INCREASING ROBUSTNESS THROUGH MULTIPLE LAYERS IN AUDIO STEGANOGRAPHY

Submitted in partial fulfillment of the Degree of Bachelor of Technology

May – 2014

Enrollment No.	– 101058
Name of Student	– Vinay Potaraju
Name of Supervisor	– Mr. Akhil Ranjan

DEPARTMENT OF ELECTRONICS AND COMMUNICATION
ENGINEERING
JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY,
WAKNAGHAT

TABLE OF CONTENTS

SUMMARY

‘Increasing Robustness through Multiple Layers in Audio Steganography’ is a project relating to cryptography that uses multiple cryptographic methods under a project. The multiple cryptographic method ensures the complexity of decryption. This cryptographic method also uses multiple layers for each cryptographic method. The system uses three blocks for encryption namely cipher-text, text steganography and audio steganography. The first two blocks can further be into number of layers. The decryption is also achieved through the same reverse process. Further details of multiple layers will be discussed in the rest of the paper. In this project, we wxplore the potential of steganography in increase of robustness by introducing multiple cryptographic techniques in an encryption of text file so that it becomes difficult to decrypt it. We use two algorithms for the encryption, they are LSB and MSB embedding technique.

Signature of Student	Signature of Supervisor
Name	Name
Date	Date

LIST OF FIGURES

LIST OF TABLES

LIST OF FLOWCHART

CERTIFICATE

I hereby certify that the work which is being presented in the B.Tech. Major Project Report entitled ***"Increasing Robustness Through Multiple Layer Audio Steganography"***, in partial fulfillment of the requirements for the award of the Bachelor of Technology in Electronics & Communication Engineering and submitted to the Department of Electronics & Communication Engineering and submitted to the ***Department of Electronics & Communication Engineering*** of ***Jaypee University of Information Technology*** Waknaghat HP is an authentic record of my own work carried out during a period from July 2013 to May 2014 under the supervision of ***Mr. Akhil Ranjan, Grade II Assistant Professor.***

The matter present in this thesis has not been submitted by me for the award of any other degree elsewhere.

Signature of Candidate
VINAY POTARAJU
101058

This is to certify that the above statement made by the candidate is correct to the best of my knowledge

Date:

Signature of Supervisor
Mr. AKHIL RANJAN
Grade II Assistant Professor

ACKNOWLEDGEMENT

I have taken efforts in this project. However, it would not have been possible without the kind support and help of many individuals and organizations. I would like to extend sincere thanks to all of them.

I am highly indebted to Jaypee University of Information Technology for their guidance and constant supervision as well as for providing necessary information regarding the project and also for their support in completing the project. I would like to express my gratitude towards my project guide Mr. Akhil Ranjan for his constant support in completion of the project.

I would like to express my special gratitude to my parents for their positive encouragement in the completion of the project.

REFERENCES

[1] S. Katzenbeisser, F.A.P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Norwood, MA, 2000.

[2] Sridevi R., Damodaram A., SVL.Narasimham, Efficient Method of Audio Steganography by Modified LSB Algorithm and Strong Encryption Key with Enhanced Security, Journal of Theoretical and Applied Information Technology, 2009.

[3] G. J. Simmons, "The prisoners' problem and the subliminal channel" in Proc. Advances in Cryptology (CRYPTO '83), pp. 51-67.Berglund, J.F. and K.H. Hofmann, 1967. Compact semitopological semigroups and weakly almost periodic functions. Lecture Notes in Mathematics, No. 42, Springer-Verlag, Berlin-New York.

[4] Masoud Nosrati, Ronak Karimi, Mehdi Hariri, An introduction to steganography methods, World Applied Programming, Vol (1), No (3), August 2011. 191-195.

[5] Bender W, Gruhl D & Morimoto N (1996) Techniques for data hiding. IBM Systems Journal 35(3): p 313–336.

[6] Nedeljko Cvej, Algorithms for audio watermarking and steganography, Oulu 2004, ISBN: 9514273842.

[7] Sos S. Agaian, David Akopian, Sunil A. D’Souza1, Two algorithms in digital audio steganography using quantized frequency domain embedding and reversible integer transforms, USA.

[8] “audio steg: methods”, Internet publication on www.snotmonkey.com http://www.snotmonkey.com/work/school/405/methods.html

[9] Samir K Bandyopadhyay, Debnath Bhattacharyya, Debashis Ganguly, Swarnendu Mukherjee and Poulami Das, “A Tutorial Review on Steganography”.

[10] Beixing Deng, Jie Tan, Bo Yang, Xing Li, A Novel Steganography Method Based on Modifying Quantized Spectrum Values of MPEG/Audio Layer III, Proceedings of the 7th WSEAS International Conference on Applied Informatics and Communications, Athens, Greece, August 24-26, 2007.

[11] Alaa Ismat Al-Attili, Osamah Abdulgader Al-Rababah, New technique for hiding data in audio file, IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.7, July 2010.

[12] H.B.Kekre, Archana Athawale, Swarnalata Rao, Uttara Athawale, Information Hiding in Audio Signals, International Journal of Computer Applications (0975 – 8887) Volume 7– No.9, October 2010.

[13] Mazdak Zamani, Azizah A. Manaf, Rabiah B. Ahmad, Akram M. Zeki, and Shahidan Abdullah, A Genetic-Algorithm-Based Approach for Audio Steganography World Academy of Science, Engineering and Technology 54 2009.

[14] Nedeljko Cvejic, Tapio Seppänen, Increasing Robustness of LSB Audio Steganography Using a Novel Embedding Method, Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04).

[15] Ajay.B.Gadicha1, Audio Wave Steganography, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-1, Issue-5, November 2011.

1. OBJECTIVE

The present project titled ‘Increasing Robustness through Multiple Layers in Audio Steganography’ is an attempt to implement more than one cryptographic algorithm to increase the complexity. The project uses the LSB as well as embedding algorithm and substitution cypher text on the MATLAB Version 7.1.0.246 (R14) Service Pack 3.

2. STEGANOGRAPHY

Steganography is an art of concealing a message (usually, text or audio or image file) into another file like text or audio or image. Steganography is derived from the Greek words *‘steganos’* meaning ‘covered or protected’ and *‘graphei’* meaning ‘writing’. The difference between the steganography and cryptography lies in the fact that in Steganography it doesn’t draw the attention that message is concealed. The fact that message is concealed is not known to the public, since the very thing that it is encrypted is concealed, while on the other hand in cryptography it exposes the fact that it is encrypted because cryptography is entirely in the different platform.

Let us take an example of an image steganography, the following two images fig 1 and fig 2 shows the contrast between the original and encrypted image. The first image is the original image and the second image is the encrypted image. As we can see, one can hardly point out the difference between the original and watermarked image.

Figure 1 Original Image

Figure 2 Encrypted Image

Similarly the example can be extended to the audio files too where we are going to embed a text file, which is the core part of the present project. The fig 3 and 4 shows the audio steganography using LSB technique.

3. AUDIO STEGANOGRAPHY

In audio steganography, a secret message in the form of text or image or audio is embedded into the audio file. Here, in this project I am using a .wav file to embed the text file into the audio file. The algorithms used in audio steganography are as follows:

3.1 Least Significant Bit (LSB) coding: In this method of coding, the information to be embedded is converted into binary and also the cover image (in this case audio), is also converted into binary, and the algorithm of LSB is applied. Usually, one bit of the cover image is XORed with each bit of the secret message.

3.2 Parity Coding [8]: Instead of breaking a signal down into individual samples, the parity coding method breaks a signal down into separate regions of samples and encodes each bit from the secret message in a sample region's parity bit. If the parity bit of a selected region does not match the secret bit to be encoded, the process flips the LSB of one of the samples in the region. Advantage: The sender has more of a choice in encoding the secret bit, and the signal can be changed in a more unobtrusive manner. Disadvantage is that this method like LSB coding is not robust in nature.

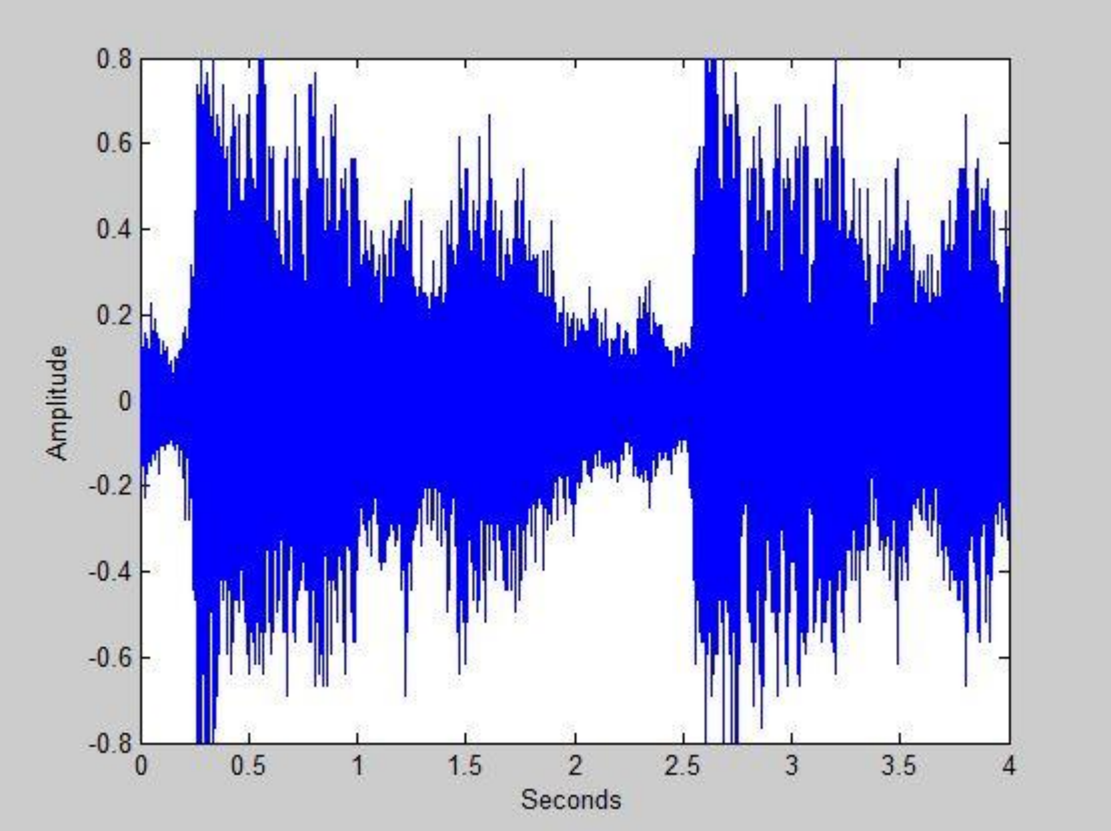


Figure 3 Original Audio

3.3 Phase Coding [9]: Phase coding relies on the fact that the phase components of sound are not as perceptible to the human ear as noise is. It “works by substituting the phase of an initial audio segment with a reference phase that represents the data. The phase of subsequent segments is then adjusted in order to preserve the relative phase between segments”. Disadvantage: It is a complex method and has low data transmission rate.

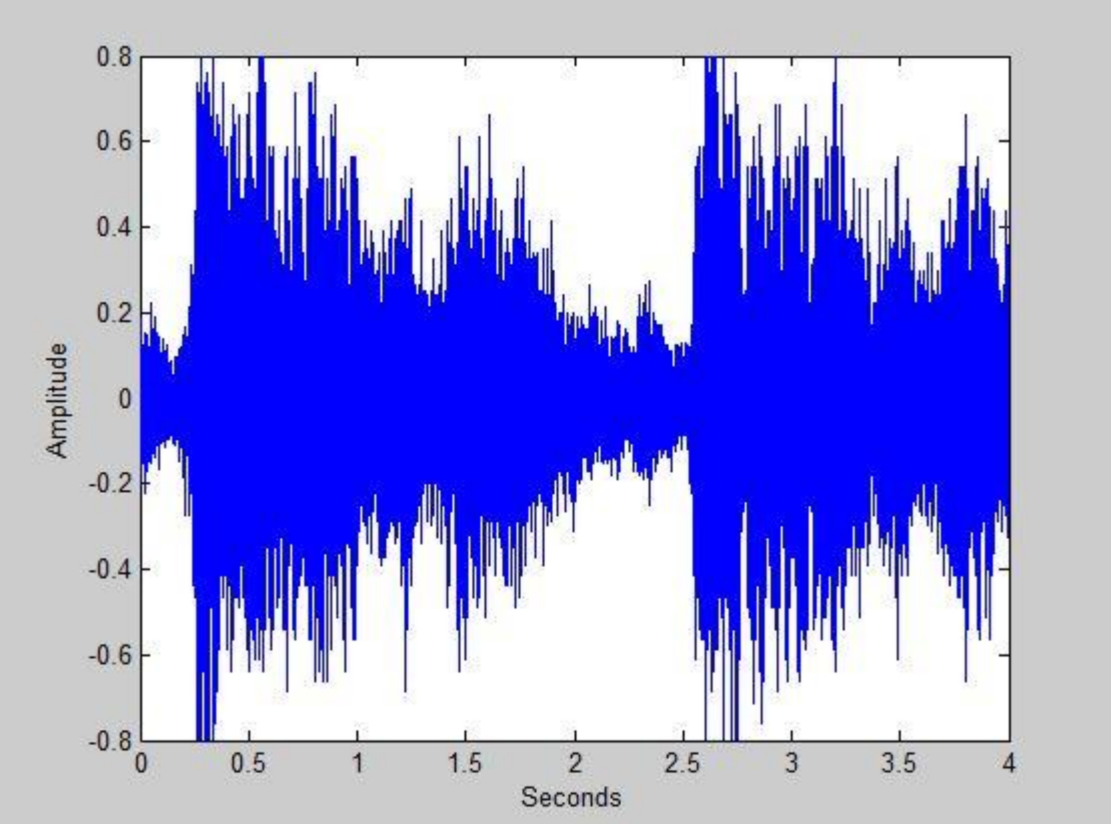


Figure 4 Encryted Audio

4. MULTIPLE LAYERS

The multiple layer is analogy to a locked black box where a secret message is safe. It is similar to placing an important object into a box, which in turn is put into another box and so on, here the different layers on different levels are implemented. The layers that has been used in this project work are as follows:

- Cipher-texting
- Text Steganography
- Audio Steganography

Multiple layers ensures the data to be safe and increases the complexity of the decryption. The advantage of multiple layers over the normal cryptographic method is that, instead of increasing the mathematical complexity of a single cryptographic method, it is better to induce different cryptographic method on a single secret message and repeat it over and over again.

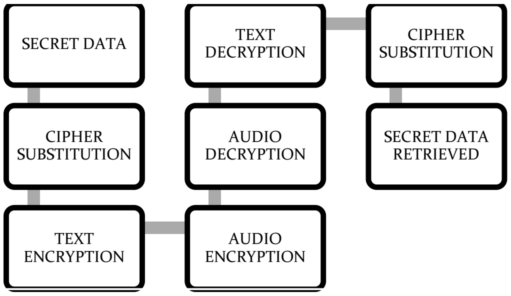


Figure 5 Block Diagram of Multiple Layer Audio Steganography

Figure 5 is the flowchart of the current project, where each block represents specific cryptography technique. The diagram starts with secret data block and then the first block represents cipher substitution. The cipher substitution is the most classical cipher encryption method, where cipher key is used to encrypt the data that is called plain text. After the encryption the text file becomes cipher text which is not readable to the general public. To decipher the cipher text there is a need of cipher key that is shared only by the sender and receiver. The technique of choosing the right cipher key determines the complexity of encryption. Here, in this project I made use of multiple layers, that is similar to multiple black box. For an instance, a very important object is kept inside a black box, and then the black box is again kept in another black box, and again this is kept inside another black box. The main advantage of this method is that the cracker does not have any idea how many black boxes are present. This is the main crux, firstly, it is very difficult procure the cipher key and then to guess the number of layers.

The next block is text encryption block that is text steganography. It is a very unique cryptographic method where message is concealed in such a way that only the ones sharing the message knows about it. In text steganography is achieved using MSB embedding technique. In this we require a text file that is larger than the ciphered text from the first block (roughly 8 times), and using the MSB algorithm we embed the ciphered text into the larger text resulting in the encrypted text. This block too can be used to create multiple layers by encrypting the encrypted text into another text file and so on.

For the fourth block i.e. audio steganography, the resulting encrypted text from block 3 is then embedded in the audio using the LSB technique. The message is securely retrieved by the recipient with his cipher key, audio and text file.

For the decryption part, the fifth block represents the audio retrieving, where a text file is retrieved from the audio file. This text file is text steganographed file, which is retrieved using the LSB technique and the original audio file.

The sixth block i.e. a text file is decrypted using MSB technique and the original text file. After decryption the text file that is retrieved will be the ciphered text file, which needs to be deciphered using the cipher-key.

The text file in the seventh block can only be decrypted by using the cipher-key and a number of layers that was used to encrypt it, without it, it would be impossible to decipher it. There are many methods to decipher a ciphered text file using the character frequency model but the lack of knowledge of number of layers can prove it impossible to decipher it. It is also due to the brief message that is being communicated it is not possible to decipher it.

5. CIPHER ENCRYPTION

Cipher Encryption is a cryptographic method in which a plaintext (the secret message to be delivered) is encrypted using a secret word called cipher, the encrypted plain text is then called cipher-text. There are many types of cipher, the cipher which we are going to use will be the substitution cipher. In substitution cipher each alphabet is replaced by another alphabet, so each letter in the original text file is replaced by another letter according to the table.

Alphabets	Substitution	Alphabets	Substitution
A	T	B	E
C	S	D	L
E	A	F	B
G	C	H	D
I	F	J	G
K	H	L	I
M	J	N	K
O	M	P	N
Q	O	R	P
S	Q	T	R
U	U	V	V
W	W	X	X
Y	Y	Z	Z

Table 1 Substitution Cipher

Suppose we have a message as “*this is an audio steganography project*”, then this will be ciphered as “*rdfq fq tk tulfm qractkmcptndy npmgasr*”. This can further be ciphered by using the same cipher as “*plbo bo rh ruibj optsrhjsnrkly knjctqp*”, which is called the second layer, and so on. The main advantage of using multiple layers is that it will be very difficult to decipher it, as it has to be deciphered multiple times. In this project we can use more 1000 layers for cipher itself. We can see that after ciphering the above message 1000 times the message becomes “*aklc lc ep euhlq cabjepqjterky rtqmbga*”.

6. TEXT STEGANOGRAPHY

Steganography are of many kinds it can be text, video, audio and image, depending upon the kind of the cover we are using. In text steganography the text acts as a cover where the message is embedded. The message can be text or audio or even an image. There are many algorithms for text steganography that can be used. In this project, the main focus is on the MSB embedding of the text file. The algorithm is theoretically explained below.

The prerequisite of the text steganography is that we need a text file for covering and a secret message. The secret text file is embedded into another text file that is the cover file. It is done through a algorithm called MSB embedding. Both the text file is first converted into the ASCII format. ASCII stands for American Standard Code for Information Interchange. It assigns an integer value to the each alphabet, these integers in turn can be converted into 8-bit binary number.

6.1 MSB Embedding Technique

The secret message to be embedded into the text file is shown in the following table:

Text File ASCII	Letter to be Embedded	Resulting ASCII
00001101	0	00001101
00110011	1	10110011
11001010	0	11001010
00011010	1	10011010
10101010	1	00101010
01011101	1	11011101
11100010	0	11100010
01010111	1	11010111

Table 2   XORing the MSB of a text file

The table 2 shows the embedding, and to retrieve the ASCII binary number we make use of the original text file as a key to decrypt the message.

The table 3 shows the decryption mechanism of retrieving ASCII from the embedded text.

Embedded Text	Original Text	ASCII
00001101	00001101	0
10110011	00110011	1
11001010	11001010	0
10011010	00011010	1
00101010	10101010	1
11011101	01011101	1
11100010	11100010	0
11010111	01010111	1

Table 3 XORing the MSB of a text file

7. AUDIO STEGANOGRAPHY

The present project makes use of Audio in order to embed the final text file that has been ciphered and text embedded into the audio file. Here, we use a random .wav file. The algorithm used to embed the text file into the audio file is the LSB embedding. We make use of multiple bit LSB embedding. Multiple bit LSB embedding is much more developed version than the normal LSB embedding since it makes use of 2-LSB bits to embed the text. Here, in this case, we read the audio file in two formats, mainly 8-bits for 1-bit LSB embedding and 16-bits for 2-bits LSB embedding. There is hardly any difference between the original and encrypted audio file.

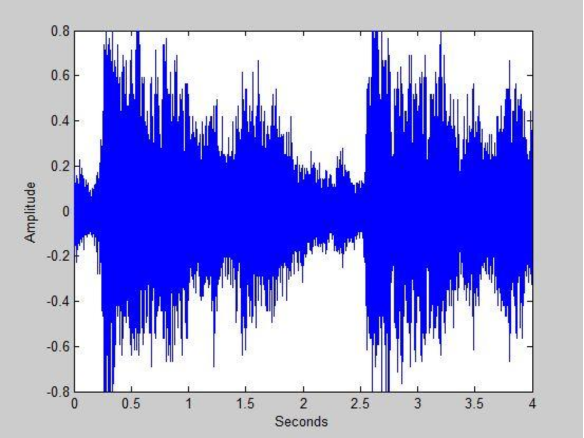


Figure 6 Original Audio

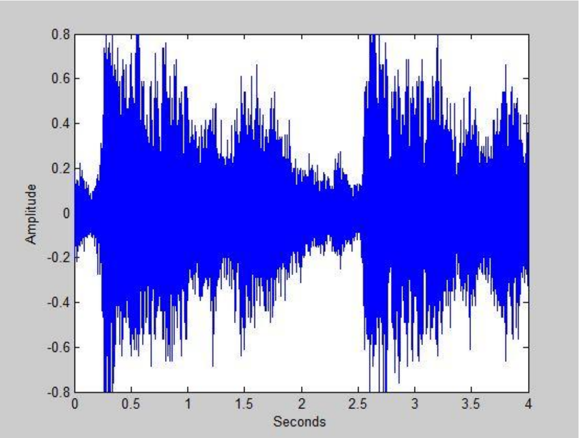


Figure 7 Encrypted Audio

The fig. 6 and fig. 7 shows the amplitude vs time graph of both original and encrypted audio file. It is observed that there is hardly any difference between the two. This is quite expected from the LSB embedding technique, the reason lies in the fact that, since only the LSB part is altered, i.e., 0 to 1 or 1 to 0, and sometimes there is no bit alteration due the fact that we apply XOR function.

7.1 LSB EMBEDDING TECHNIQUE

The following table will depict the LSB embedding technique that is used to encrypt an audio file with a text file.

Text File ASCII	Letter to be Embedded	Resulting ASCII
00001101	0	00001101
00110011	1	00110010
11001010	0	11001010
00011010	1	00011011
10101010	1	10101011
01011101	1	01011100
11100010	0	11100010
01010111	1	01010110

Table 4 XORing the LSB of an audio file

The table 4 shows the embedding, and to retrieve the ASCII binary number we make use of the original audio file as a key to decrypt the message.

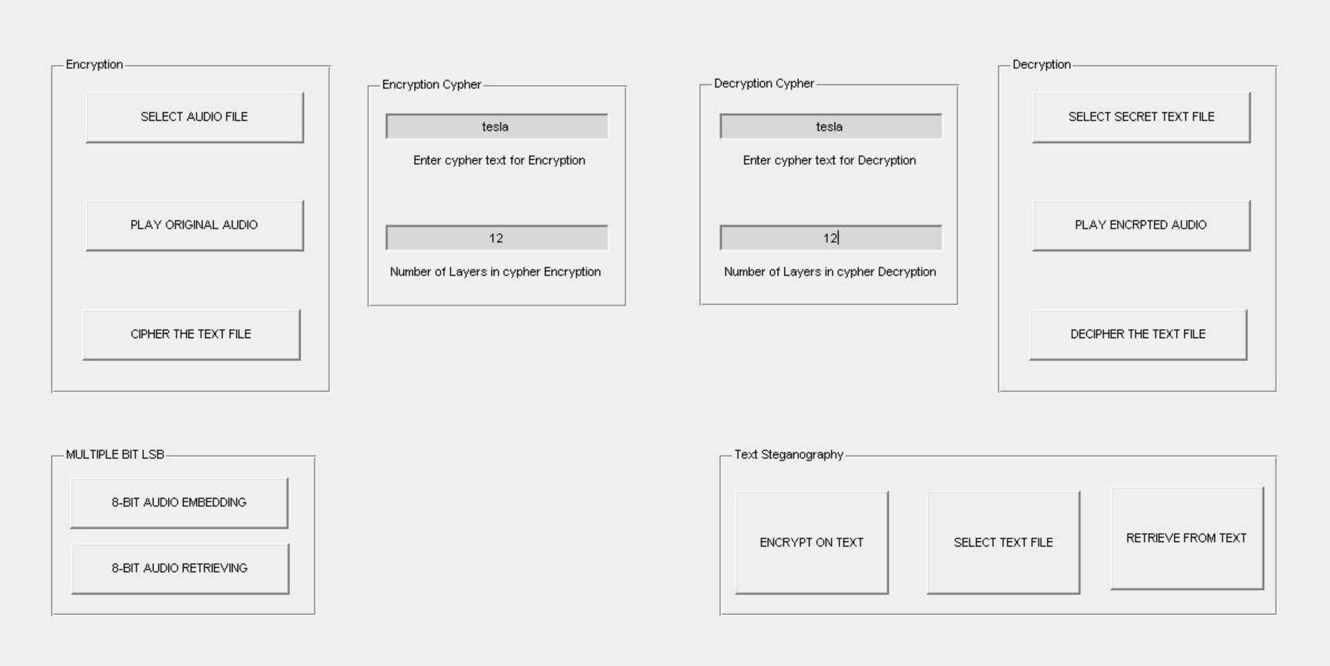
The table 5 shows the decryption mechanism of retrieving ASCII from the embedded text.

Embedded Text	Original Text	ASCII
00001101	00001101	0
00110010	00110011	1
11001010	11001010	0
00011011	00011010	1
10101011	10101010	1
01011100	01011101	1
11100010	11100010	0
01010110	01010111	1

Table 5 XORing the LSB of an audio file

8. GUI IMPLEMENTATION

MATLAB GUI is implemented in this project to make it user-friendly. GUI is implemented by using the GUI simulation found under file icon in the MATLAB taskbar. The GUI implemented is shown the following figure 6



Encryption Cypher

tesla

Enter cypher text for Encryption

12

Number of Layers in cypher Encryption

Decryption Cypher

tesla

Enter cypher text for Decryption

12

Number of Layers in cypher Decryption

Figure 8 GUI Implementation

8.1 OPERATIONS OF GUI WINDOW:

I. SELECT AUDIO FILE:

A .wav audio file is selected as a cover to the secret message. The audio file selected should be no less than 6 seconds.

II. PLAY ORIGINAL AUDIO:

It plays the audio file that we have selected.

III. SELECT SECRET MESSAGE:

A secret message text file is selected from the PC to be encrypted on the audio file.

IV. CIPHER THE TEXT FILE:

The secret message selected is ciphered via cipher key that has to be entered in the text edit box. The cipher-key must be such that no letters in the word is repeated, for example, ‘*yeshua*’, ‘*mother*’ and so on.

V. SELECT TEXT FILE:

A text file is select for text steganography. The text file selected must be roughly 8 times the original text file, since we make use of MSB embedding technique.

VI. ENCRYPT ON TEXT:

The ciphered text is encrypted on the larger text file selected. The algorithm applied is MSB embedding.

VII. 8-BIT AUDIO EMBEDDING:

Finally, the text steganographed text is encrypted in the audio file with the help of LSB embedding technique.

VIII. PLAY ENCRYPTED AUDIO:

This push button plays the audio that has been encrypted with the text.

IX. 8-BIT AUDIO RETRIEVEING:

The first step in the decryption process is the 8-bit audio retrieving. It uses LSB algorithm to retrieve the text file.

X. RETRIEVE FROM TEXT:

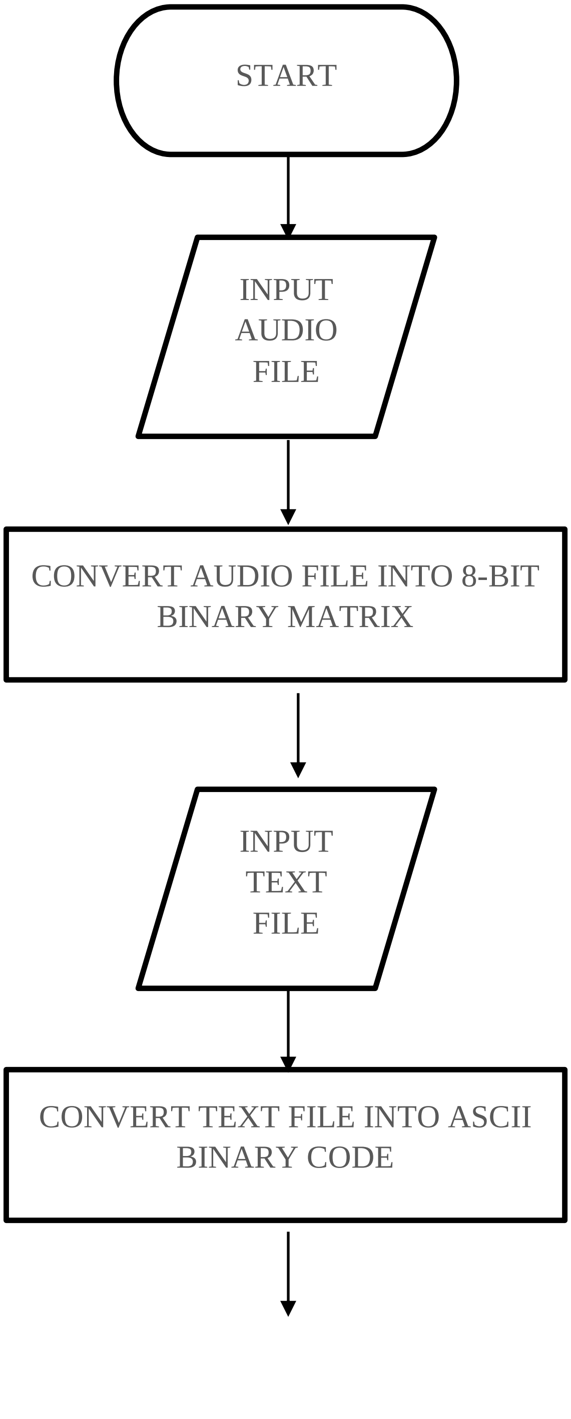
This push button will help to retrieve the ciphered text from the text file. It does it with the help of original text file present.

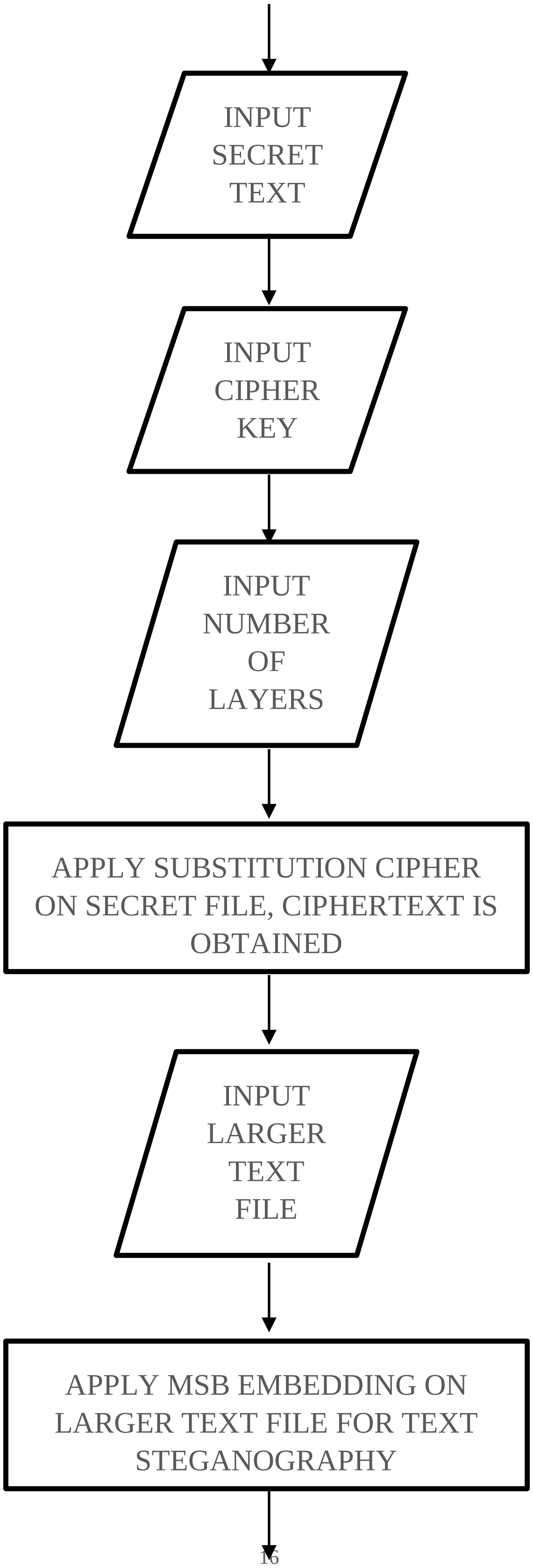
XI. DECIPHER THE TEXT FILE:

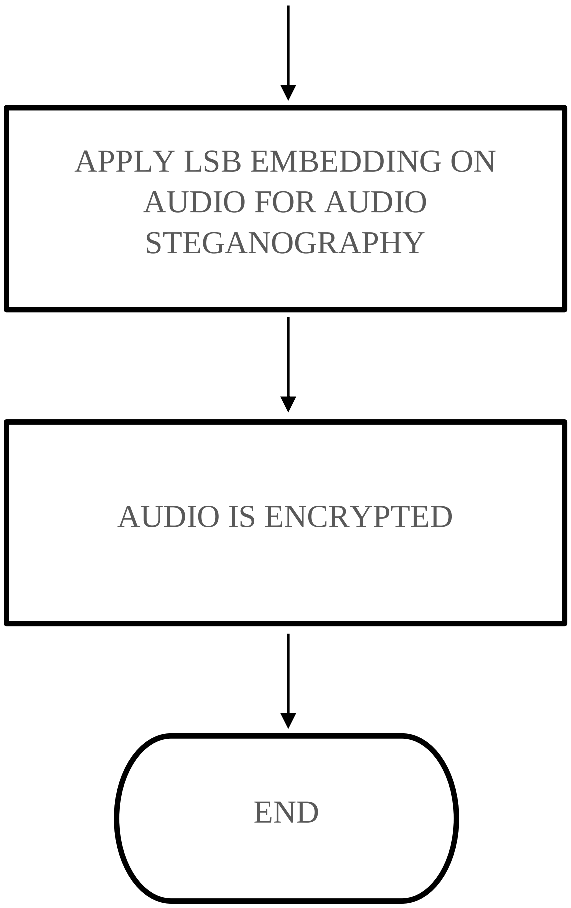
The cipher key entered in the edit text box and the number of layers entered in the edit text box will help to decipher the encrypted text.

9. FLOWCHART

9.1 ENCRYPTION

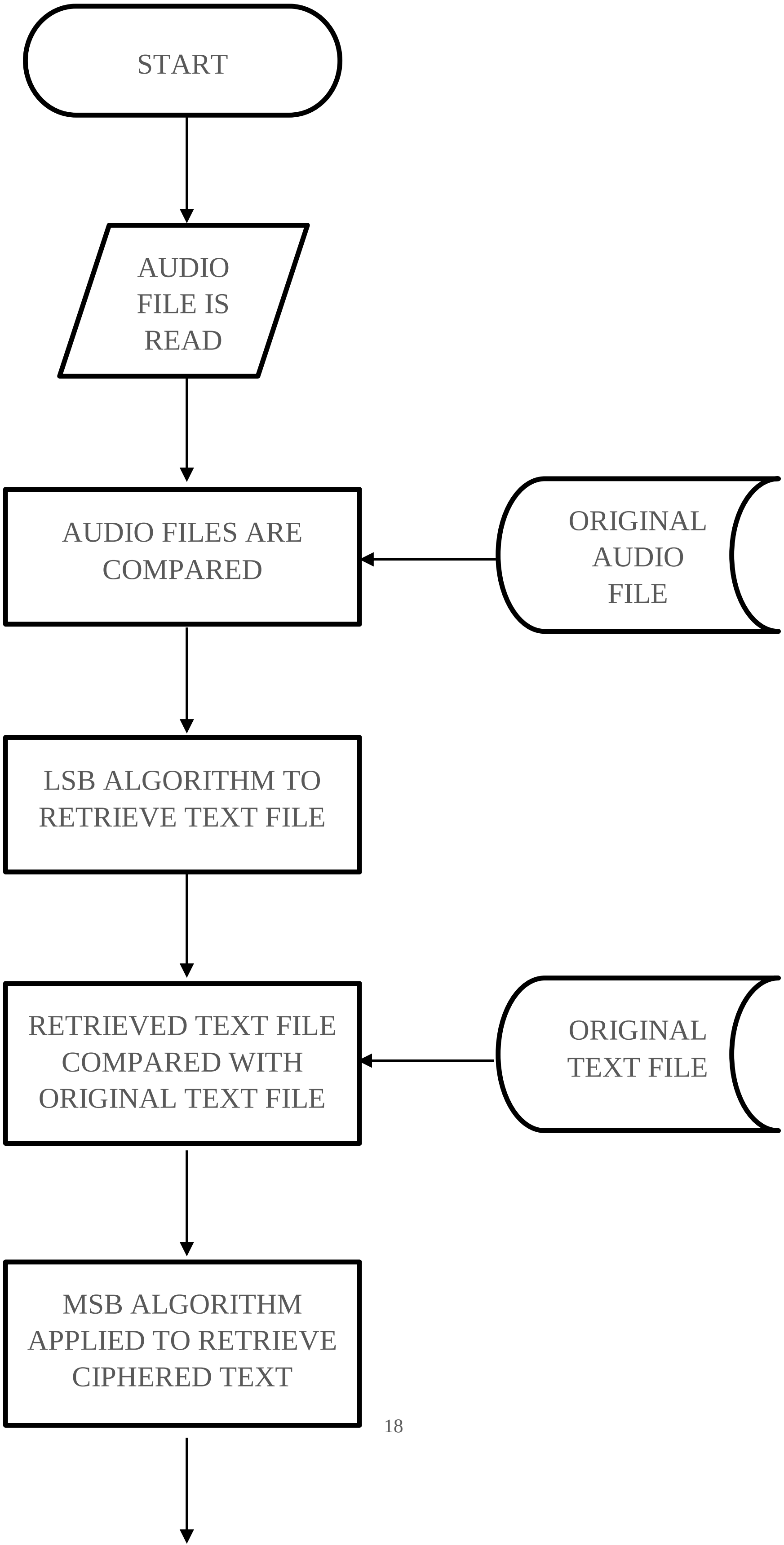

START
INPUT AUDIO FILE
CONVERT AUDIO FILE INTO 8-BIT BINARY MATRIX
INPUT TEXT FILE
CONVERT TEXT FILE INTO ASCII BINARY CODE

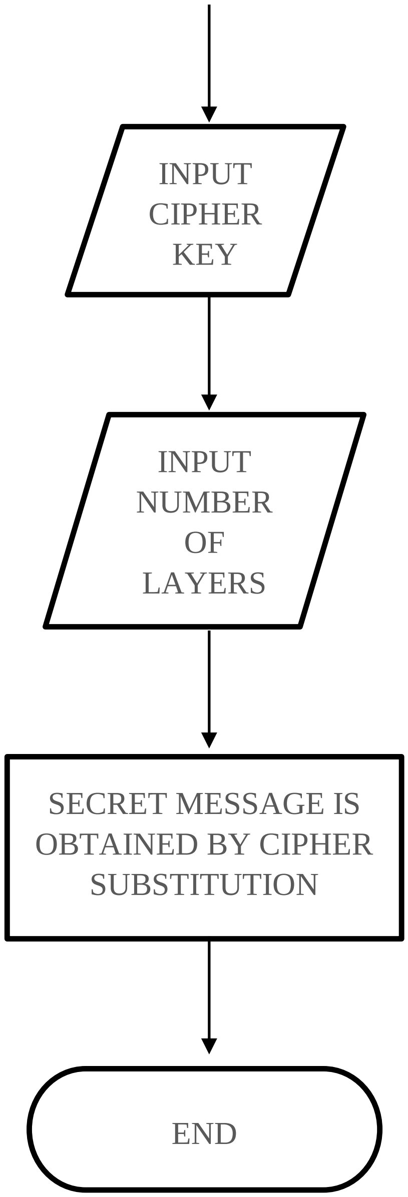

INPUT SECRET TEXT
INPUT CIPHER KEY
INPUT NUMBER OF LAYERS
APPLY SUBSTITUTION CIPHER ON SECRET FILE, CIPHERTEXT IS OBTAINED
INPUT LARGER TEXT FILE
APPLY MSB EMBEDDING ON LARGER TEXT FILE FOR TEXT STEGANOGRAPHY



Flowchart 5Multiple Layer Encryption

9.2 DECRYPTION


START
AUDIO FILE IS READ
AUDIO FILES ARE COMPARED
ORIGINAL AUDIO FILE
LSB ALGORITHM TO RETRIEVE TEXT FILE
RETRIEVED TEXT FILE COMPARED WITH ORIGINAL TEXT FILE
ORIGINAL TEXT FILE
MSB ALGORITHM APPLIED TO RETRIEVE CIPHERED TEXT



Flowchart 6 Multiple Layer Decryption

10. ALGORITHM

The steps involved in the implementation of '*Multiple Layer Audio Steganography*' on MATLAB are as follows:

10.1 ENCRYPTION

Step 1 The audio file is read in the MATLAB using wavread function.

Step 2 The values returned by the wavread function is between -1 to +1.

Step 3 The matrix is then multiplied by 255, since it has to be converted into 8-bit binary number.

Step 4 The absolute of the matrix is taken, in order to have all the positive values.

Step 5 The matrix is converted into 8-bit binary by using a function de2bi.

Step 6 The matrix is stored in yfewb

Step 7 Now, the text file is read by using a function text read.

Step 8 We define a user-defined function text2ascii and ascii2text on order to convert text into ASCII and ASCII to text.

Step 9 We apply substitution cipher on the text file.

Step 10 We replace each letter with a corresponding cipher letter in the text file and save it as cipheredtext.txt.

Step 11 We read another long text file for the cipheredtext.txt to be embedded into it using Text steganography.

Step 12 The ciphered text is embedded using MSB embedding in order to differentiate it from ciphered text.

Step 13 The final text file is then saved as texthide.txt.

Step 14 Now, the texthide.txt is ready to be embedded into the audio file by using LSB embedding.

Step 15 The resulting texthide.txt is converted into ASCII code using the text2ascii function.

Step 16 Each binary digit of the text file is XORed with the 8th or LSB of each element of the audio file.

Step 17 Hence, a new set of numbers is then available and it is then compared with the original audio file.

Step 18 The negative 1 is multiplied to this resulting matrix where there is a negative value in the original audio file.

Step 19 The matrix is then divided by 255.

Step 20 A function wavwrite is then used to save the encrypted audio file.

10.2 DECRYPTION

Step 21 The encrypted audio file is read using wavread function and the resulting matrix is multiplied by 255.

Step 22 The matrix is then converted to all the positive values by applying a MATLAB inbuilt function abs.

Step 23 The keys here in this case are the original audio file and the text file that should be present with the receiver in order to decode the message, but the presence of both the original files does not ensure the safe recovery of the message, since there is another cipher key needed and the value of the layers to be decoded to be known.

Step 24 The audio matrix is compared with the original audio matrix and 8th bit is XORed or 15th and 16th bit is XORed in order to retrieve the text embedded file.

Step 25 The text embedded file is then decoded by using the MSB algorithm.

Step 26 The decoded text is then deciphered by using the cipher key word and the number of layers to be decoded.

Step 27 The secret message is then decrypted.

11. RESULTS

We take text file named ‘Secret Message.txt’, with the data as ‘*the final audio steganography project*’. This message will then be ciphered with a cipher key. The ciphered text will again be ciphered as many times as we need the number of layers. Then the ciphered text file will be encrypted in a text file (cover text), which is called the text steganography. Later, the text encrypted file will be encrypted into the audio file which is called audio steganography.

For the decryption the process just reverses and we will be needing the cipher key, value of number of layers used, original text file (cover text) and the original audio file.

After encrypting ‘*the final audio steganography project*’ with the cipher key as ‘*inure*’ and number of layers as 124. We get the ciphered text file as ‘*lse rmnpt pojmu hlegpnugfpasy afudeql*’. The cover text which we will be taking in this case will be ‘*many years ago i napoleon hill had an abiding interest in higher education and post secondary education in general, throughput his adult life, and he was associated with a variety of teaching institutions. His constant theme was that educatiton should not simply focus on "imparting knowledge," but on texhing students how to organize knowledge and apply it to accomplish specific objectives.*’

After the text steganography the above cover text file becomes ‘maîù ùåaòó açï i nápoìåon hilì haä aî ábédéîg éntåòåsô in hiçèår eäuãáôion anä post óåãoîäáòy åduãaôiiî én çeîårál¬ ôèòoughpuô his ádõìt léæe¬ aîd he ÷aó ássïãiated ÷éth á váòiåtù ïæ tåáãhiîç iîótiôõtions® Èió conóôaîô tèåíe waó ôèat eduãatéton óèouìä nïô óiípìù focõs iî ¢iípaòôiîg kîï÷ledçå,¢ b’. This file will be encrypted in the audio file.

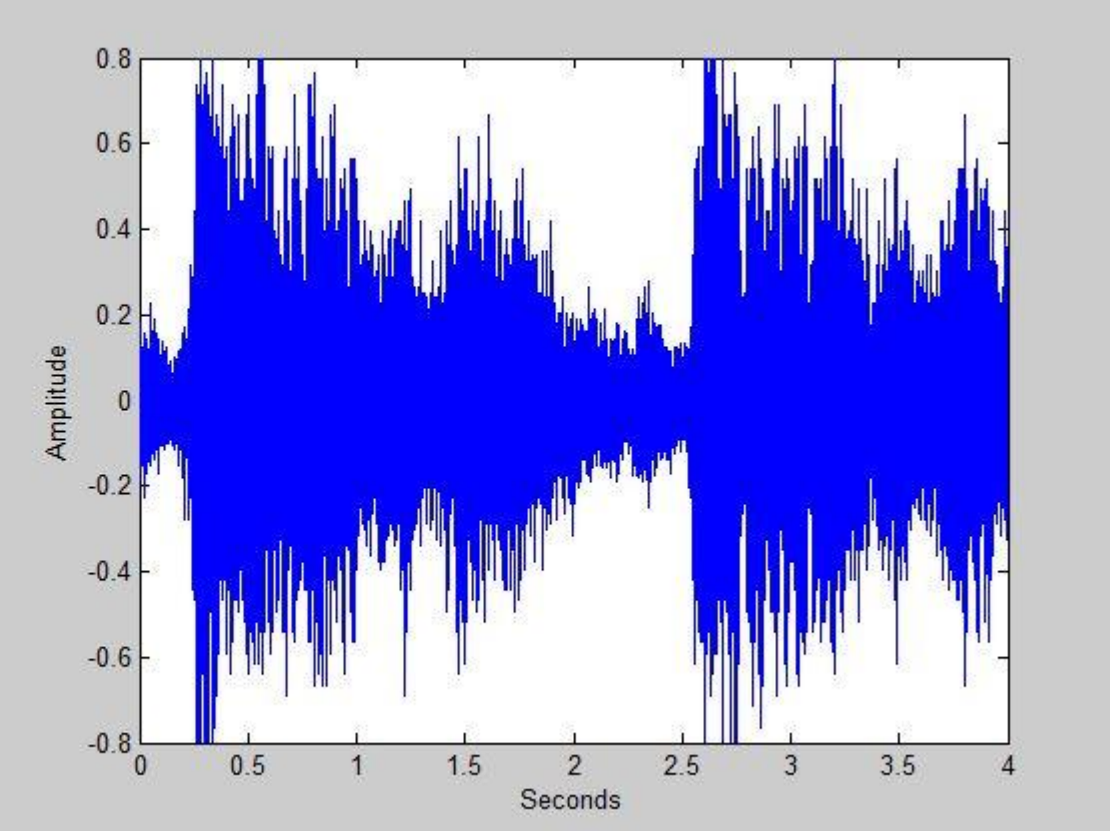


Figure 9 Original Audio File

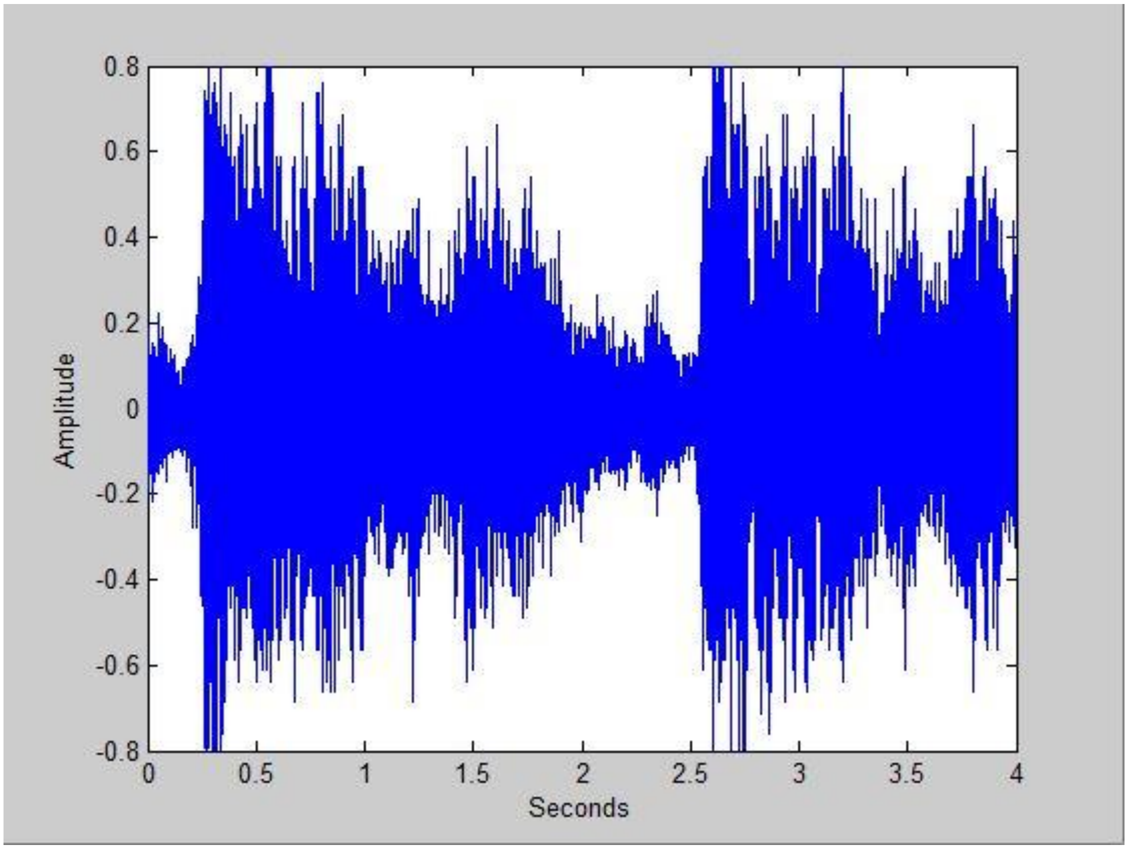


Figure 10 Encrypted Audio File

The fig. 9 shows the amplitude vs time graph of the original audio .wav file used. The text steganographed file is then embedded into the above audio file and the resulting graph obtained is shown in the fig.10. As we can notice there is hardly any difference between the fig.9 and fig.10, therefore the text file has been successfully implemented without much change in the audio file.