

A PROJECT REPORT

on

**DIGITAL WATERMARKING OF AUDIO SIGNALS
FOR ENHANCED SIGNAL PROTECTION**

Submitted in partial fulfillment for the award of the degree

of

BACHELOR OF TECHNOLOGY

in

ELECTRICAL AND ELECTRONICS ENGINEERING

by

Gautam Nag (RA1811005010278)

Shruti Srivastav (RA1811005010271)

Under the guidance of

Dr. C. Naveen

(Assistant Professor, Department of Electrical and Electronics Engineering)



FACULTY OF ENGINEERING AND TECHNOLOGY

SRM Nagar, Kattankulathur- 603 203
Kancheepuram Dist.

APRIL 2022

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.

It is then weighted in the time domain to account for temporal masking. We discuss the detection of the watermark and assess the robustness of our watermarking approach to attacks and various signal manipulations.

We believe that doing so will uniquely enhance security of the audio signal.

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
4. Data Integrity is the biggest threat in cyberspace
5. One can't prove whether encryption security is working

These are the gaps present with encrypting media and through our research we are trying to reduce these gaps to minimal.

CHAPTER 01

INTRODUCTION

Audio watermarking is currently at the forefront of technology development to detect illegal reproduction and redistribution of audio recordings. Because the human auditory system (HAS) is more sensitive than the human visual system, audio watermarking is more challenging than visual watermarking.

A reliable digital audio watermarking shall have imperceptibility, data capacity, and robustness. The watermark must be inaudible within the host audio to maintain audio quality. The watermark data capacity is the information embedded or hidden in the host audio without perceptible distortion. The watermark robustness is that the watermark must remain intact or identifiable through signal processing such as compression, time-scaling, filtering, and resampling performed on the watermarked audio.

Therefore for our project we have aimed at a way to protect an audio signal or audio file by encrypting it with a watermark which will ensure that each audio signal transmission and reception is protected from both ends of the communication. Basically an **Audio Watermarking is the process of adding a distinctive sound pattern undetectable to the human ear to an audio signal to make it identifiable to a computer.**

Watermarking is the process of embedding information into a signal (audio, video or pictures) which becomes difficult to remove. If the signal is copied, then the information is also carried in the copy. Watermarking has become essential to enable copyright protection and ownership verification.

One of the most secure techniques of audio watermarking is **spread spectrum audio watermarking (SSW)**. In the above method a narrow-band signal is transmitted over a much larger bandwidth such that the signal energy presented in any signal frequency is undetectable. Thus the watermark is spread over many frequency bands so that the energy in one band is undetectable. In order to destroy this watermark technique a noise of high amplitude is required to be added in all frequency bands.

Spreading Spectrum is done using a Pseudo Noise commonly referred to as PN sequence. In SSW approach the receiver must know the PN sequence that is used at the transmitter as well as the location of the watermark in the watermarked signal for detecting hidden information. This is a high security feature since any unauthorized user who doesn't have access to this information will not be able to detect any hidden information. Detection of the PN sequence is the key factor for detection of hidden information from SSW.

NEED FOR DIGITAL WATER MARKING

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 checkups 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 a process of hiding digital information in a carrier signal where the hidden information need not contain a relation with the carrier signal. Digital Watermarks intend to verify the authenticity or integrity of the carrier signal or to show the identity of its owners.

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.

PRINCIPLE OF DIGITAL WATERMARKING

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.

The PNN is used during watermark extraction.

CHAPTER 2

LITERATURE OBJECTIVE

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.

Based on the research we conducted we have gained information that different authors have proposed different methods to encrypt the data without affecting the quality of the video or audio during transmission and on the receiving end.

After analyzing some research papers we found that audio signals have somewhat standardized levels depending on the application. Outputs of professional mixing consoles are most commonly at line level. Consumer audio equipment will also output at a lower line level. Microphones generally output at an even lower level, commonly referred to as mic level. For our project we will focus on the line level.

Therefore for our project we have aimed at a way to protect an audio signal or audio file by encrypting it with a watermark which will ensure that each audio signal transmission and reception is protected from both ends of the communication. In order to accomplish our goal we have used MATLAB and AUDACITY - open source multi-platform software.

LITERATURE REVIEW

To accomplish the targets of this research project on “**DIGITAL WATERMARKING OF AUDIO SIGNALS FOR ENHANCED SIGNAL PROTECTION**”, I have reviewed some literature papers to gain insights and to identify the gaps as it is the foremost and mandatory step to proceed with the research and to fulfill the requirement of the research. Having drawn inferences from the literature, I would like to summarize the points under this topic here for the audience to get a better understanding about this project as this topic is not much familiar and research in this field is in the growth phase.

Before going to the facts and understanding the methods that others opted for, let me explain to you in brief that adding a watermark to data is similar to installing a lock on entry of the house. The times have changed and with the times, the technology has also evolved and so have the crimes. Therefore to protect our assets our solution should also be advanced and this is what this topic speaks about the different ways that the researchers have developed to tackle the problem of stealing the data, manipulating it and redistributing it illegally by making pirate attacks to it.

With everything going digital post pandemic it therefore demands the security of data even more than before. One familiar solution or method that is available to us to solve this problem is “Steganography or Data Hiding” but as locks on the entry of houses do not provide 100 percent security this method also does not guarantee security cent percent. A research paper written by Ahmed H. Tew k and Khaled N. Hamdy discusses how they have generated a watermark by filtering a PN sequence with a filter that approximates the frequency masking characteristics of the human auditory system. According to them it is then weighted in the time domain for temporal masking. Hence basically they have discussed the detection and accessing the watermarks from attacks by various signal manipulations.

According to them, a pirate can defeat a watermarking scheme in two ways. Either it may manipulate the audio signal to make the watermark undetectable or it may establish that the watermarking scheme is unreliable, e.g., that it produces too many false alarms by detecting a watermark where none is present. Both goals can be achieved by adding inaudible jamming signals to the audio piece. They have proposed the method of where they have taken N. The largest frequency components of an image are modified by Gaussian noise. The gap identified in their research work is that it only modifies a subset of frequency components and does not take Human Visual System into account.

The research paper proposes a spread time echo method by using pseudo noise sequencing for digital watermarking. The research paper have proposed in their paper a blind and audio/speech watermarking algorithm that combines the discrete Tchebichef moment transform (DTMT), the chaotic system of the mixed linear–nonlinear coupled map lattices (MLNCML), and discrete wavelet transform. In addition, the adopted strategy has a blind nature, where no original audio/speech is needed in watermark extraction.

The paper written by F.Benedetto, G.Guinta, A.Neri has proposed audio watermarking signal processing technique to provide a quality assessment of the received audio signal after coding/transmission process. A fragile watermark is hidden in an MP3-like host data audio transport stream (MPEG-1 layer III) using a spread-spectrum approach. At the receiving side, the watermark is extracted and compared to its original counterpart. The Quality of Service assessment is based on the evaluation of the mean-square-error between the estimated and the actual watermark.

But this algorithm proposed by them is designed for and limited to mobile multimedia communication systems and does not apply to all types of audio.

The paper is a study presenting a blind quantum audio watermarking scheme based on quantum discrete cosine transform (qDCT). The quantum audio signal in quantum representation of discrete signal (QRDS) is transformed into a frequency domain using qDCT. The medium frequency components are selected as the target of watermarking. Moreover the proposed scheme employs parallel processing, the intrinsic powerful property of quantum computing, to perform embedding processes efficiently and reduce quantum gates in presented quantum circuits.

The method presented by is complex and complicated due to which watermarking data would become difficult at high frequency.

The paper presents a technique for watermarking that is executed by incorporating multi-level DWT along with the use of multiple images with different sizes as watermarks. But the challenge with the proposed algorithm is it is only restricted to images and has also not clarified whether it is black and white or it implies to coloured images.

Since this research field is in the growth phase therefore there is a lot of categorization and there has been no solution developed that is applicable for all in one category be it the audio or video. Also the categorization is dependent on a different frequency spectrum that makes the solutions more complicated.

CHAPTER 3

APPROACH & METHODOLOGY

1. ALGORITHMIC APPROACH

The encryption of audio signals is a task that requires the utmost optimisation in the user and sender's end. Keeping this in mind we did a survey of many literature papers and articles and landed on the conclusion that in order to maximize the efficiency and minimize the system load on which the program will run it is very important that we find the best suitable algorithm to solve the problem. Therefore after reading about 20+ papers on the matter subject we handpicked 6 such papers that guided us towards a solution/approach we needed.

These papers were titled as mentioned in the following order:

- A.** An Effective Watermarking Method Based on Energy Averaging in Audio Signals
- B.** Digital Watermarks for Audio Signals
- C.** Efficient watermarking algorithm for digital audio/speech signal
- D.** Digital audio watermarking for QoS assessment of MP3 music signals
- E.** A blind quantum audio watermarking based on quantum discrete cosine transform
- F.** Development of an audio watermarking with decentralization of the watermarks

The first paper proposes a spread time echo method by using pseudo noise sequencing for digital watermarking and uses the phenomenon of repetition of sound on reflection from an obstacle and encrypts it using PRN, also known as pseudo random noise. This method uses a signal on the same length as a noise and satisfies it using statistical randomness. Therefore since this algorithm uses statistical randomness, it requires the software to run many patterns and regularities that are non recognizable and therefore rely on the mean of the statistical value. We therefore came to the conclusion that this will use much of the system resources and is hence not variable for low end users.

The second paper elaborates the term “pirate” and how PN sequencing can easily decrypt normal encryption and therefore why it is important to do digital - watermarking. Ignoring the motivation of the paper and focusing solely on the method it discusses we find that the method of focus is PN sequencing. PN sequencing stands for Pseudo-random Noise sequence and uses sets of bits that are statistically meant to be random. This Approach is an improvement on the previous approach as it depends on a function that can be utilized by any software and can run even on low end systems.

The third paper discusses A blind and audio/speech watermarking algorithm that combines the discrete Tchebichef moment transform (DTMT), the chaotic system of the mixed linear–nonlinear coupled map lattices (MLNCML), and discrete wavelet transform (DWT). In addition, the adopted strategy has a blind nature, where no original audio/speech is needed in watermark extraction. This paper came from M. Yamini, H.Karmouni and M.Sayyouri and uses a very well optimized algorithm that not only improves the process of audio encryption but at the same time provides Tchebichef moment transform (DTMT) method to compress the digital images. It uses a novel set of orthogonal moments applied in the fields of image analysis and pattern recognition.

Although this algorithm is extremely fast and provides a solution for the image compression as well, we voted to not use this as the scope of mathematics required to implement the method is way beyond our scope and will not meet/line up with the deadline of the project.

The fourth paper discusses Digital audio watermarking for QoS assessment of MP3 music signals. This is another paper that discusses the type of audio signal that we are aiming at. And at the same time this paper proposes an audio watermarking signal processing technique to provide a quality assessment of the received audio signal after coding/transmission process. But this paper has no mention of any encryption algorithm but uses signal processing to assess the quality of the signal. But since this was the only paper (among few) that talks about the quality assessment of audio signal using an open source software we found this approach to be quite helpful for using in the testing phase of our project.

The fifth paper discusses A blind quantum audio watermarking method based on quantum discrete cosine transform. It uses the integration of LSB (least significant bit) and MSB (most significant bit) based on quantum discrete cosine transform (qDCT). The quantum discrete cosine transform expresses a finite sequence of data points in terms of a sum of cosine functions oscillating at different frequencies. This is a very advanced approach as it requires a very large dataset to fine tune the regression value. It also requires some capital to get the dataset and the software required to work on. But since our work is focused on an open source approach we decided to not go with this approach.

The sixth paper talks about the Development of an audio watermarking with decentralization of the watermarks. The proposed technique is executed by incorporating multi-level DWT along with the use of multiple images with different sizes as watermarks. This approach uses Discrete Wave Transform. Using the same on a multi level signal allows the extraction of multilevel time-frequency features from a time series by decomposing the series as low and high frequency sub-series level by level.

Therefore after analyzing the approach discussed in the above mentioned 6 papers we have come up with the decision to use the method discussed in the 4th paper (QoS assessment) and use the quality assessment of signal processing and how to improve on it from the second paper (PN sequencing).

We found that using PN sequencing to test the encryption with digital watermarking proves to be the most fruitful as pseudo-noise code (PN code) or pseudo-random-noise code (PRN code) has a spectrum similar to the random sequence of bits that the random function provides. Some of the most commonly used sequences in direct-sequence spread spectrum systems are maximal length sequences, Gold codes, Kasami codes, and Barker codes. These are also the same max length sequences that are followed as a protocol by most transmission services so it becomes the perfect approach to carry out the project.

2. ADVANTAGES

The essential advantage of QoS is that it guarantees the availability of servers and the services that depend on it. It facilitates the secure and convenient movement of data over the network. QoS also enables enterprises to make better use of their existing bandwidth rather than upgrading network equipment to increase capacity.

Some of which can be condensed into:

- a. Mission-critical applications have access to the resources they require.
- b. Administrators can manage traffic better.
- c. Organizations can reduce costs by eliminating the need to purchase new network infrastructure.
- d. User experience is improved.

Performance of service tools select packets in order to make the most of their network's limited bandwidth. In other words, the connectivity can only transfer so much data in a given length of time. As a result, QoS tools select packets in such a way that bandwidth is managed to give the best network infrastructure feasible in the time allotted.

Packets relevant to a call, for example, would take precedence over packets connected to an email file. This is due to the fact that a direct transmission that is happening live is a more contemporaneous medium of speech than a method that is then provided by an email, which again must occur in real time. When a packet is lost or interrupted during or after a teleconference, the client application may notice jitter or lag. If packets are missed or delayed during the emailing transaction, they can indeed be delivered later and the terminal will not be affected. They will not see the email until all of the packets have been composed, but someone streaming video will see the packets as they come.

To classify packets, a QoS spatial analysis analyzes the packet headers. Packet headers are chunks of data that notify the application and other communication ports whatever the register holds, where it's going (its destination's IP address), and what it'll be used for. However, for our project which uses digital watermarking of audio signals, we will not require the IP address of the receiver to be used in the code as that function is provided by the transmission services and they take care of such stuff for due to the compliance of their routing protocols.

The QoS tool may also scan the incoming packets and detect if a packet is relevant to video streaming, choosing it above less time-sensitive packets. The shipping and return ids on something like a physical package can be referred to as packet headers. To select priority, the QoS tool modifies a section of the packet header.

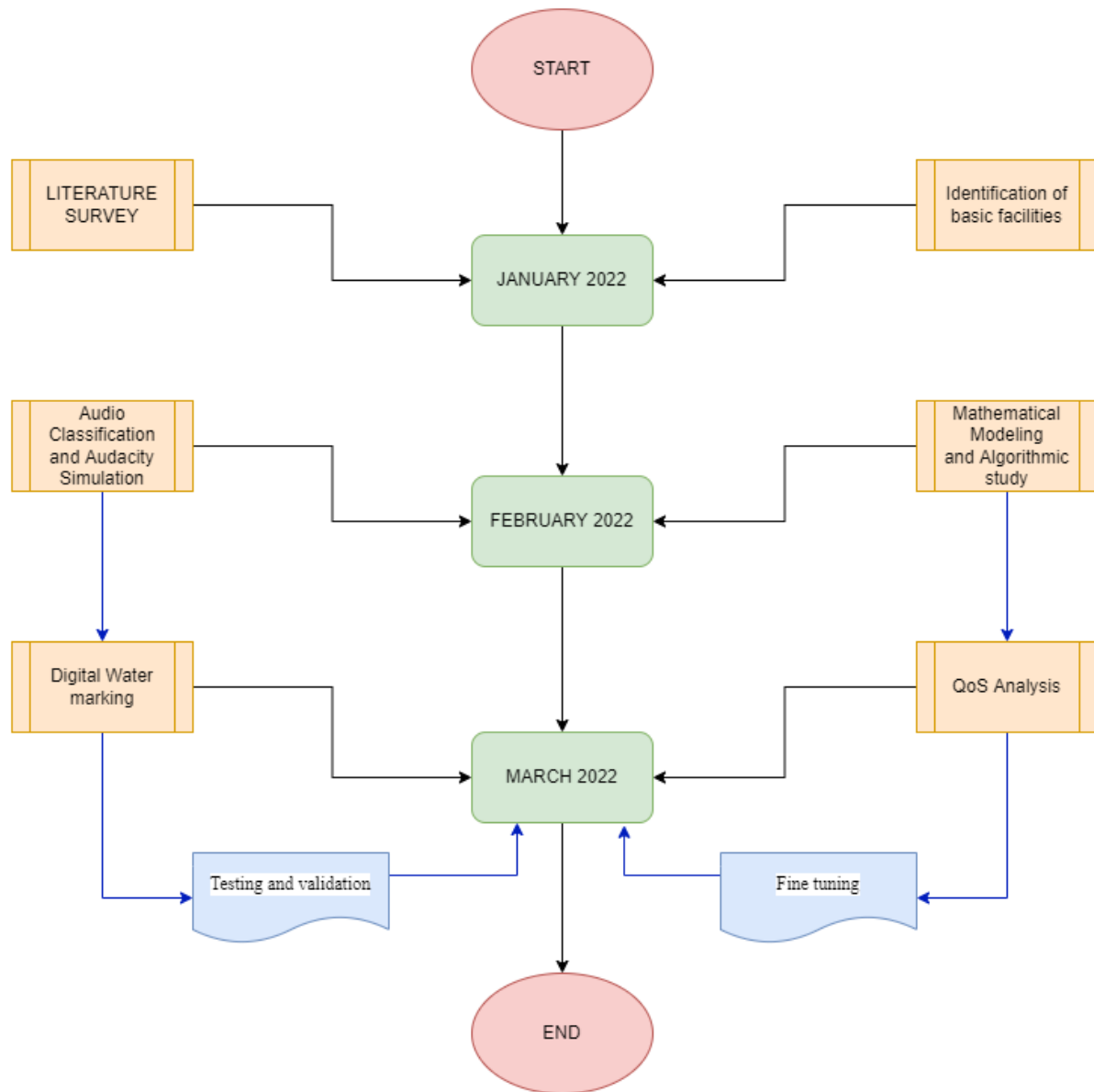
For example, voice traffic can be assigned a higher priority than other types of traffic. Packets are assigned priorities using Differentiated Services Code Point (DSCP) for classification. DiffServ also uses per-hop behavior to apply QoS techniques, such as queuing and prioritization, to packets.

CHAPTER 4

WORKING & ANALYSIS

I. PLANNING

For the working of our project we came up with a methodology framework and divided it into 3 months worth of work. An “.io” diagram showing our framework is attached below:



Working Flowchart

We started with the classification of the audio signal and dividing it by parameters such as their bandwidth, nominal level, power level in decibels (dB), and voltage level. The relationship between power and voltage is determined by the impedance of the signal path. Signal paths may be single-ended or balanced.

After analyzing some research papers we found that audio signals have somewhat standardized levels depending on the application. Outputs of professional mixing consoles are most commonly at line level. Consumer audio equipment will also output at a lower line level. Microphones generally output at an even lower level, commonly referred to as mic level. For our project we will focus on the line level.

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:

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

Table 1.0

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:

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

Table 2.0

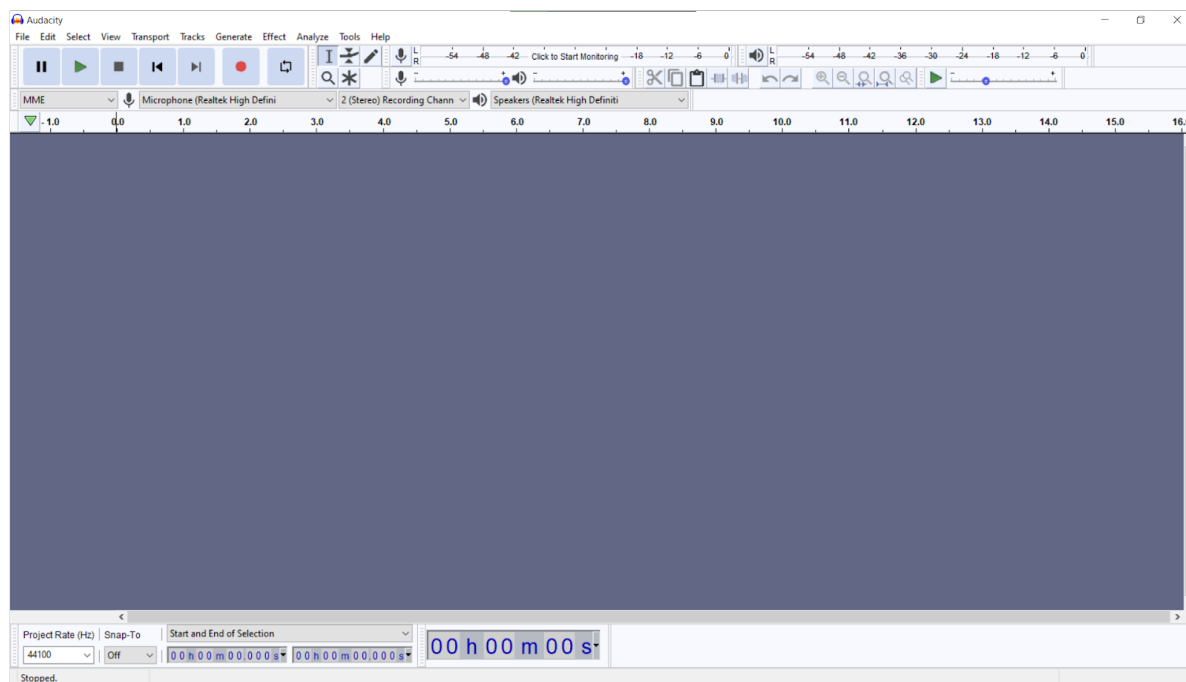
During this we found that any traditional form of watermarking on an audio file can be easily decrypted at 'line level' using software. To prove this we added a water mark at one junction and decrypted the signal using the "same software" and varying the parameters mentioned above. And found that the watermark (called as sis - gen) could easily be retrieved. Then we varied it with 4 other forms of waves (sine, square, sawtooth, triangle) and took the readings (comparison is yet to be done) with gain set at +5 dB and frequency at 440 Hz.

II. ENCRYPTION METHODS

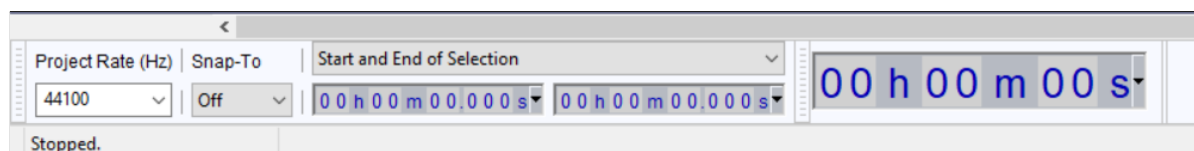
A. USING OVERLAPPING

During our literature survey we came across an existing process of signal encryption that uses a software or tool to overlap an audio signal with another audio signal before transmission and then proceeds to remove that same overlapped signal on the receiver's end.

We used a similar software called Audacity to replicate the same and to find out for ourselves whether the theoretical flaws we found were practical or not.

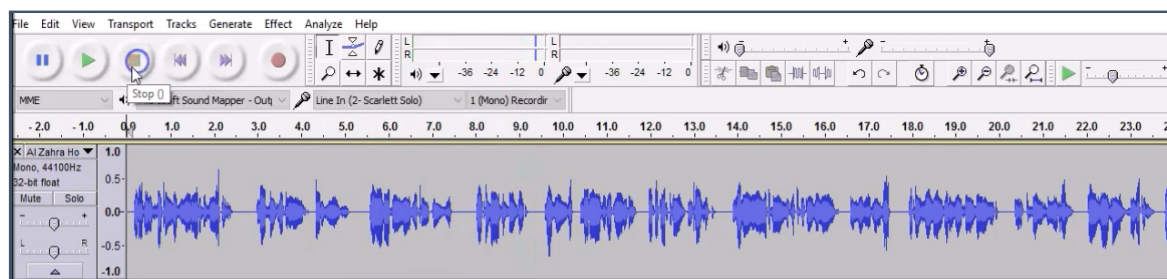


Audacity Homepage



Audacity Editables

For our audio we used a 1 minute clip from the audiobook called “The Adventures Of Sherlock Holmes”. This is an open source audio book available for sampling and free using. We added that audio file as a mono stereo file as tract one. Then we generated a secondary white noise and added it into track two (just below the previous track).

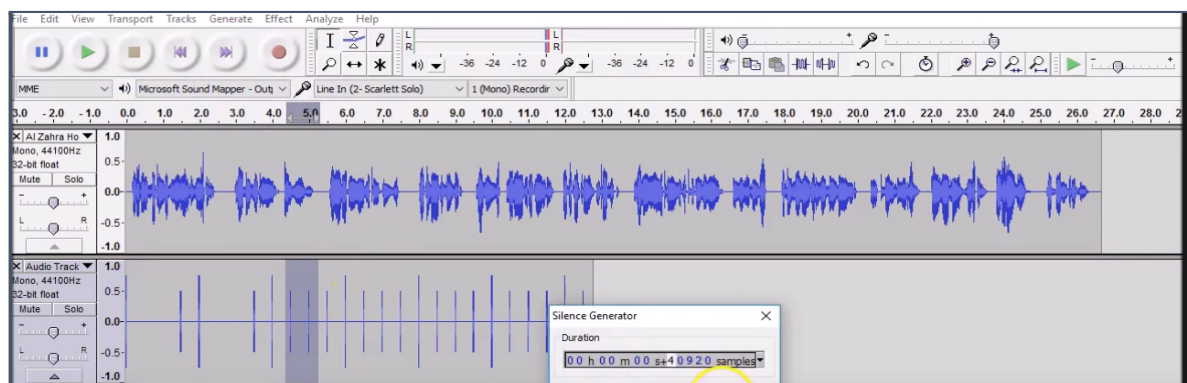


Then we generate a tone (from the software) and superimpose it on the original audio file. In Audacity we can basically change every single parameter of an audio file. For our sampling test we changed it to the following settings:

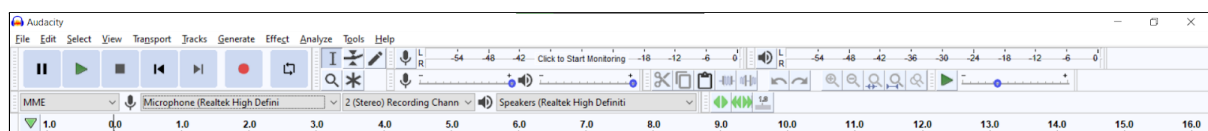
Parameter Name	Value Set
Audio Type	MP3 or WAV
Audio Channel	Mono
Frequency	44100 Hz
Bit point (floating)	32 bit
Mapping (range)	- 1.0 - 1.0
Time Sampled	Duration = 60 seconds

Table 3.0

The result screenshot is attached below:



Overlapped audio



Audacity toolbar

We then generated the traditionally encrypted audio signal and studied its pros and cons. We believe that encrypting an audio file like this has several advantages and disadvantages. But in the domain of encrypting an audio signal the disadvantages top the advantages.

Some of the disadvantages are which are:

1. The original audio signal will be susceptible to noise.
2. Anyone with the audio file can easily see the tune used to encrypt the file and remove it using a mediocre level software.
3. The sender has almost no control over the encryption.
4. The raw audio signal gets quite messy to discern the original content of the file

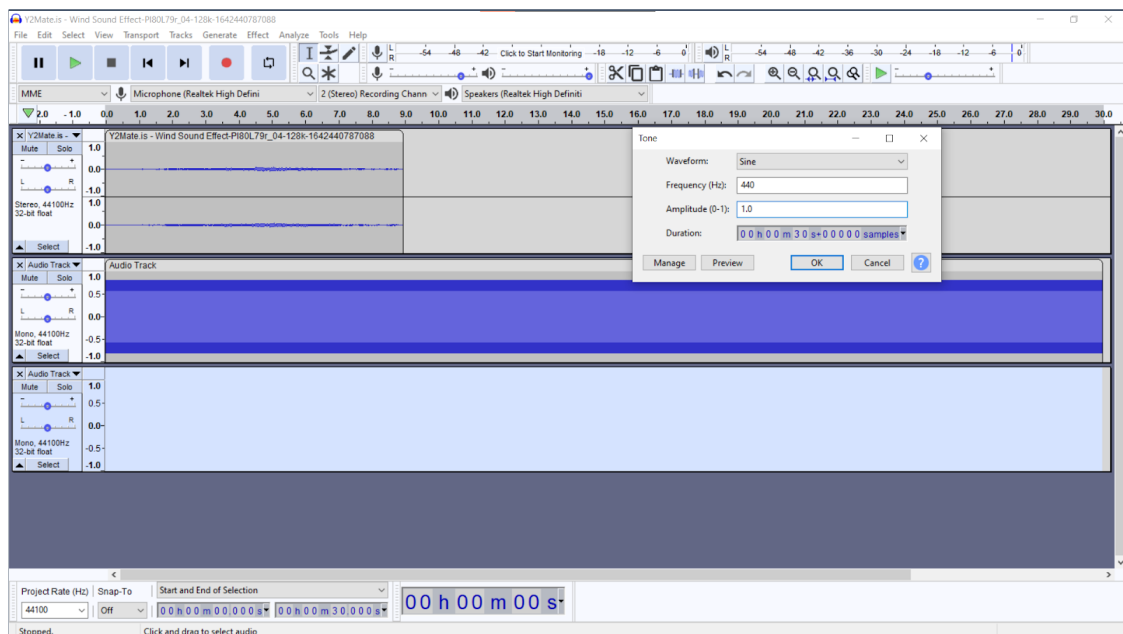
Therefore with these crucial disadvantages we proceeded to test it with another method to see if this method actually be improved upon and whether digital watermarking is actually needed.

B. USING WAVEFORM VARIATION

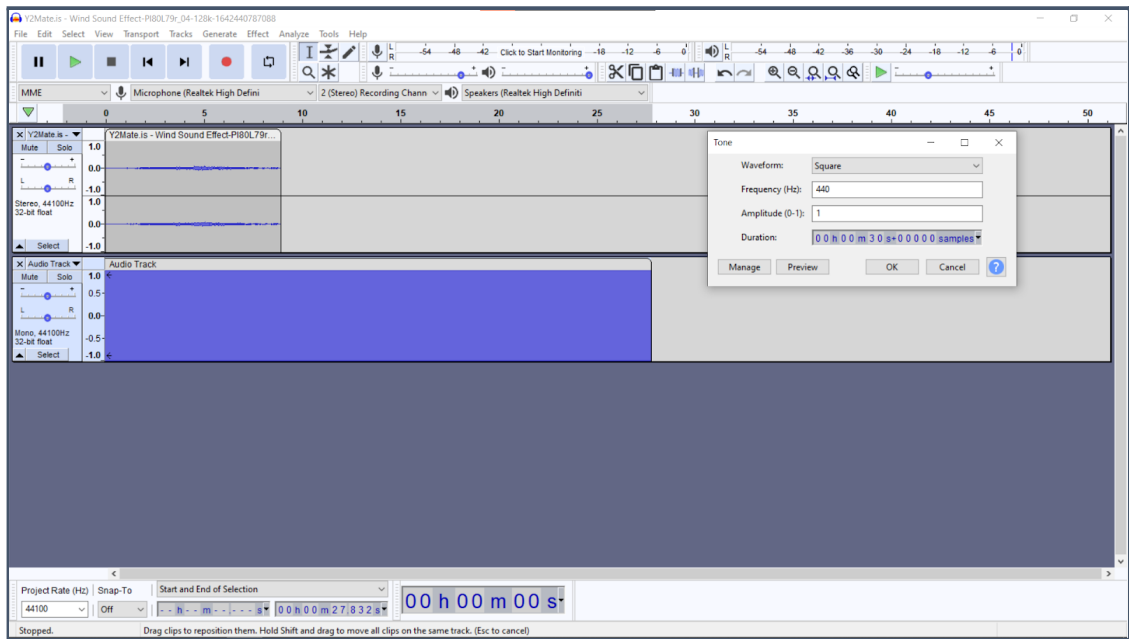
From the first method we saw that one of the major disadvantages was that “A TONE” was being used as the overlapping signal. This in turn generated noise that made the original audio quality bad. However what if we used a single waveform rather than a whole tone.

We used Audacity as before to do the same. We kept our original audio the same but changed the overlapping signal from a tone to a single waveform. We did this with 4 separated waveforms (sine, square, sawtooth and triangle).

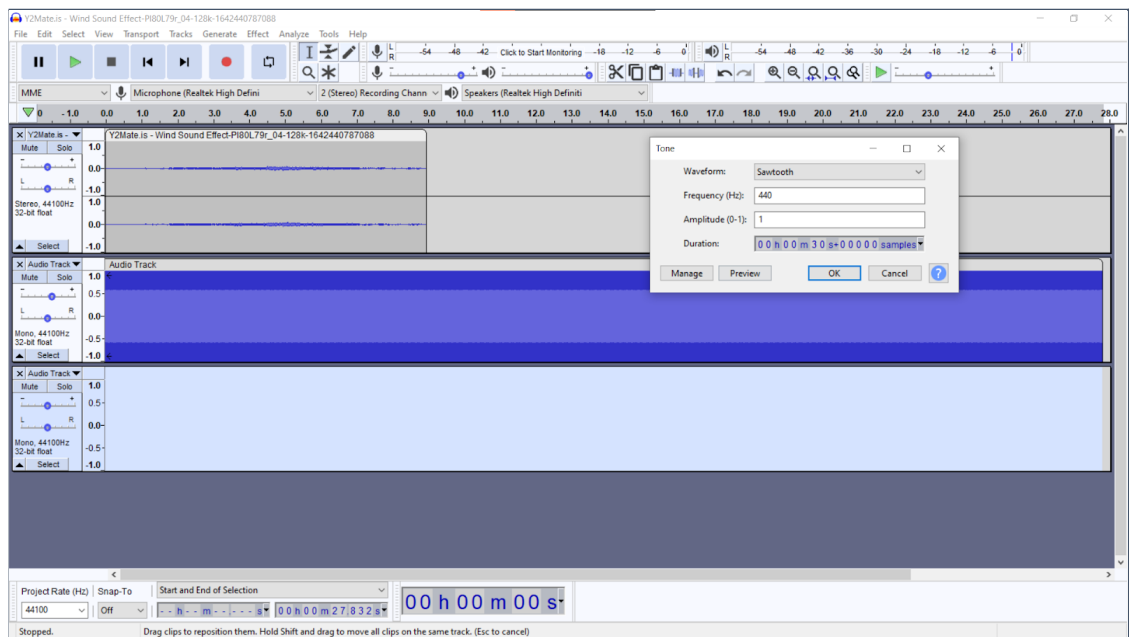
Firstly we used a sine wave (400Hz, 1.0 Amplitude). From this we find that even though the raw audio file ended up retaining its original audio quality it showed no improvement in terms of encrypting the audio. All the open loopholes that were present when using tone overlapping are still present when using a waveform overlapping. The same result was seen while using square waveform, sawtooth waveform, triangle.



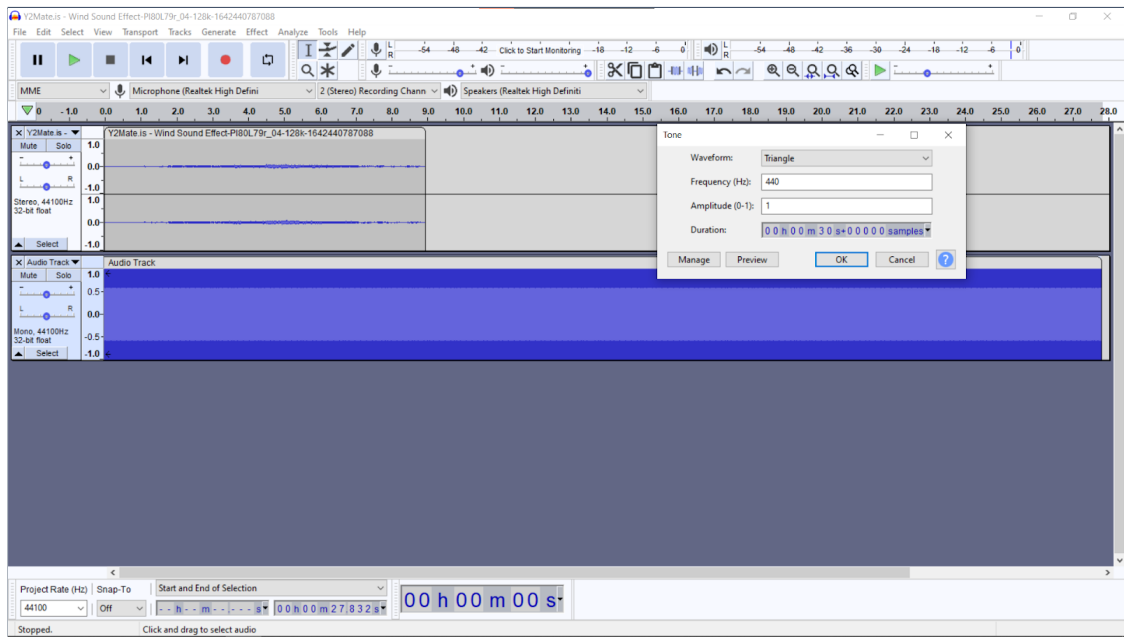
Sine wave overlapping



Square wave overlapping



Sawtooth wave overlapping



Triangle wave overlapping

Therefore after testing it with waveforms we are still left with 3 major disadvantages to this type of audio encryption that make it susceptible to 3rd party attacks and decryption:

1. Anyone with the audio file can easily see the tune used to encrypt the file and remove it using a mediocre level software.
2. The sender has almost no control over the encryption.
3. The raw audio signal gets quite messy to discern the original content of the file

III. CODING

Therefore after analyzing 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.

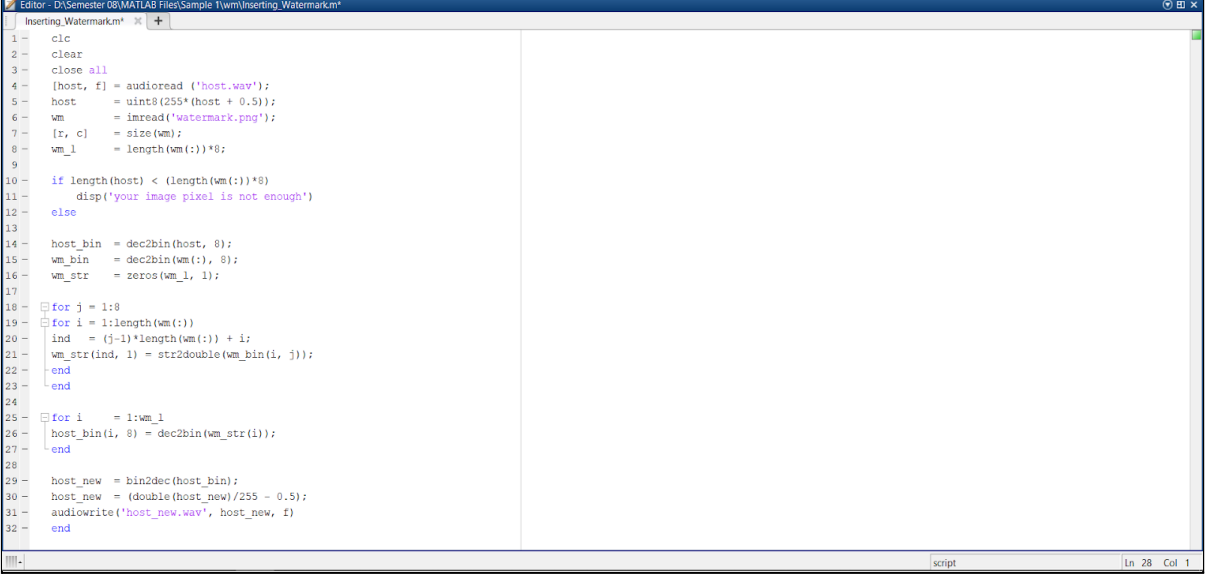
Our project includes 2 MATLAB function files (write) and 1 sample MP3 files (read). It works like the commands WAVWRITE and WAVREAD.

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.

A. INSERTING WATERMARK

The insert watermark code script follows the following hierarchical approach:

- Clear memory and command window
- Load data
- Watermarking
- Prepare host
- Prepare watermark
- Insert watermark into host
- Watermarked host
- Save the watermarked host

A screenshot of a MATLAB script editor window titled 'Inserting Watermark'. The script contains the following code:

```
1 clc
2 clear
3 close all
4 [host, f] = audioread('host.wav');
5 host = uint8(255*(host + 0.5));
6 wm = imread('watermark.png');
7 [r, c] = size(wm);
8 wm_l = length(wm(:))*8;
9
10 if length(host) < (length(wm(:))*8)
11     disp('your image pixel is not enough')
12 else
13
14     host_bin = dec2bin(host, 8);
15     wm_bin = dec2bin(wm(:), 8);
16     wm_str = zeros(wm_l, 1);
17
18     for j = 1:8
19         for i = 1:length(wm(:))
20             ind = (j-1)*length(wm(:)) + i;
21             wm_str(ind, 1) = str2double(wm_bin(i, j));
22         end
23     end
24
25     for i = 1:wm_l
26         host_bin(i, 8) = dec2bin(wm_str(i));
27     end
28
29     host_new = bin2dec(host_bin);
30     host_new = (double(host_new)/255 - 0.5);
31     audiowrite('host_new.wav', host_new, f)
32 end
```

Inserting watermark code

Working of the code:

- 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 “imread” 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:
 - 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 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))”
- Finally host the watermark using the bin2dec() function and specify the data type as “double”.
- End the code block.
- Save the host code.
- RUN the code to insert the watermark.

After running the code the workspace values obtained are attached below.

Workspace	
Name ^	Value
c	50
f	8000
host	62747x1 uint8
host_bin	62747x8 char
host_new	62747x1 double
i	20000
ind	20000
j	8
r	50
wm	50x50 uint8
wm_bin	2500x8 char
wm_l	20000
wm_str	20000x1 double

Workspace (inserting code)

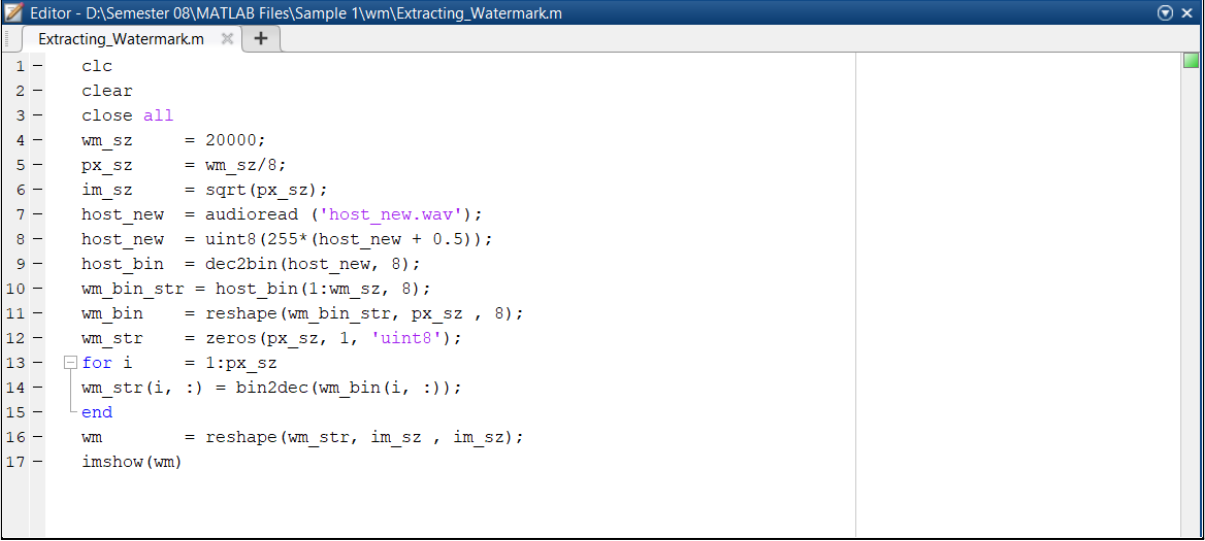


Watermark

B. EXTRACTING WATERMARK

The insert watermark code script follows the following hierarchical approach:

- Clear memory and command window
- Load data
- Prepare host
- Extract watermark
- Display image and supporting html file



```
1 - clc
2 - clear
3 - close all
4 - wm_sz = 20000;
5 - px_sz = wm_sz/8;
6 - im_sz = sqrt(px_sz);
7 - host_new = audioread('host_new.wav');
8 - host_new = uint8(255*(host_new + 0.5));
9 - host_bin = dec2bin(host_new, 8);
10 - wm_bin_str = host_bin(1:wm_sz, 8);
11 - wm_bin = reshape(wm_bin_str, px_sz, 8);
12 - wm_str = zeros(px_sz, 1, 'uint8');
13 - for i = 1:px_sz
14 -     wm_str(i, :) = bin2dec(wm_bin(i, :));
15 - end
16 - wm = reshape(wm_str, im_sz, im_sz);
17 - imshow(wm)
```

Extracting watermark

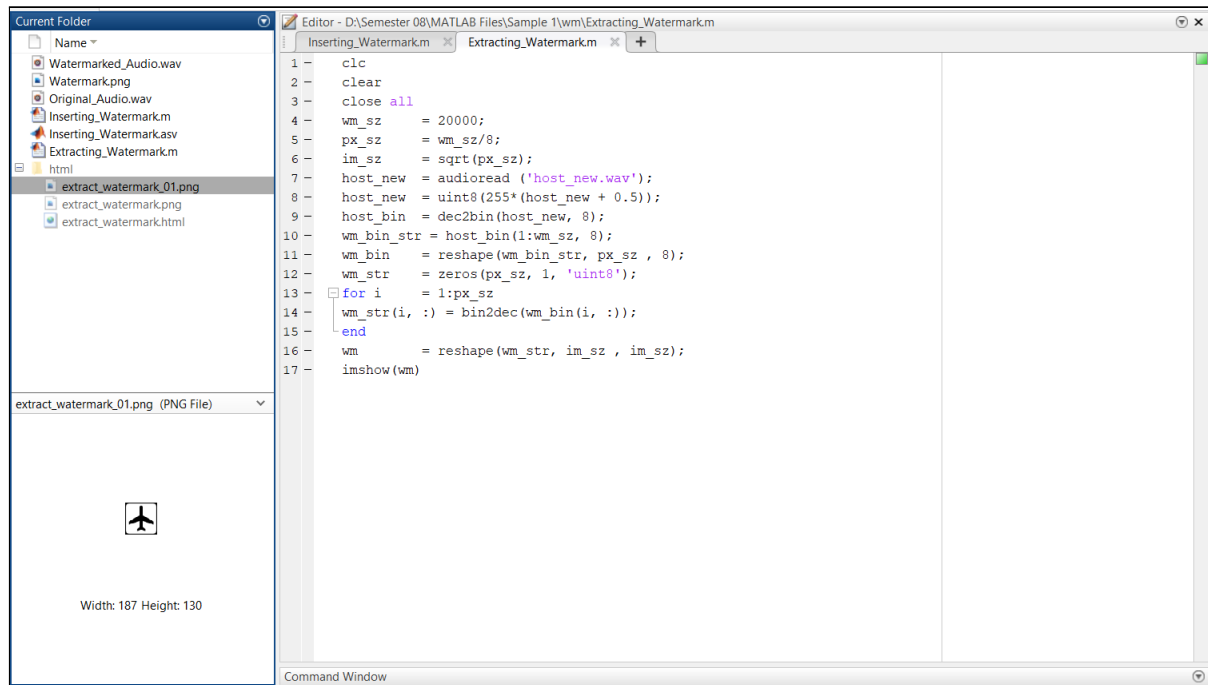
Working of the code:

- 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.
- 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:
 - 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.

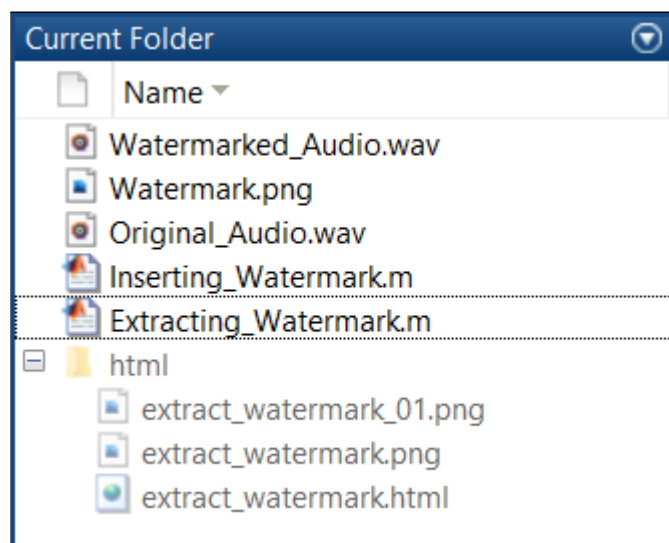
After running the code the workspace values obtained are attached below.

Workspace	
Name ^	Value
host_bin	62747x8 char
host_new	62747x1 uint8
i	2500
im_sz	50
px_sz	2500
wm	50x50 uint8
wm_bin	2500x8 char
wm_bin_str	20000x1 char
wm_str	2500x1 uint8
wm_sz	20000

Workspace (extracting code)



Extracted watermark



Folder screenshot

Note that the HTML File (attached below) stays hidden unless the received specifically wants to access it:

Contents

- clear memory & command window
- load data
- prepare host
- extract watermark
- show image

clear memory & command window

```

clc
clear
close all

```

load data

```

wm_sz      = 20000;           % watermark size
px_sz      = wm_sz/8;        % number of pixels
im_sz      = sqrt(px_sz);    % image size
host_new   = audioread('host_new.wav'); % new (watermarked) host signal
host_new   = uint8(255*(host_new + 0.5)); % double [-0.5 +0.5] to 'uint8' [0 255]

```

prepare host

```

host_bin   = dec2bin(host_new, 8); % binary host [n 8]

```

extract watermark

```

wm_bin_str = host_bin(1:wm_sz, 8);
wm_bin     = reshape(wm_bin_str, px_sz , 8);
wm_str     = zeros(px_sz, 1, 'uint8');
for i      = 1:px_sz % extract water mark from the first plane of host
    wm_str(i, :) = bin2dec(wm_bin(i, :)); % Least Significant Bit (LSB)
end
wm         = reshape(wm_str, im_sz , im_sz);


```

show image

```

imshow(wm)

```



HTML output

#Note

The above HTML snippet shows the live script ONLY TO THE RECEIVER and can be accessed only if he/she wishes to see it and test the authenticity of the encryption.

IV. 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.

Also we drew the inference that using this form of audio encryption solves all the 4 disadvantages mentioned in the overlapping method of 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.

CHAPTER 5

FINAL RESULT & SCOPE

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. We believe that the 21st century has seen a big blast in the era of information warfare and hence protecting the privacy of a user is absolutely essential.

That is why after analyzing 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:

TESTING PARAMETERS	Digital Watermarking Of Audio Signal	Discrete Wave Transform Method	Traditional Overlapping Signal Tone Method
High system specs. required?	NO	YES	NO
Additional hardware required?	NO	YES	NO
Requires integration of AI and ML?	NO	NO	NO
Fluctuating results?	NO	NO	NO
Damage to the original audio?	NO	NO	YES
Receiver's needs integrated?	YES	YES	NO

Table 4.0

REFERENCES

1. "Change Topic: Pseudorandom Noise (PRN) Expansion" (PDF). GPS.GOV. Retrieved July 13, 2011.
2. Public Domain This article incorporates public domain material from the General Services Administration document: "Federal Standard 1037C". (in support of MIL-STD-188)
3. Pi seems a good random number generator – but not always the best, Chad Boutin, Purdue University
4. 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.
5. Yongge Wang. Statistical Testing Techniques For Pseudorandom generation. <http://webpages.uncc.edu/yonwang/liltest/>
6. Yongge Wang: On the Design of LIL Tests for (Pseudo) Random Generators and Some Experimental Results. PDF
7. 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.
8. Knuth, Donald (1998). *The Art of Computer Programming Vol. 2 : Seminumerical Algorithms*. Addison Wesley. pp. 93–118. ISBN 978-0-201-89684-8.
9. N. Suryana, Siaw-Lang Wong (2010). "An efficient compact Tchebichef Moment for image compression": *Information Sciences Signal Processing and their Applications (ISSPA)*, 2010 10th International Conference on
10. 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*
11. 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.
12. 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 Imouzzar Road, Fez, Morocco.
13. 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.
14. Mohsen Yousefi Nejad, Mohammad Mosleh, A blind quantum audio watermarking based on quantum discrete cosine transform, Department of Computer Engineering, Tabriz Branch, Islamic Azad University, Tabriz, Iran.
15. Amita Singha, Muhammad Ahsan Ullah, Development of an audio watermarking with decentralization of the
16. Watermarks, Department of Computer Engineering, Tabriz Branch, Islamic Azad University, Tabriz, Iran