data (software program, photos, songs, videos) without causing destruction to it to embed a message about that work. Multimedia watermarking is the practice of imperceptibly altering a work.

The watermarking is a technique related to steganography which means keeping the existence of messages secret by hiding them within objects, media, or other messages. There are two types of digital watermarking- visible and invisible. The visible watermark is similar to the corporation logo displayed at its letterhead but the invisible one that is embedded in the media is unnoticeable and undetectable to the human eye. There are some six types of watermarks- visible, non-visible, private, public, perceptual and bit stream. This is a blind watermarking technique that meets the requirements of invisibility and robustness. Watermarking is performed by embedding a watermark in the middle-frequency coefficient block of three DWT levels.

After analysing the previous outputs and studying their disadvantages we see that using digital watermarking of audio signals for enhanced signal protection is indeed one of the most convenient ways to go about the problem statement of audio encryption. Hence for our project we have used MATLAB to achieve the same. The entire process is divided into parts of MATLAB code namely “Embedded the watermark” and “Extracting the water marking”. It was important to use two separate code scripts for this process as mentioned in the QoS literature review, it protects the integrity of the code snippet in case some “pirate” affects one section of the code, the others will remain intact and free of interference from the 3rd party.

Our project includes 2 MATLAB function files (write) and 1 sample MP3 files (read). It works like the commands WAVWRITE and WAVREAD. It must be noted that this version was made in MATLAB for WINDOWS only. Also note that we are using DOUBLE data type with double [-0.5 +0.5] to 'uint8' [0 255] as the parameter and this can be changed according to the receiver's need or the size of the watermark /Host signal.

3.1.1 Insertion of the Watermark

First of all, we run a command to clear all the previous system clutter(memory) and get a clean command window. Then we use the “audioread” command to load the host audio and store it in a variable with its address stored into an index variable (which in our code is named as f). Then we load the watermark image (which is a png) into a using the “iread” command and store it is a variable named “wm”. Then we use a 2D array to store the dimensions of the image we are using as a watermark. Then we use a conditional statement to check if the length of the host file is less than the length of the watermark * 8. If it is then we reject that image as a watermark and display a message saying to use a different watermark. Then we call the predefined MATLAB function called “dec2bin” to start the binary host. Then we write the code to prepare the watermark: a. Firstly we call the dec2bin function used just above this function. Then we declare a n X 8 zeroes matrix (where n in the proportional row size 24 of the watermark). Then we run a for loop to insert a watermark into the first plane of the host signal. Then for every iteration of the for loop declare the LSB by using the command “host_bin(i, 8) = dec2bin(wm_str(i))” 9. Finally host the watermark using the bin2dec() function and specify the data type as “double”.

3.1.2 Extraction of Watermark

First of all, we run a command to clear all the previous system clutter(memory) and get a clean command window. Specify an upper range for the watermark size and store it in a variable. Divide that with 8 to get the number of pixels used in generating the size. Store the image size in a variable as the square root of the pixel size. Call the “audioread” function and pass the path of the watermarked host signal’s path name into the function. Use the double [-0.5 +0.5] to 'uint8' [0 255] parameter to match the watermark dimensions matched to the double data type. Define the host bin size at (1:max size) and store it in a variable. 8. Call the “reshape function” and pass the above variable along with the pixel size and the constant number 8(that we used to divide in step 2 into the function. Define a zeros matrix. Run a for loop on this matrix: a. For every iteration of the for loop use the bin2dec to generate a LSB and store it in a variable. End the for loop. Call the reshape function used before and replace the constant 8 with the image size variable. Call in the imshow() function to finally extract and display the watermark.

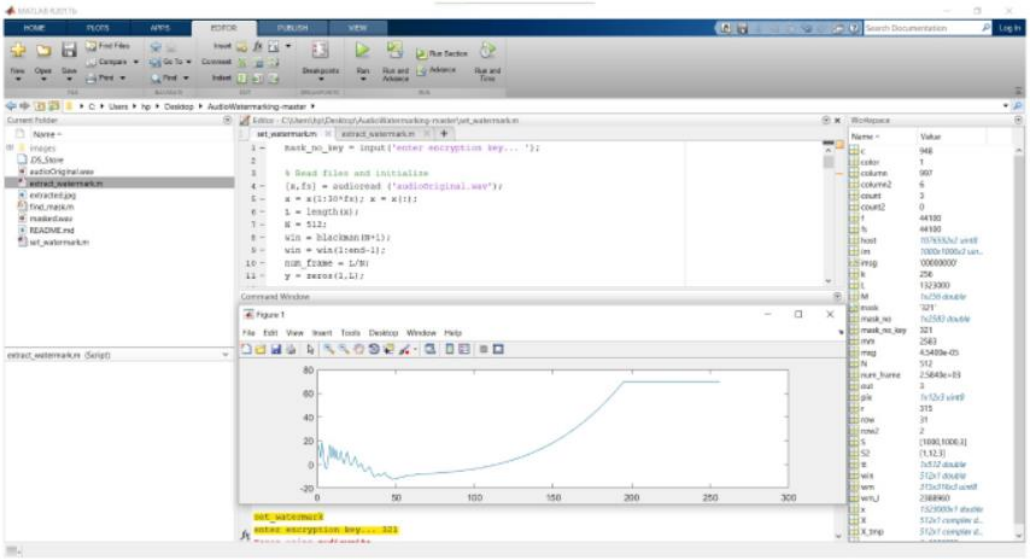

Figure 3.1.2.1 – Extraction of watermark

3.2 Masking the Watermark onto the audio

Psychoacoustics is used for the Masking Effects. In the project A “weak” sound is difficult to be heard while a “strong” sound is also being played. So, to tackle this problem we use masking such as:

a. Temporal Masking - Amplitude (Volume)
b. Frequency Masking - Amplitude in Frequency

Keeping the Image parameters at width="370" height="270“for testing the code that will mask the audio. Then we incorporate DC Watermarking i.e., puts the information into the part of music, where the magnitude is lower than the perceptual threshold of human ears and Frequency Watermarking for feedback i.e. For Frequency Watermarking, since human ear has limit on distinguishing audio frequency, it is possible to find out a frequency band loud enough while the frequency near it is rather quiet. Therefore, we replace the frequency band with low magnitude to our information to make the watermark.

Therefore, we implemented these in this project to achieve our goal. The original soundtrack we used in this project is:

a. Length: 30 seconds
b. Sampling Rate: 44100 (1/s)
c. Frame Length: 512 samples

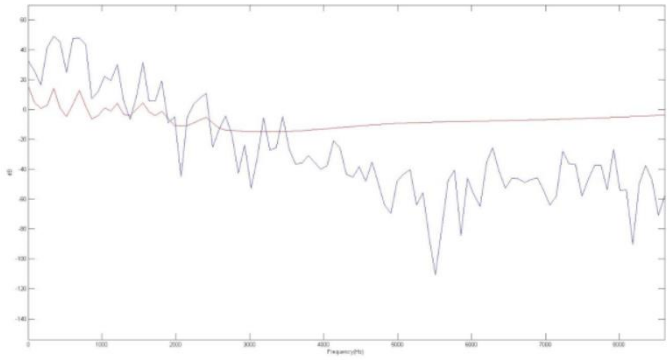

Figure 3.2.1 – Pre FFT masking

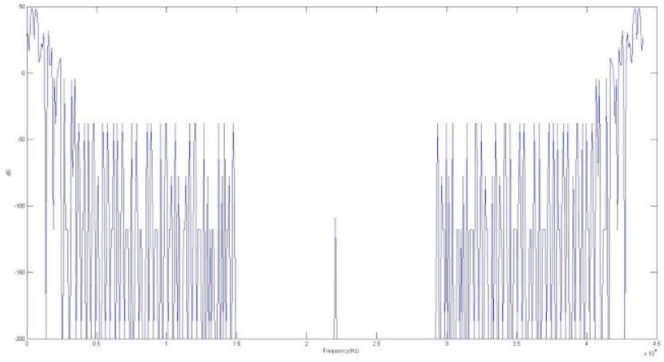

Figure 3.2.2 Post FFT masking

4. Analysis

After the completion of the project, we inferred that using digital watermarking for enhanced signal protection not only keeps the original quality of the sound unaltered but also encrypts the signal. On top of that the watermark stays hidden therefore it preserves the integrity of the encryption, making this approach a very fruitful form of audio encryption. For starters not anyone who gets the encrypted audio can decode the audio as the sender has the numbers required to decrypt and extract the watermark. Secondly the sender has total control over the encryption which was not possible in the traditional encryption methods. And lastly the integrity of the original audio signal stays preserved and does not get out of sync or phase, so if we want to send the audio file to a 3rd party, we can do so with the watermarked audio intact.

5. Final Result and Summary

In today's world we know the importance of encryption and privacy and with data being the most prized possession it is more important than ever to protect that data. Therefore, by keeping that as our motivation in our minds we started this project. And finally, after the completion of this project we have found that using digital watermarking for enhanced

signal protection is the most convenient way to target the masses and make audio encryption a better part of everybody's lives. That is why after analysing 20+ literature reviews 5+ algorithms in the field of audio encryption we came up with the idea of digital watermarking. And we are proud to present the result of our experiment for the same where we have seen that digital watermarking strikes a perfect balance between audio encryption and capital spent/encryption. Therefore, to lay bare the final results of our work in a comprehensive form we have summarized the gist of the above work of 40+ pages into the table as the result of our work:

Table 5.1 – Result Comparison Summary

TESTING PARAMETERS	Digital Watermarking Of Audio Signal	Discrete Wave Transform Method	Quantum Discrete Cosine Transform Method	Traditional Overlapping Signal Tone Method
High system specs. required?	NO	YES	YES	NO
Additional hardware required?	NO	YES	NO	NO
Requires integration of AI and ML?	NO	NO	YES	NO
Fluctuating results?	NO	NO	YES	NO
Damage to the original audio?	NO	NO	YES	YES
Receiver's needs integrated?	YES	YES	NO	NO
Dynamic real time encryption?	YES	YES	NO	NO
Can handle complex files?	NO	YES	YES	NO
Additional security can be added?	NO	YES	YES	NO

6. Conclusions

The method "Digital watermarking of Audio Signals" was found more efficient and reliable to encrypt the audio signals as it retained the original audio quality. Furthermore, it is convenient to use as it contains simple MATLAB coding. The only criteria's being the image is confined to the .png and .jpeg extension and the image size should be greater than the host file i.e the original audio. Not only is this method unique from other proposed methods but also this would pave the way for many researchers to do advanced research in the near future.

REFERENCES

[1] Kendall, M.G.; Smith, B. Babington (1938). "Randomness and Random Sampling Numbers". Journal of the Royal Statistical Society. 101 (1): 147–166. doi:10.2307/2980655. JSTOR 2980655.

[2] Yongge Wang. Statistical Testing Techniques for Pseudorandom generation.

[3] Yongge Wang: On the Design of LIL Tests for (Pseudo) Random Generators and Some Experimental Results. PDF

[4] Wang, Yongge; Nicol, Tony (2015). "Statistical Properties of Pseudo Random Sequences and Experiments with PHP and Debian OpenSSL". Computers and Security. 53: 44–64. doi:10.1016/j.cose.2015.05.005.

[5] Knuth, Donald (1998). The Art of Computer Programming Vol. 2 : Seminumerical Algorithms. Addison Wesley. pp. 93–118. ISBN 978-0-201-89684-8.

[6] N. Suryana, Siaw-Lang Wong (2010). “An efficient compact Tchebichef Moment for image compression”: Information Sciences Signal Processing and their Applications (ISSPA), 2010.

[7] S. E. Tsai and S. M. Yang, An Effective Watermarking Method Based on Energy Averaging in Audio Signals: Hindawi Mathematical Problems in Engineering Volume 2018

[8] Laurence Boney, Ahmed H. Tewk and Khaled N. Hamdy, Digital Watermarks for Audio Signals, Département Signal, Department of Electrical Engineering, University of Minnesota: Minneapolis, MN 55455.

[9] M. Yamini, H.Karmouni, M.Sayyouri, Efficient watermarking algorithm for digital audio/speech signal, Engineering, Systems and Applications Laboratory, National School of Applied Sciences, Sidi Mohamed Ben Abdellah University, BP 72, My Abdallah Avenue Km. 5 Imouzzer Road, Fez, Morocco.

[10] F.Benedetto,G.Guinta, A.Neri, Digital audio watermarking for QoS assessment of MP3 music signals, Dept. of Applied Electronics, University of ROMA TRE, Rome, Italy.