National College of Ireland

AES Hybridization with DWT Audio Steganography

MSc Internship
Cyber Security

Ashwin P Patil
Student ID: x17170664

School of Computing
National College of Ireland

Supervisor: Ross Spelman

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Ashwin Prabhugouda Patil		
Student ID:	X17170664		
Program:	MSc Cyber Security	**Year:**	2019
Module:	MSc Internship		
Supervisor:	Ross Spelman		
Submission Due Date:	12/08/2019		
Project Title:	AES Hybridization with DWT Audio Steganography		
Word Count:	5923	**Page Count:**	20

I hereby certify that the information contained in this (my submission) is information pertaining to the research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: ……

Date: ……...

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on the computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

AES Hybridization with DWT Audio Steganography

Ashwin Patil
x17170664

Abstract

Simple text exchanged on the internet can be intercepted and confidentiality can be compromised by an intruder. In this paper, a solution is proposed that uses a combination of encryption and steganography to maintain the confidentiality of the simple text exchanged. From the time people have started using the internet, security has become a major concern. Steganography provides security up to some level, there has been a huge amount of research done in relation to steganography. Steganography is considered to be secure only until someone knows that the steganography is applied, the moment attacker knows that the steganography is applied steganography fails. Steganography can be easily broken, and the original text can be obtained. In the proposed system, if the intruder/attacker breaks steganography, he/she will not be able to get the original text as it would be encrypted. The proposed technique provides a high quality of Peak Signal-to-Noise Ratio (PSNR) and Signal to Noise Ratio (SNR) when steganography is applied. There is no major audible distortion after the encrypted text is hidden in the audio file.

1 Introduction

The internet has evolved rapidly since the time it was made available for public use; security has always been a concern. Billions of people use the internet, terabytes of information are exchanged every day. As the number of people and the amount of data exchanged through internet increases, information security becomes a huge issue.

Confidentiality, Integrity, and Availability (CIA) are the key pillars of information security. Simple text exchanged on the internet can be intercepted and confidentiality can be compromised by an intruder. Hence, securing the confidentiality of the information becomes vital. There are many techniques that can be applied to maintain the confidentiality of the information. Steganography is one of such techniques that provide confidentiality by hiding the text or a file in another host/cover file such as image, audio or a video file. Encryption is another technique by which confidentiality can be maintained, the data or text is converted into the unreadable or encoded form using the encryption keys.

Redundancy is the factor that makes audio and video files an excellent carrier for the purpose of steganography (Asad et al., 2011). The cover audio file used before applying steganography and after applying steganography sounds the same, due to the presence of redundancy (Asad et al., 2011). The Human Auditory System is more sensitive than the Human Visual System, as a result, audio steganography is considered to be challenging than video or image steganography (Gopalan, 2003). There has been a lot of research done in the field of steganography and encryption, but the attackers always find new ways of exploiting the known and unknown vulnerabilities.

The objective of the proposed system is to use the combination of encryption and steganography to maintain the confidentiality of the simple text exchanged. Steganography provides a certain degree of confidentiality but once the attacker knows that the steganography is applied, he/she can break the steganography easily. A solution is proposed that uses both encryption and steganography to maintain the confidentiality of the simple text exchanged. In the proposed approach, simple text is encrypted using the AES algorithm and then the encrypted text/ciphertext is embedded into an audio file using DWT algorithm.

When this approach is applied, if the attacker can break the steganography there will be another layer of protection, as the text would be encrypted before steganography is applied.
The audio steganography is considered to be secure because most of the hackers do not suspect the presence of a hidden message in an audio file. The proposed methodology must be applied without degrading the quality of audio. If the quality of the audio is degraded and there are noticeable changes in the cover audio file, it causes suspicion.

2 Related Work

To appreciate the novelty of the paper, it is important to pursue detailed literature review to comprehend the related work and efforts that were made by the authors who have published the papers in the field of encryption and steganography. It is possible to discover or invent new approaches or enhance the existing work only by studying the previous research done in the respective fields.

2.1 Steganography

Steganography is at the core of the proposed methodology, the method of hiding data or information in a cover audio, video or image file is called steganography. Steganography is often confused with cryptography, but they are very different from each other.

2.1.1 Audio File

Human Auditory System (HAS) is considered to be more sensitive than the Human Visual System (HVS), as a result using an audio file for steganography is a tough task. According to (Asad et al., 2011), audio steganography can be made possible due to the presence of redundancy. A technique that works against the HAS should be used to perform audio steganography, the technique should gratify capability, transparency, and robustness (Asad et al., 2011). The amount of information that can be embedded into a cover file is called capability, how well the information is embedded is called transparency and the capability of the embedded secret to withstanding the attacks is called robustness (Asad et al., 2011).
There are multiple audio file formats that are available, the most popular once used for steganography are .wav and .mp3. In the paper "Steganography implementation on android smartphone using the LSB (least significant bit) to MP3 and WAV audio (Lindawati and Siburian, 2017)" the authors have used both .wav and .mp3 files as a cover file for steganography. They have used PSNR (Peak Signal to Noise Ratio) value to measure the quality of reconstructed the audio file. The discoveries made from this paper are that, if the PSNR value is less than 30 dB the steganography is of poor quality and the audio concealment quality is better in WAV files than in the MP3 file format (Lindawati and Siburian, 2017).

2.1.2 DWT Algorithm

Applying cryptography is not enough while exchanging sensitive information through the internet. Cryptography makes the information secure, but cryptography can be broken with the evolution of computing power (Surse and Vinayakray-Jani, 2017). This is mentioned the paper "A Comparative Study on Recent Image Steganography Techniques Based on DWT (Surse and Vinayakray-Jani, 2017)" the authors conclude that using DWT algorithm for steganography makes it more secure and robust for image steganography (Surse and Vinayakray-Jani, 2017).

The authors (Geethavani et al., 2013) have come up with a technique, which uses the Blowfish algorithm for encryption of the data and DWT algorithm to hide the encrypted data into audio. Initially, LSB (Least Significant Bit) algorithm was used for audio steganography, it is simple to perform steganography with LSB but leads to change in signal. The authors state that an effective audio steganography technique ought to provide more payload, capacity, transparency, and robustness (Geethavani et al., 2013). To overcome the disadvantages of Short-Time Fourier Transform (STFT) and to analyze the time-frequency signals, non-stationary representation of the signal, the authors used a new algorithm called Discrete Wavelet Transform (DWT). Authors claim that DWT algorithm requires optimal resources and takes less computation time, it is simple to implement as it can calculate the wavelet transform quickly and is based on sub-band coding. Multiple trials were led to prove the proficiency of the system proposed by the author, Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) are the two metrics used to compare the quality of compression (Geethavani et al., 2013). By analyzing the PSNR and MSE values, it is renowned that there is not a visible difference between the normal audio file and the audio file after applying steganography. The below graph represents the PSNR value for multiple types of cover files, from the graph it is clear that the PSNR value is not of the best quality and there is room for improvement.

Audio file	PSNR
Hip-hop	43.65
Jazz	63.18
Pop	57.52
Rock	33.99

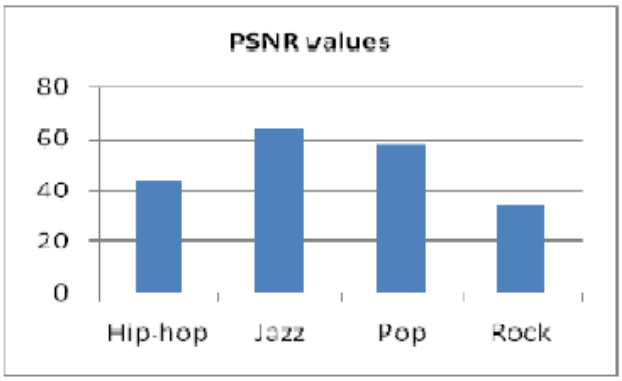

Figure 1: Visual Representation of PSNR Value (Geethavani et al., 2013)

The authors settle that the DWT algorithm is one of the finest algorithms that can be used for audio steganography.

The most common and simplest technique to perform audio steganography is LSB technique. The authors (Rajput et al., 2017), in the paper "An Efficient Audio Steganography Technique to Hide Text in Audio" allusion that LSB is easy to implement but the major drawbacks of applying LSB for audio steganography is, it has a very low embedding rate and low robustness (Rajput et al., 2017). Hence, two new algorithms were proposed by the authors. From this paper, it is clear that the LSB technique is not the best technique to use for audio steganography.

A novel technique to hide an image in an audio file considering least significant bit by using DWT is proposed by the authors (Gupta and Sharma, 2014) in the paper" DWT and LSB Based Audio Steganography". LSB technique is considered as the most straight forward and common for steganography but it is not secure. The message/data is embedded with sequence-mapping technique in the bit of a cover-audio (Gupta and Sharma, 2014). Due to the simplicity of the LBS algorithm, the attacker can decode the message with ease. The authors propose that the audio signal is read and converted into binary form, later embed the image file and convert it into binary and apply DWT algorithm by taking the higher frequency. The original message can be obtained by performing the steps in a reverse manner. Using this technique, the authors are trying to hide the data in an audio file in a manner that there are no noticeable changes to the audio file after embedding the message

(Gupta and Sharma, 2014). They also recommend that the hidden message would be more protected if it was encrypted before embedding it so that the attacker who decodes the message will obtain the encrypted form of message which is of no use to the attacker. According to the authors, the proposed technique is better as it uses DWT algorithm (Gupta and Sharma, 2014).
All the discoveries made by examining the above-mentioned papers, suggests that considering DWT algorithm for steganography would be the right decision.

2.2 Encryption

Encryption is one of the most important parts of the proposed methodology, the technique of converting plain text into an unreadable format using encryption keys is called encryption. The original message can be obtained by using the decryption key, this is called decryption. Encryption provides confidentiality to the information being exchanged.

2.2.1 AES algorithm

Confidentiality is one of the major concerns of any digital data. In the paper "AES Hybridization with Genetic Technique for guarded Image Transmission" authors (Bindra and Bawa, 2018), have proposed a novel technique of using a combination of encryption and steganography to increase the security and confidentiality of the data. They have used the Advanced Encryption Standards (AES) algorithm for encrypting the text, the encrypted text is embedded in an image using a genetic algorithm (Bindra and Bawa, 2018). The authors found that by using the hybrid technique proposed they were able to provide more guarantee and security to the digital data transferred.
There are multiple cryptographic algorithms available to protect the confidentiality of the data, they are chosen based on user requirement. The authors (Semwal and Sharma, 2017) compare various cryptographic algorithms in terms of their features and discuss their performance cost to determine the most suitable algorithm for different operations. The algorithms chosen were DES, 3DES, Blowfish, RSA, IDEA, CAST128, AES and ABE. Comparative analysis was performed based on attributes like key size, the number of rounds, block size, different vulnerable attacks and security level. The discoveries that were made from this paper are, each of the algorithms have their own strengths and weaknesses. They are chosen based on the user requirements, the blowfish algorithm is fit to be used in embedded applications and the devices that have small memory. RSA algorithm takes a large amount of encryption and decryption time (Semwal and Sharma, 2017). AES algorithm has the highest avalanche effect, so it is ideal to be used with an application where privacy and integrity are of high interest (Semwal and Sharma, 2017). The below table represents all the algorithms that were compared along with the security level provided by each of them and the possible attacks that can be performed on them.

TABLE-Ishows comparison of various key features of different encryption algorithms

Algo & Yr	*Block Size (Bits)*	*Key Len (Bits)*	*No Of Rounds*	*Security level*	*Attacks vulnerable*
DES (1977)	64	56	16	Not adequate	Brute force, Differential Attack, Men in Middle attack
3-DES (1978)	64	112-168	48	Vulnerable	Brute force, Differential Attack
CAST-128 (1996)	40-128	128	12-16	Vulnerable	64 bit version is vulnerable to linear attack
IDEA (1991)	64	64-128	5-8	Vulnerable	Linear Attack
AES (2000)	128	128-256	10-14	Excellent	Side Channel Attack
Blowfish (1993)	64	32-448	16	High	Not yet but prone to Key related attacks Boomerang attack
RSA (1977)	Not Fixed	>=1024	Nil	Very High	Brute force & Timing Attack

Source:-www.serc-org\journal\IJSIA\vol19_no4_2015\27.pdf

Table 1: Comparison of encryption algorithms (Semwal and Sharma, 2017)

Least Significant Bit (LSB) algorithm is one of the most common and easiest algorithms used in steganography. The major drawback of LSB algorithm is that it can be easily broken by an attacker, hence the authors (Kanhe et al., 2015) in the paper "Robust Audio Steganography based on Advanced Encryption Standards in Temporal Domain" proposes a technique of combining AES with LSB algorithm. The data is encrypted using AES algorithm, which is considered to be one of the best algorithms for maintaining the integrity and confidentiality of the data later this encrypted data is hidden into the cover file using LSB algorithm. The author uses the above-mentioned technique so that if the attacker/intruder is able to break the LSB algorithm and obtain the data, it'll be encrypted by AES algorithm and hence the attacker/intruder will not be able to get the original data as it'll be encrypted. The main purpose of the proposed system is to prove that by apply encryption and steganography the quality of the file is not degraded. Five different sets are taken and examined using the Signal to Noise Ratio (SNR) plot (Kanhe et al., 2015). The tests prove that by combining AES and LSB algorithm the SNR values are not compromised to a greater extent.

3 Research Methodology

Confidentiality of the information is at stake with the rapid growth of the internet. A lot of efforts and various methodologies that are adopted to deal with the confidentiality issues are discussed in the literature review section. Each of the approaches discussed has its strengths and weaknesses, hence a new approach is essential to tackle the problems in the existing methodologies.

The demonstrated model is proposed in order to provide confidentiality to the information exchanged. The proposed model uses an amalgamation of cryptography and steganography, cryptography is used to encrypt the secret text and steganography is used to hide the encrypted text. Encryption provides confidentiality and steganography keeps the existence of the encrypted text a secret.

For the approach proposed in this paper to be different from all the existing methodologies, there should not be any noticeable changes in the quality of the cover file used. The hypothesis of this paper can be achieved by using a diverse set of tools, software, algorithms, and metrics.

To develop the application MATLAB is required, it is one of the best tools to analyze signal processing and wavelet analysis. It is also used for image, audio, video processing, develop application and develop new algorithms or use the existing algorithms ("What is MATLAB?" n.d.). MATLAB can be downloaded from the MATLAB website.

AES algorithm is applied in order to encrypt the text. From the literature review conducted in the previous section, it is clear that AES algorithm is one of the best algorithms that can be used in a situation when integrity and confidentiality of the data is the top priority. The conclusion to use AES algorithm was made after conducting a literature review of various cryptographic algorithms. From the literature review, it was clear that the selection of the algorithm depends on the operation to be performed by that algorithm. The code for AES algorithm is available on GitHub, it was written by Nicholas Lau. The code was downloaded from GitHub [(Lau, 2017)], and the required modifications must be made. After the modification, the text was successfully encrypted and the ciphertext was obtained.

Two inputs are required for DWT algorithm, one is the ciphertext and another one is the cover audio file. From the literature review in the above section, it was discovered that the ciphertext must be converted to ASCII value and then these ASCII values can be converted into binary. Once the ciphertext is obtained it must be hidden in an audio file, there are a wide variety of algorithms available to perform steganography on an audio file. DWT algorithm was chosen after conducting the literature review, from the literature review it was found that the DWT algorithm is an efficient algorithm to hide data in an audio file. LSB algorithm can be easily applied for the audio file, applying DWT algorithm for steganography was a major task and I was stuck at this point. An attempt was made to contact the authors (Geethavani et al., 2013) of the paper "A new approach for secure data transfer in audio signals using DWT" by email. The question was asked on how they were able to apply DWT algorithm for audio steganography and will they be able to share the knowledge of the same with me, after sending multiple emails there was no response from any of the authors. A repository on GitHub was found which has the code for DWT algorithms, the package was downloaded (Melo, 2016) and the required modifications were made to take the .wave audio file as input.

The metrics for measuring the quality of the steganography are Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and Signal to Noise Ratio (SNR). PSNR is the ratio between the maximum possible value of a signal and the power of distorting noise that affects the quality of its representation ("Peak Signal-to-Noise Ratio as an Image Quality Metric - National Instruments," n.d.). The PSNR ratio is used as a measure of quality between the original and a compresses cover file, it is a measure of peak error. Higher the PSNR value

better the quality of compression or reconstruction ("Compute peak signal-to-noise ratio (PSNR) between images - Simulink - the MathWorks United Kingdom," n.d.). MSE is the cumulative squared error between the compressed and original cover file [("An Introduction to Image Compression," n.d.)]. SNR is the comparison between the level of signal power to a level of noise power, it is represented in terms of decibels (dB). Higher the SNR value better the specification, as there is more useful information than there is unwanted data (industry et al., n.d.).

4 Design Specification

The techniques Design Specification section of the paper is designated to represent and elaborate on the architectural view of the system developed by integrating the algorithms and the components discussed in the methodology section.
The below figure represents the architecture of the proposed system, AES and DWT algorithms are the two major components which have their own functionality. At the sender's end, plain text is taken as input and then the plain text is converted into ciphertext by applying AES algorithm. The resulting ciphertext along with the cover audio file is provided as the input for the DWT algorithm. DWT algorithm embeds the ciphertext into the cover audio file and the resulting steganographic audio file is sent to the receiver.

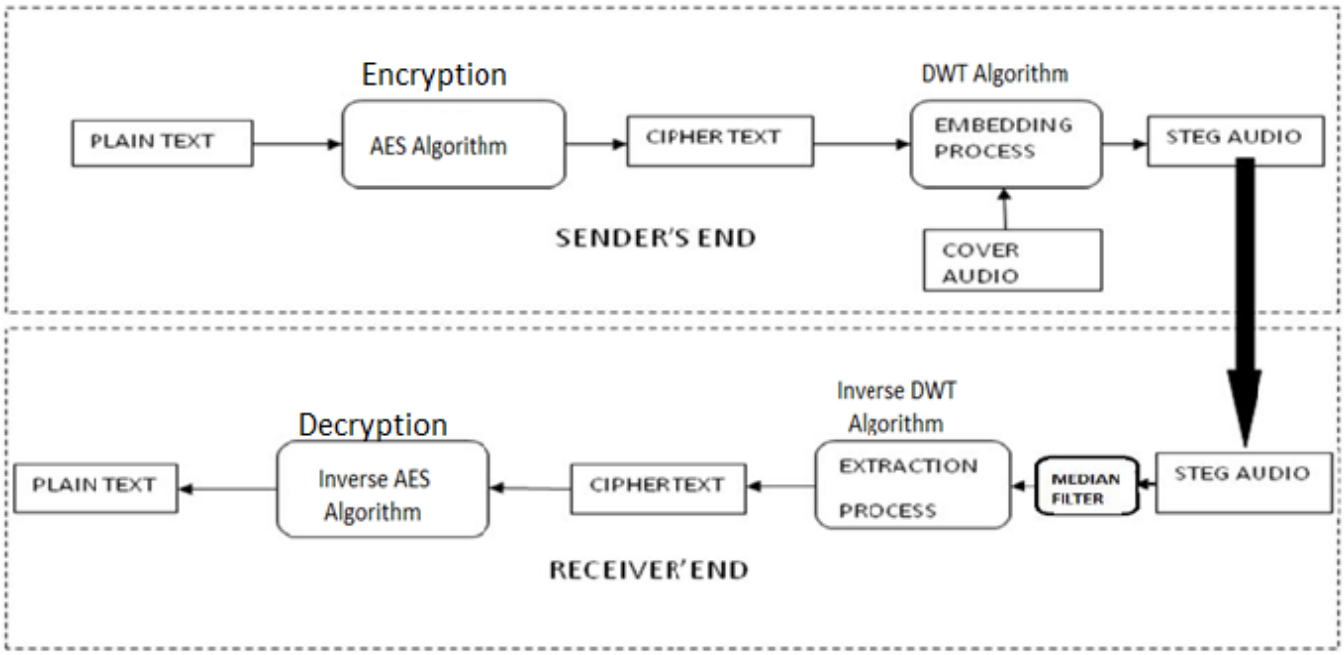

Figure 2: Architectural Diagram of the Proposed System (Geethavani et al., 2013)

At the receiver's end, the steganographic audio file is received. To obtain the original text, the inverse of the process applied to the sender's end is used. Inverse DWT algorithm is applied to extract the ciphertext, the obtained ciphertext must be decrypted to obtain the original plain text. By applying the inverse AES algorithm, plain text is obtained.

4.1 Sequence Diagram

Sequence diagram illustrates the interaction among the objects in sequential order. Two actors are involved in the proposed system, sender and receiver. There are four major steps involved, these steps are showcased in the below-mentioned sequence diagram.

The first step is encryption, the plain text is encrypted to obtain ciphertext. Then the ciphertext is encoded or embedded in the audio file using DWT. Later this steganographic audio file is sent to the receiver, it is decoded and decrypted. This entire process is represented by the sequence diagram below.

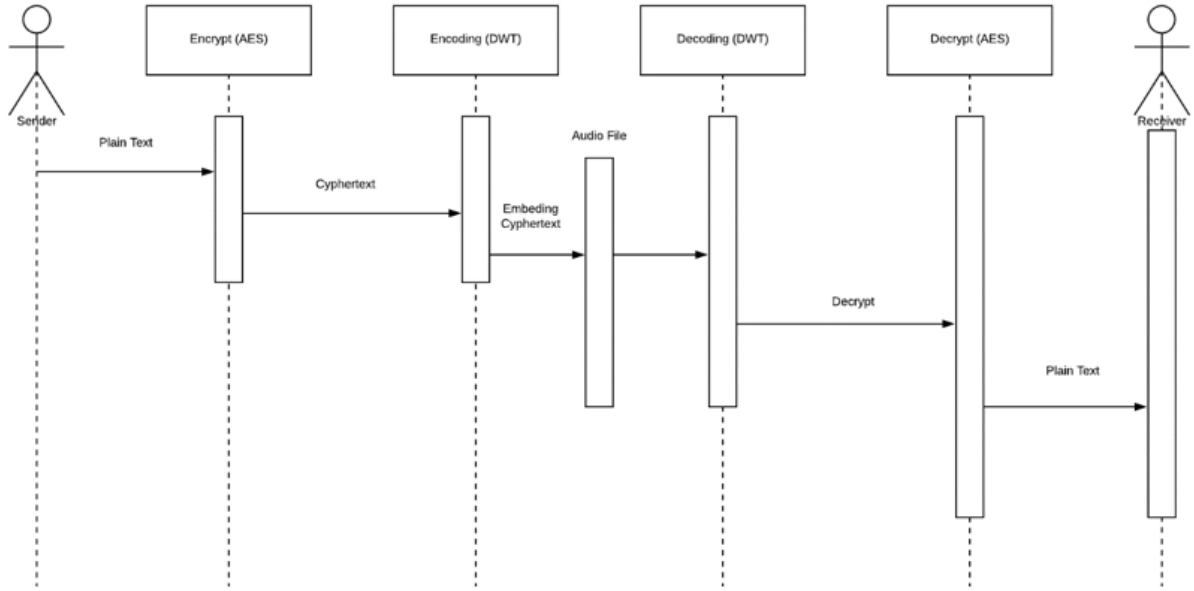

Figure 3: Sequence Diagram of the Proposed System

4.2 UML Diagram

Unified Modeling Language (UML) is a method of visually representing a system in terms of its main roles, actors, classes, and artifacts for a better understanding of the proposed system. The functionalities and importance of each component are represented in the UML diagram. The UML diagram of the proposed system is as follows.

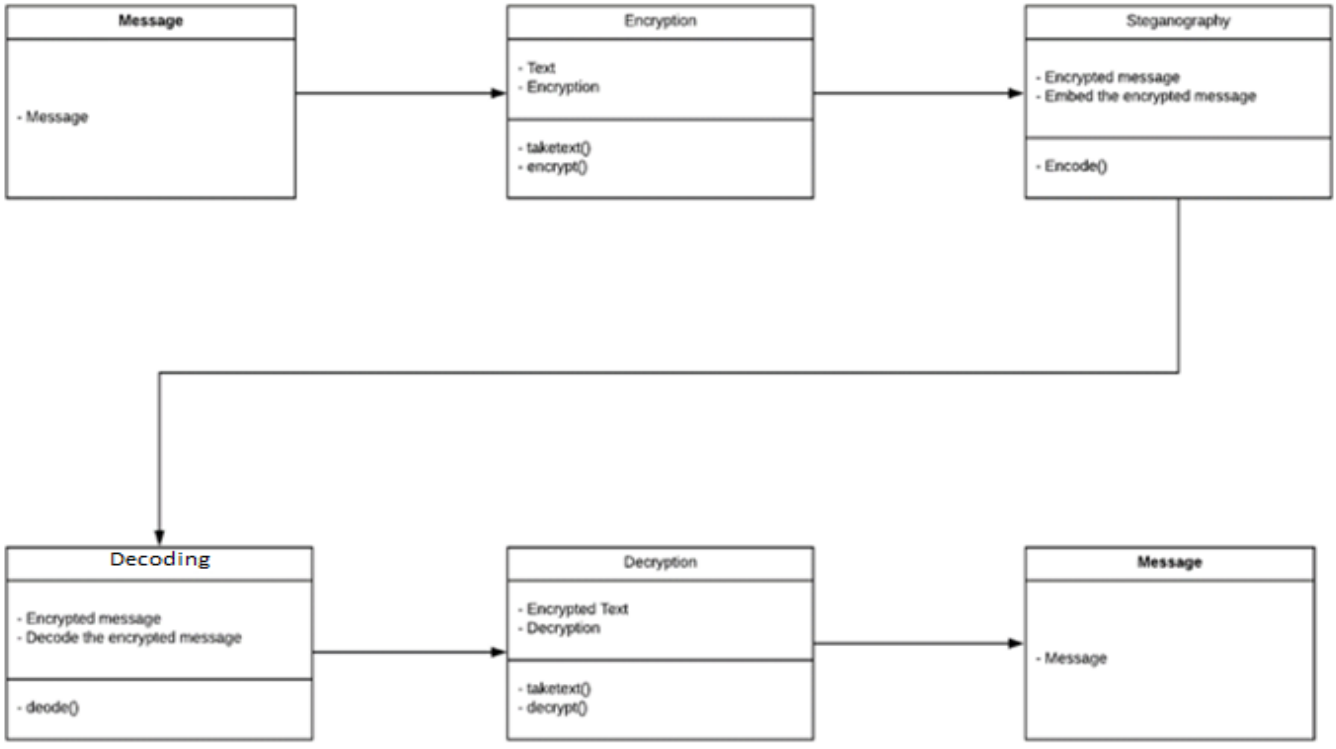

Figure 4: UML Diagram of the Proposed System

5 Implementation

The implementation section consists of the details of the technologies, techniques, and algorithms that are the building blocks of the proposed solution for the research question. MATLAB version R2015a is used to develop the proposed solution. This section involves different phases of a solution such as encryption, steganography (encoding), decoding and decryption.

5.1 Encryption

This is the first step of the implementation phase; the plain text is taken as input and the AES algorithm is used to encrypt the plain text. The code for AES encryption is developed and published by the author Nicholas Lau (Lau, 2017) on GitHub. As AES algorithm is a symmetric encryption algorithm it uses the same key to encrypt as well as for decryption. The steps involved in the working of the same are as follows.

1. Convert the input text into ASCII of int64.
2. Generate a key for encryption.
3. Data is converted into square matrix and an ASCII integer.
4. Add the key to data.
5. Repeat the following in repetition
    a. Shift the row
    b. Create an array based on the column and multiply them
    c. Add the key to the data
6. Shift the row the last time.
7. Add the key to the data the last time.

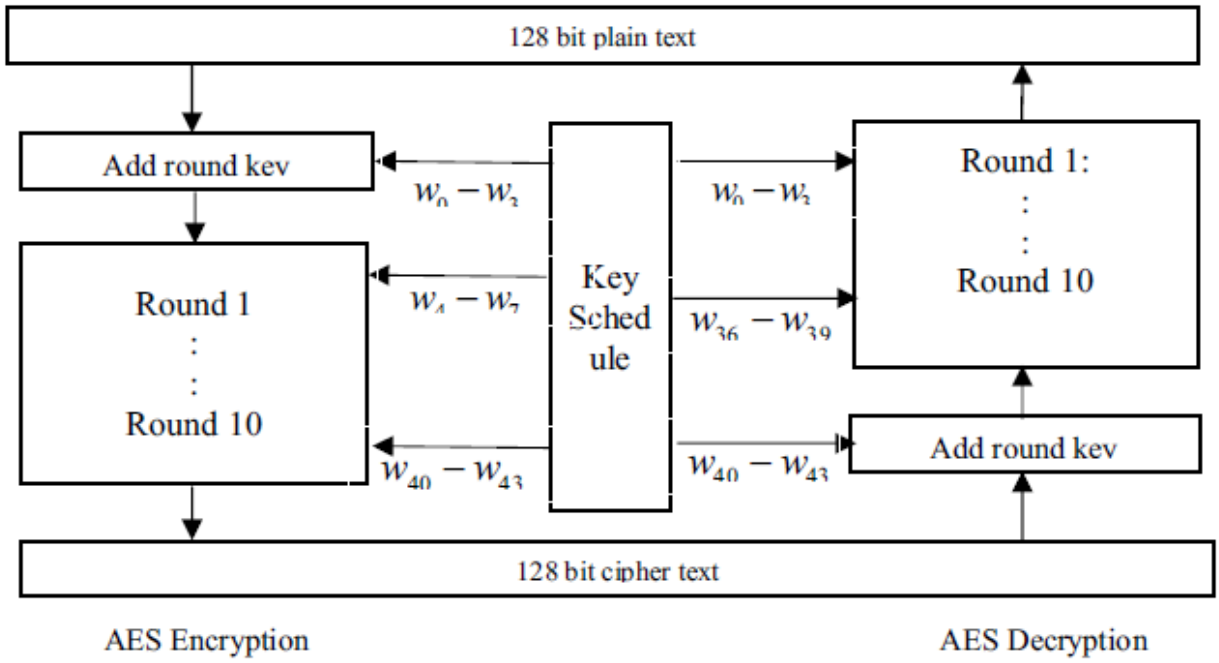

Figure 5: Block Diagram of AES Encryption (Kanhe et al., 2015)

The above diagram represents the block diagram of the AES algorithm. The above-mentioned steps are represented in the diagram below. The figure represents the 128-bit encryption. By

performing the above-mentioned steps on the input text, the ciphertext is obtained. This ciphertext is provided as one of the inputs for the next step.

5.2 Steganography

To apply steganography using DWT algorithm, wave audio files are used as a cover file. The wave audio files are not compressed, and they provide a high sound quality, hence it is appropriate to use them for steganography. To perform steganography using DWT algorithm, two inputs are required. One of the inputs is the ciphertext obtained from AES encryption and the other one is the .wav audio file.

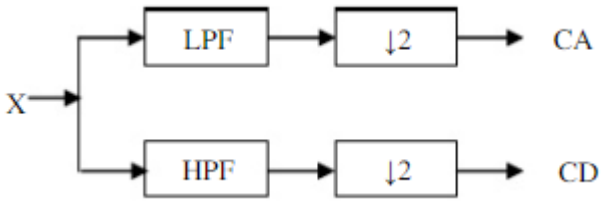

Figure 6: Coefficients of Audio File ("(PDF) A Novel DWT & Correlation Based Audio Steganography | International Journal IJRITCC - Academia.edu," n.d.)

In the above figure, X is the wave audio file; it is divided into Low Pass Filter (LPF) and High Pass Filter (HPF). The wave audio file has two coefficients, they are average coefficient (CA) and detailed coefficient (CD). Out of which proposed system uses only CD coefficient for the purpose of hiding the data ("(PDF) A Novel DWT & Correlation Based Audio Steganography | International Journal IJRITCC - Academia.edu," n.d.).

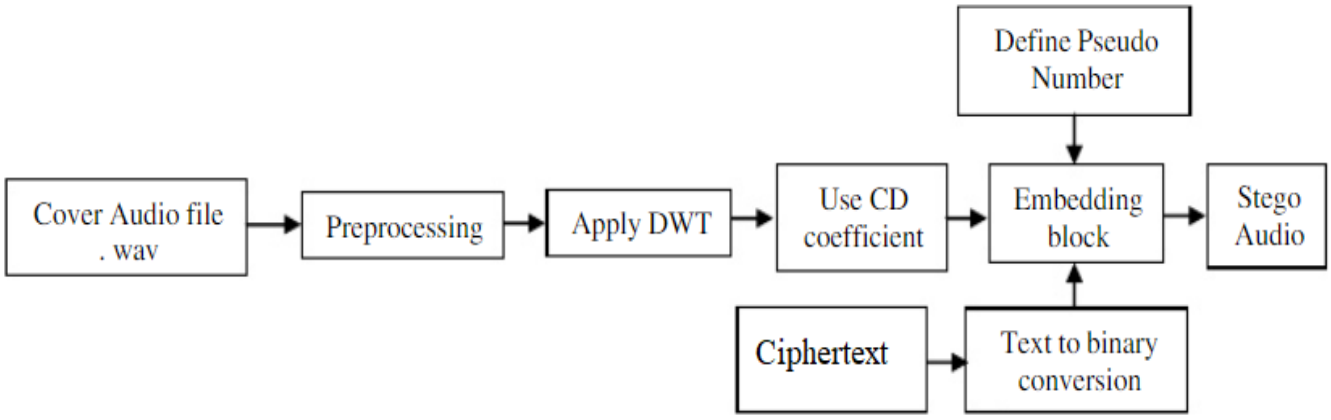

Figure 7: Block Diagram of Embedding Process ("(PDF) A Novel DWT & Correlation Based Audio Steganography | International Journal IJRITCC - Academia.edu," n.d.)

The above figure represents the process of steganography using DWT algorithm. An additional component used here is a pseudo-random number, it exhibits statistical randomness and a secret key is taken as the input to secure the steganography. The ciphertext data obtained in the previous step is converted into ASCII code and this ASCII code is converted into binary for the purpose of hiding it in a cover audio file. The actual hiding process starts now, a stego-key is taken as an input and the ciphertext will be concealed in cover audio by applying the DWT algorithm to produce the stego-audio file. This stego-audio file can be sent to the receiver ("(PDF) A Novel DWT & Correlation Based Audio Steganography | International Journal IJRITCC - Academia.edu," n.d.).

5.3 Decode

Once the receiver receives the stego-audio file, it must be decoded to obtain ciphertext. To extract the ciphertext from the stego-audio correlation theory is used. Inverse DWT algorithm is applied, the correlation between two same size matrices can be calculated by 1Xn carrier audio and a 1Xn stego-audio, the output would be the ciphertext hidden in the stego-audio file ("(PDF) A Novel DWT & Correlation Based Audio Steganography | International Journal IJRITCC - Academia.edu," n.d.). The secret key and the random number are provided as input to decode the stego-audio.

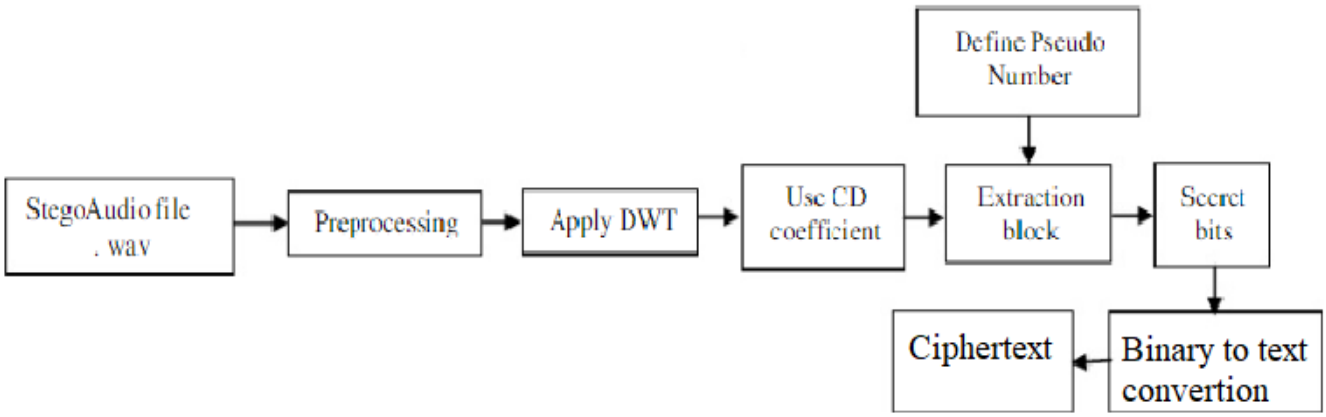

Figure 8: Block Diagram of the Decoding Process ("(PDF) A Novel DWT & Correlation Based Audio Steganography | International Journal IJRITCC - Academia.edu," n.d.)

The ciphertext is obtained by using the extraction block, it uses the correlation theory to obtain the ciphertext. The data extracted from the stego-audio file will be in binary format, hence binary to text conversion must be performed ("(PDF) A Novel DWT & Correlation Based Audio Steganography | International Journal IJRITCC - Academia.edu," n.d.). The binary bits are converted to ASCII values and later these ASCII values are converted to respective characters to obtain the ciphertext.

5.4 Decryption

The ciphertext obtained by decoding the stego-audio must be decrypted using the decryption key with AES algorithm. The following steps must be followed in order to perform the decryption of the ciphertext obtained.

1. Convert the input text into ASCII of int64.
2. Use the key used for encryption as a decryption key.
3. Shift the row the last time.
4. Repeat the following in repetition
    a. Shift the row
    b. Create an array based on the column and multiply them
    c. Add the key to the data
5. Add the key to data.
6. Data is converted into square matrix and an ASCII integer.
7. Add the key to the data the last time.

Decryption is the reverse process of encryption, by following the above-mentioned steps the original text is obtained.

6 Evaluation

The quality of the stego-audio defines the quality of the steganography applied. The quality of the stego-audio can be determined by comparing the quality of the original audio file. Quality of audio file can be measured by various parameters, in this paper PSNR, SNR and MSE are used to determine the quality of the stego-audio.

a. SNR

SNR is the measure used to compare the level of the desired signal to the level of background noise. It can be calculated as the ratio of signal power to noise power. The formula for calculating it is as follows.

$$SNR = \frac{Psignal}{Nsignal}$$

P is the average power. The power ratio between meaningful information and unwanted signal.

b. PSNR

PSNR is the ratio between the maximum possible value of a signal and the power of distorting noise that affects the quality of its representation ("Peak Signal-to-Noise Ratio as an Image Quality Metric - National Instruments," n.d.). The PSNR ratio is used as a measure of quality between the original and a compresses cover file, it is a measure of peak error. Higher the PSNR value better the quality of compression or reconstruction ("Compute peak signal-to-noise ratio (PSNR) between images - Simulink - the MathWorks United Kingdom," n.d.), in some cases it might not be true.

$$PSNR = 10log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$

c. MSE

The average of the square of errors is called MSE (Mean Squared Error). It is a risk function, corresponding to the expected value of the squared error loss. MSE is the cumulative squared error between the compressed and original cover file.

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

MSE is calculated by using the above-mentioned formula.

d. Spectrogram

Short-time Fourier transform of a signal is computed by Spectrogram ("spectrogram (Signal Processing Toolbox)," n.d.). Below is the spectrogram for the original audio file.

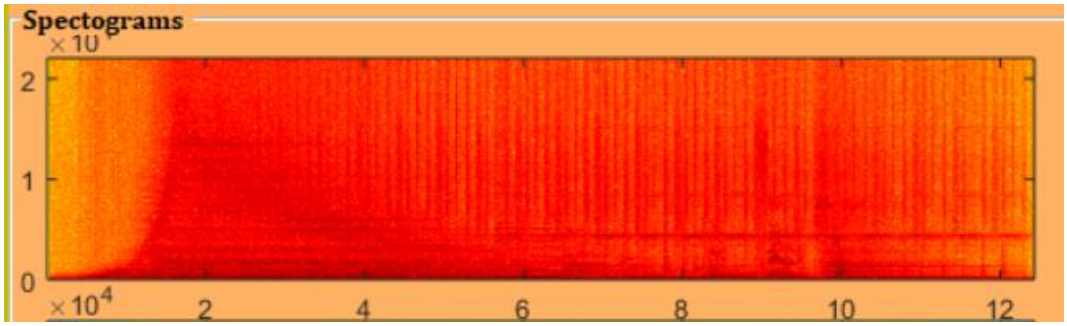

Figure 9: Spectrogram for Original Audio File

6.1 Case Study 1

Multiple tests are conducted by taking the input text of different size and the corresponding PSNR, SNR, MSE values and time is noted down to analyze.
A simple text of size 1.28 KB is encrypted and then it is hidden in the original audio file. Below is the resulting spectrogram. PSNR, SNR, and MSE values are 80.25, 63.88 and 9.39 respectively. The resulting spectrogram can be used to compare it with the spectrogram of the original audio file. The difference can be observed by comparing both the spectrograms.

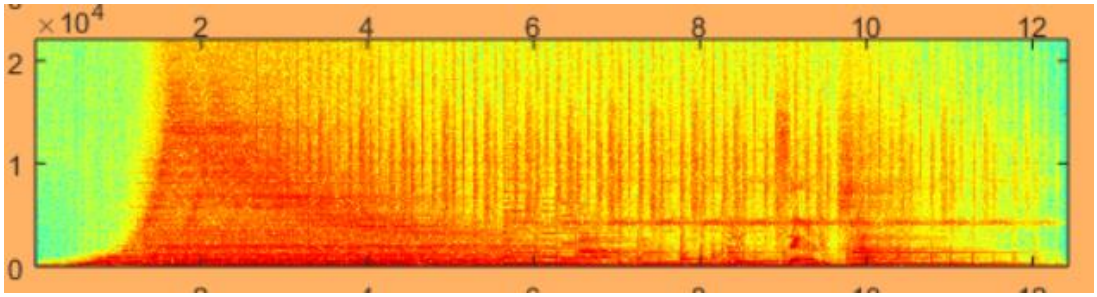

Figure 10: Spectrogram for Stego-Audio in Case 1

6.2 Case Study 2

A simple text of size 0.15 KB is encrypted and then it is hidden in the original audio file. Below is the resulting spectrogram. PSNR, SNR, and MSE values are 89.41, 73.05 and 1.13 respectively. The resulting spectrogram can be used to compare it with the spectrogram of the original audio file and with case 1.

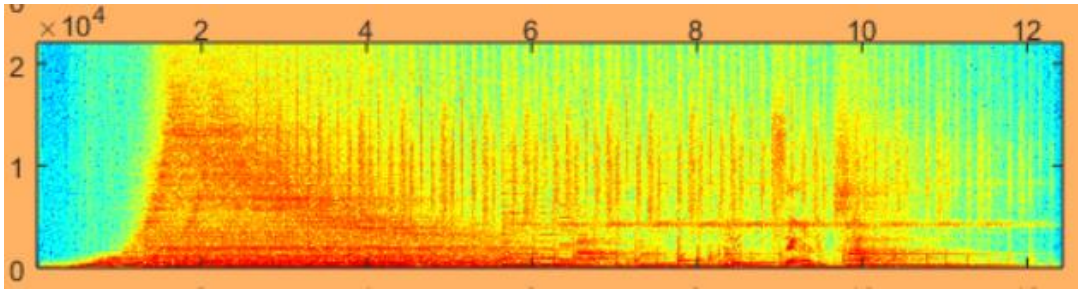

Figure 11: Spectrogram for Stego-Audio in Case 2

6.3 Discussion

By conducting the above test cases the following table can be obtained. The below table represents test cases for different text sizes and their corresponding PSNR, SNR, MSE, encoding and decoding time.

Text Size (KB)	PSNR	SNR	MSE	Time to Encode	Time to decode
1.28	80.25	63.88	8.6	0.86	0.18
0.15	89.41	73.05	1.13	0.51	0.7
1.88	78.53	62.17	9.36	1.04	0.18
0.112	90.62	74.26	1.39	0.48	0.13

Table 2: Test Cases

The graph in the figure 12 is generated from the table 2, a graph is plotted for PSNR and SNR values with respect to text size. From the graph, it is evident that greater the text size, lower the PSNR and SNR values.

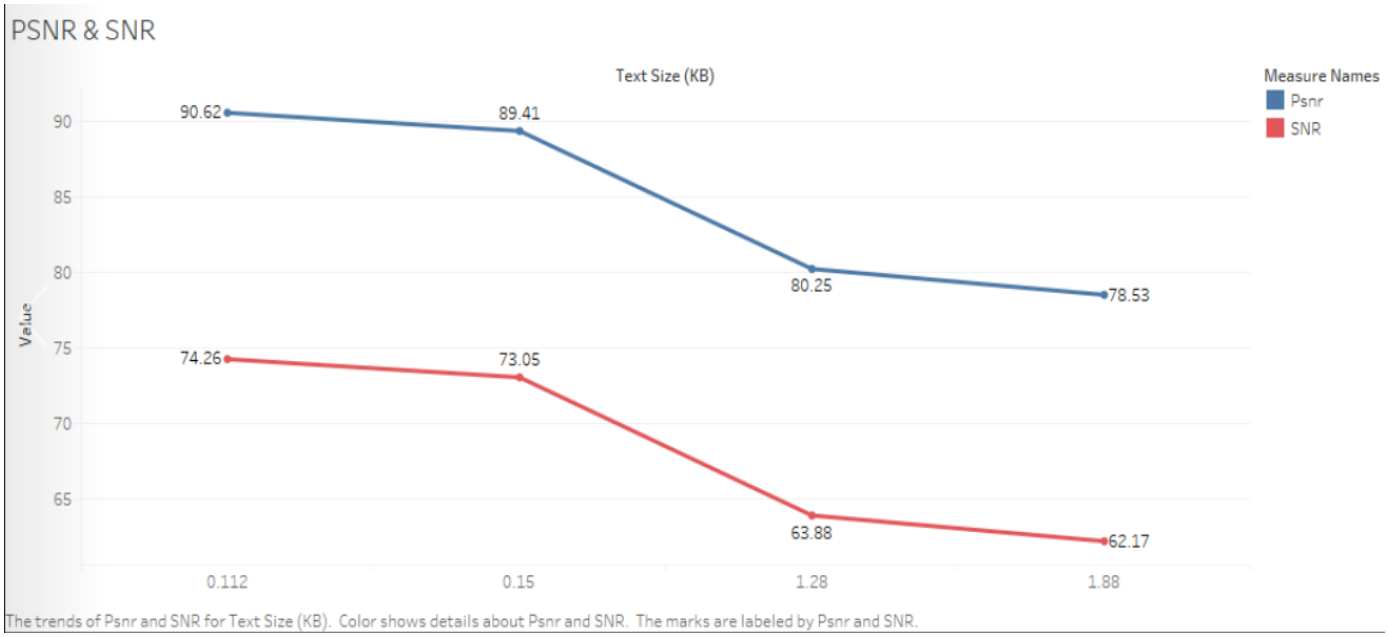

Figure 12: PSNR and SNR Graph

MSE is the mean square error, graph in the figure 13 represents how MSE value varies for the text of different size. From the graph, it is clear that as the size of the text increases the MSE value also increases i.e. MSE is directly proportional to size of the text.

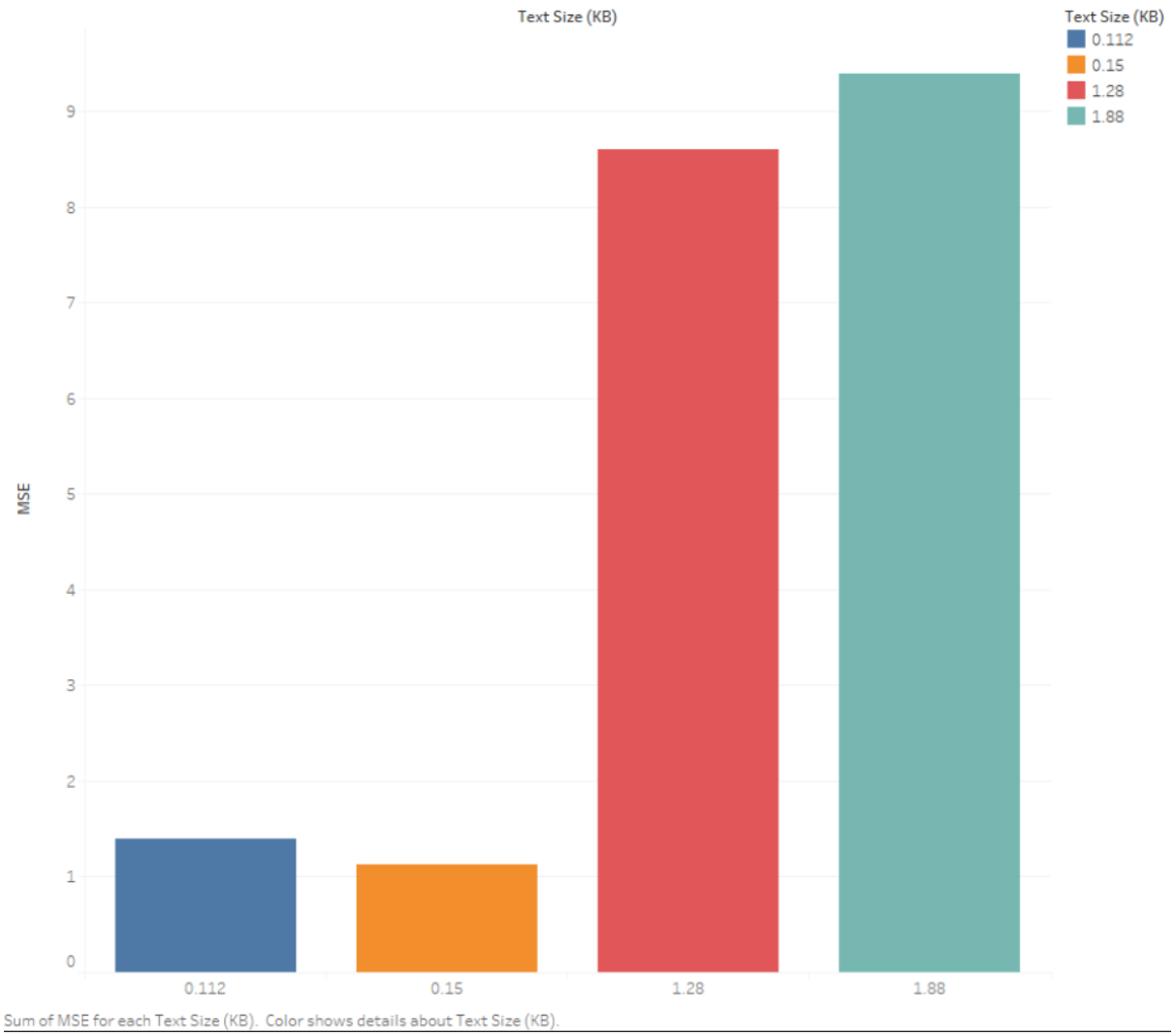

Figure 13: MSE Graph

The system developed provides a good quality of encryption and steganography. The statistical analysis conducted shows high values of PSNR and SNR for different sized text, however, MSE is more in a few cases.

7 Conclusion and Future Work

Simple text exchanged on the internet can be intercepted and confidentiality can be compromised by an intruder. A technique of encrypting simple text by AES algorithm and hiding the ciphertext obtained, by DWT algorithm in a cover audio file has been successfully showcased in this paper. There are many techniques proposed for steganography and for encryption, each technique has its own advantages and disadvantages. Steganography fails the moment the attacker or intruder knows that steganography has been applied, hence it is important to maintain the secrecy of the steganography. To maintain the secrecy of the steganography, there should not be a noticeable difference in the quality of the original audio file and the stego-audio file. The proposed technique provides a high quality of steganography, there are no noticeable changes in the cover file after steganography is applied. By analyzing spectrograms, PSNR, SNR and MSE values it is evident that the proposed system hides the ciphertext in the cover audio file with minimal changes and without altering the quality. In case the attacker/intruder can break the steganography, he/she

will obtain ciphertext as the plain text will be encrypted before steganography is applied. Baseline is simple text is encrypted and hidden in a cover file at the sender's end, it is decoded and decrypted at receiver's end this process is successfully showcased in this paper with a minimal amount of distortion. The proposed system successfully provides confidentiality to the simple text provided.
In the proposed system, only text can be encrypted and hidden in a cover audio file, in the future different file formats can be encrypted and hidden using a similar technique. Different formats of video files can be used as the cover file to hide the encrypted file or data in an efficient manner. Diverse combinations of encryption and steganography algorithms can be tried to provide confidentiality to the input data.

References

An Introduction to Image Compression [WWW Document], n.d. URL https://www.debugmode.com/imagecmp/ (accessed 8.9.19).

Asad, M., Gilani, J., Khalid, A., 2011. An enhanced least significant bit modification technique for audio steganography, in: International Conference on Computer Networks and Information Technology. Presented at the International Conference on Computer Networks and Information Technology, pp. 143–147. https://doi.org/10.1109/ICCNIT.2011.6020921

Bindra, S.D., Bawa, N., 2018. AES Hybridization with Genetic Technique for guarded Image Transmission, in: 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT). Presented at the 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), pp. 262–266. https://doi.org/10.1109/ICICCT.2018.8473022

Compute peak signal-to-noise ratio (PSNR) between images - Simulink - MathWorks United Kingdom [WWW Document], n.d. URL https://uk.mathworks.com/help/vision/ref/psnr.html (accessed 8.9.19).

Geethavani, B., Prasad, E.V., Roopa, R., 2013. A new approach for secure data transfer in audio signals using DWT, in: 2013 15th International Conference on Advanced Computing Technologies (ICACT). Presented at the 2013 15th International Conference on Advanced Computing Technologies (ICACT), pp. 1–6. https://doi.org/10.1109/ICACT.2013.6710492

Gopalan, K., 2003. Audio steganography using bit modification, in: 2003 IEEE International Conference on Acoustics, Speech, and Signal Processing, 2003. Proceedings. (ICASSP '03). Presented at the 2003 IEEE International Conference on Acoustics, Speech, and Signal Processing, 2003. Proceedings. (ICASSP '03)., pp. II–421. https://doi.org/10.1109/ICASSP.2003.1202390

Gupta, N., Sharma, N., 2014. Dwt and Lsb based Audio Steganography, in: 2014 International Conference on Reliability Optimization and Information Technology (ICROIT). Presented at the 2014 International Conference on Reliability Optimization and Information Technology (ICROIT), pp. 428–431. https://doi.org/10.1109/ICROIT.2014.6798368

industry, G.A.A. industry veteran in the consumer electronics, Audio, W.A.H., Systems, H.T., n.d. What Is Signal-to-Noise Ratio and Why Is It Important? [WWW Document]. Lifewire. URL https://www.lifewire.com/signal-to-noise-ratio-3134701 (accessed 8.9.19).

Kanhe, A., Aghila, G., Kiran, C.Y.S., Ramesh, C.H., Jadav, G., Raj, M.G., 2015. Robust Audio steganography based on Advanced Encryption standards in temporal domain, in: 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI). Presented at the 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 1449–1453. https://doi.org/10.1109/ICACCI.2015.7275816

Lau, N., 2017. An AES-Inspired Cryptography Program using MATLAB with character-based matrix manipulation.: nick1au/AES-MATLAB.

Lindawati, Siburian, R., 2017. Steganography implementation on android smartphone using the LSB (least significant bit) to MP3 and WAV audio, in: 2017 3rd International Conference on Wireless and Telematics (ICWT). Presented at the 2017 3rd International Conference on Wireless and Telematics (ICWT), pp. 170–174. https://doi.org/10.1109/ICWT.2017.8284161

Melo, L., 2016. Discrete wavelet transform algorithms written for multivariate analysis and classification of complex materials.: lukemelo/dwt-lv-matlab.

(PDF) A Novel DWT & Correlation Based Audio Steganography | International Journal IJRITCC - Academia.edu [WWW Document], n.d. URL https://www.academia.edu/19897988/A_Novel_DWT_and_Correlation_Based_Audio_Steganography (accessed 8.9.19).

Peak Signal-to-Noise Ratio as an Image Quality Metric - National Instruments [WWW Document], n.d. URL http://www.ni.com/en-ie/innovations/white-papers/11/peak-signal-to-noise-ratio-as-an-image-quality-metric.html (accessed 8.9.19).

Rajput, S.P., Adhiya, K.P., Patnaik, G.K., 2017. An Efficient Audio Steganography Technique to Hide Text in Audio, in: 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA). Presented at the 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA), pp. 1–6. https://doi.org/10.1109/ICCUBEA.2017.8463948

Semwal, P., Sharma, M.K., 2017. Comparative study of different cryptographic algorithms for data security in cloud computing, in: 2017 3rd International Conference on Advances in Computing,Communication Automation (ICACCA) (Fall). Presented at the 2017 3rd International Conference on Advances in Computing,Communication Automation (ICACCA) (Fall), pp. 1–7. https://doi.org/10.1109/ICACCAF.2017.8344738

spectrogram (Signal Processing Toolbox) [WWW Document], n.d. URL http://matlab.izmiran.ru/help/toolbox/signal/spectrogram.html (accessed 8.10.19).

Surse, N.M., Vinayakray-Jani, P., 2017. A comparative study on recent image steganography techniques based on DWT, in: 2017 International Conference on Wireless

Communications, Signal Processing and Networking (WiSPNET). Presented at the 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), pp. 1308–1314. https://doi.org/10.1109/WiSPNET.2017.8299975

What is MATLAB? [WWW Document], n.d. URL https://uk.mathworks.com/discovery/what-is-matlab.html (accessed 8.9.19).