

CHAPTER 1

INTRODUCTION

1.1 GENERAL

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- “The Adventures of Sherlock Holmes” 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.

1.2 NEED FOR DIGITAL WATER WATERMARKING

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 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.

1.3 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 encrypts information that is readable by machine to another form of media. It is governed by certain algorithms that are used to achieve that state in the most optimized manner possible.

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 another such practice where the goal is to make the encryption imperceptible. The watermarking is a technique related to steganography which means to hide the existence of messages in media.

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.

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.

1.4 MAJOR ISSUES IN CURRENT ENCRYPTION

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.

4. Encryptions don't work for systems.
5. Encryptions cannot be audited
6. Encryption does not work against threats made from the inside.
7. Data Integrity is often the biggest question in encryption
8. Most can't prove whether encryption in place is performing to their needs.

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

CHAPTER 2

LITERATURE ANALYSIS

2.1 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 the levels of audio signals lie on a level that is considered a nominal standard level. One such level is called line level. It is the level mostly used by trained professionals that deal with sound mixing, whereas what we as consumers use is often put at a lower line level. On the other hand, the microphone operates at such a lower level that we call it a 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.

2.2 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 [10] discusses how by using a filter that is correctly able to mask the criteria of a temporal mask we can approach the frequency of the human auditory system. Hence basically they have discussed the detection and accessing the watermarks from attacks by various signal manipulations.

According to them it is possible to correctly detect a watermark mainly in 2 ways. One such way to embed it in such a way that the watermark in itself becomes undetectable. Or else make an argument that the watermark is unreliable i.e when tested against a custom input it gives many false alarms. 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 [11] proposes a spread time echo method by using pseudo noise sequencing for digital watermarking. The research paper [12] 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 fourth paper [27] 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 watermarking signal technique to provide a quality assessment of the received audio signal after coding. 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 [31] 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 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 paper [15] presents a technique for watermarking that is executed by incorporating in the general sense a Discrete Wave Transform always returns only a single coefficient to its approximation value. Using the same on a multi level signal allows the extraction of multiple time-frequency features from a time series by decomposing the series as low and high frequency level - by - level.

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.

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- “The Adventures of Sherlock Holmes” 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.

Therefore the third and final 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. [18] 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.

2.3 INFERENCE FROM LITERATURE

Having read and worked practically on so many methods to watermark the audio signals, it was found that Digital Watermarking of Audio Signal was more efficient and reliable in encrypting the audio signals as it retained the audio quality as it is. Moreover it is a simple method and a basic MATLAB coding would work therefore it is not complicated as other proposed methods by various other researchers therefore the only prerequisite is knowing MATLAB and how to code in MATLAB which makes this method more easy and convenient to use unlike other methods. The things to keep in mind is that the images are confined to .png and .jpeg extension and the image size should be less than the original audio size.