IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 6, June 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 6, June 2021||

DOI:10.15680/IJIRSET.2021.1006042

Data Hiding Using Audio Steganography

R.Naveenkumar, C.G.Nikhil Kumar, N.Niranjan, S.M.Janani

U.G. Student, Department of Electronics and Communication Engineering, Meenakshi Sundararajan Engineering College, Chennai, Tamil Nadu, India

U.G. Student, Department of Electronics and Communication Engineering, Meenakshi Sundararajan Engineering College, Chennai, Tamil Nadu, India

U.G. Student, Department of Electronics and Communication Engineering, Meenakshi Sundararajan Engineering College, Chennai, Tamil Nadu, India

Assistant Professor, Department of Electronics and Communication Engineering, Meenakshi Sundararajan Engineering College, Chennai, Tamil Nadu, India

ABSTRACT: Steganography, which means hiding something into something. This can be used by armed forces in sharing secret messages from one place to another without knowing by others that a secret message is embedded into the cover media. Here the cover media will be an audio file. The cover audio will be the same as before, even after encoding the secret message into the audio. And moreover before embedding the message into the audio it will be encrypted using Advanced Encryption Standard technique. And a key will be given to decode the message. This project is going to be implemented in MATLAB R2021a.

KEYWORDS:Data Hiding, Discrete Wavelet Transform, Advanced Encryption Standard

I. INTRODUCTION

The main idea of this project is to hide a secret text in audio file, for which the audio file must be in .wav format. The main concept of this project is steganography, which means hiding something into something. This can be used by armed forces in sharing secret messages from one place to another without knowing by others that a secret message is embedded into the audio file. The cover audio will be the same as before, even after encoding the secret message into the audio. And moreover before embedding the message into the audio it will be encrypted using Advanced Encryption Standard technique. And a key will be given to decode the message. Only those persons with the secret key and the decoding algorithm can obtain the secret message from the cover audio file. We are using AES technique for encryption which makes the decrypting process much more difficult.Steganography is the practice of concealing a message within another message or an object. In computing/electronic contexts, message, image, or video is concealed within another file, message, image, or video

II. RELATED WORK

The Earlier method of hiding a text message in audio file was performed by K.P.Adhiya Swati A. PatilCSE Dept. SSBT's COET Bambhori,Jalgaon,Bambhori,India in the year 2012. The mentioned method used LSB (i.e) Least Significant Bit algorithm in order to embed the secret message into the audio file.In the method each audio sample is converted into bits and then the textual information is embedded in it. In embeddingprocess , first the message character is converted into its equivalent binary. The last 4 bits of this binary is taken into consideration and applying redundancy of the binary code the prefix either 0 or 1 is used. To identify the uppercase, lower case, space ,and number the control symbols in the form of binary is used. By using proposed LSB based algorithm, the capacity of stego system to hide the text increases. The performance evaluation is doneon the basis of MOS by taking 20 samples and comparison of SNR values with some known and proposed algorithm.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 6, June 2021||

DOI:10.15680/IJIRSET.2021.1006042

III. METHODOLOGY

The total process is split into two phases

(i) Embedding Phase
(ii) Extraction Phase.

In the embedding phase the secret message which is to be embedded into the audio file will be encrypted using Advanced Encryption Standard(AES) technique. Then the user will be asked to provide a key, so that the receiver can use the key to obtain the secret message from the audio file. The cipher text is then embedded into audio file using Discrete Wavelet Transform method. During this transform the samples of audio file is converted into sets which consists of two coefficients. They are Detailed coefficient and Approximate coefficient. The detailed coefficients are replaced with the binary format of the cipher text. Then Inverse DWT is done for the audio samples inorder to obtain the stego audio, which is the audio which has the secret message in it.

In the Extraction phase the stego audio will be taken and processed using DWT. After processing we will be left with sets of coefficients. As the know that the values in the detailed coefficient's place are the binary format of the cipher text. Once we get the binary format of the cipher text, it will be converted into normal cipher text. After which the cipher text will be processed using Inverse AES, so that we can obtain the original secret message. Before all these processes the receiver will have to provide the secret key which was given by the user in the transmitter side.

We also can measure the parameters of the audio file like

- Capacity
- SNR (Signal to Noise Ratio)
- PSNR (Peak Signal to Noise Ratio)
- MSE (Mean Squared Error)

IV. EXPERIMENTAL RESULTS

Figure shows the results of matlab simulations of the project.

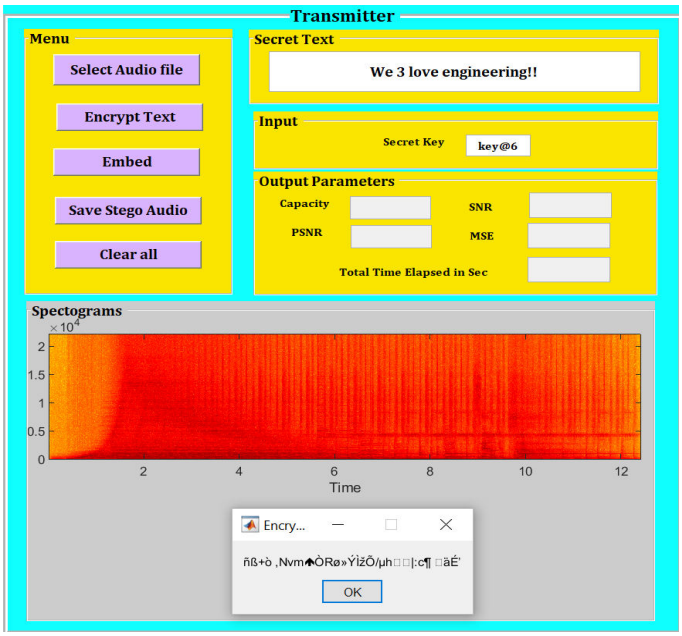

Fig 1. Encrypting the text and providing the secret key (Transmitter Side)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 6, June 2021||

DOI:10.15680/IJIRSET.2021.1006042

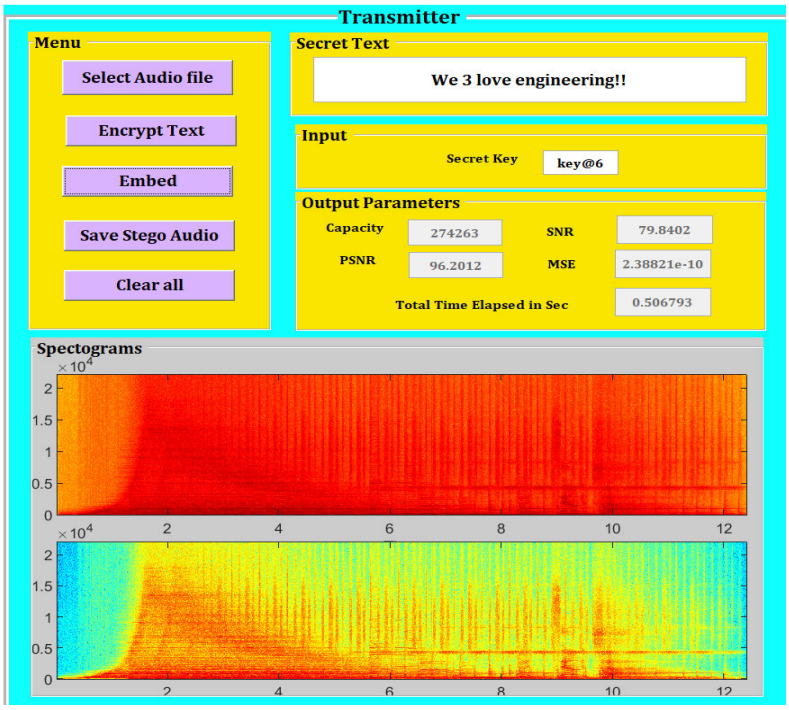

Fig 2. Embedding the cipher text and obtaining the paramters (transmitter)

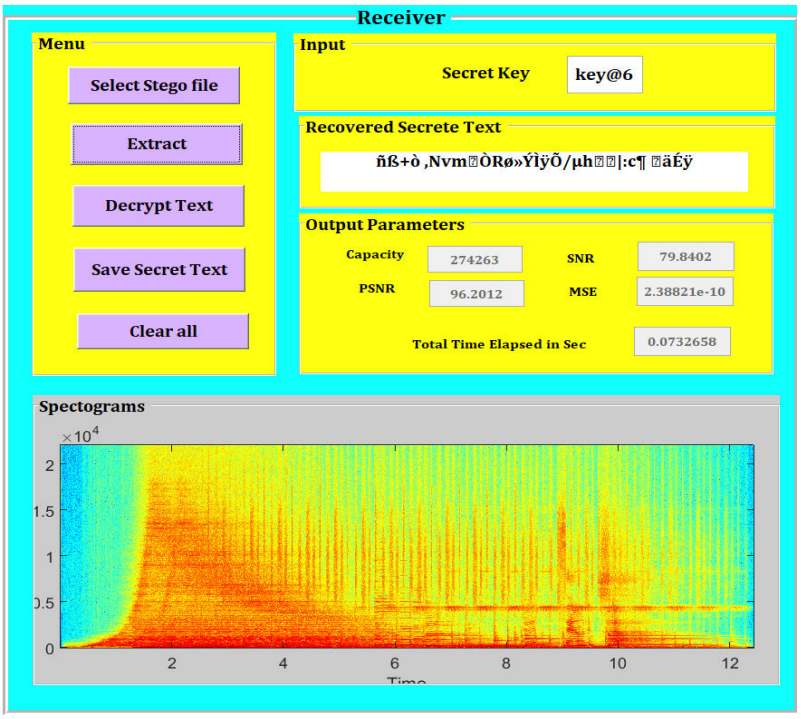

Fig 3. Obtaining the cipher text from the audio and parameters (Receiver)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 6, June 2021||

DOI:10.15680/IJIRSET.2021.1006042

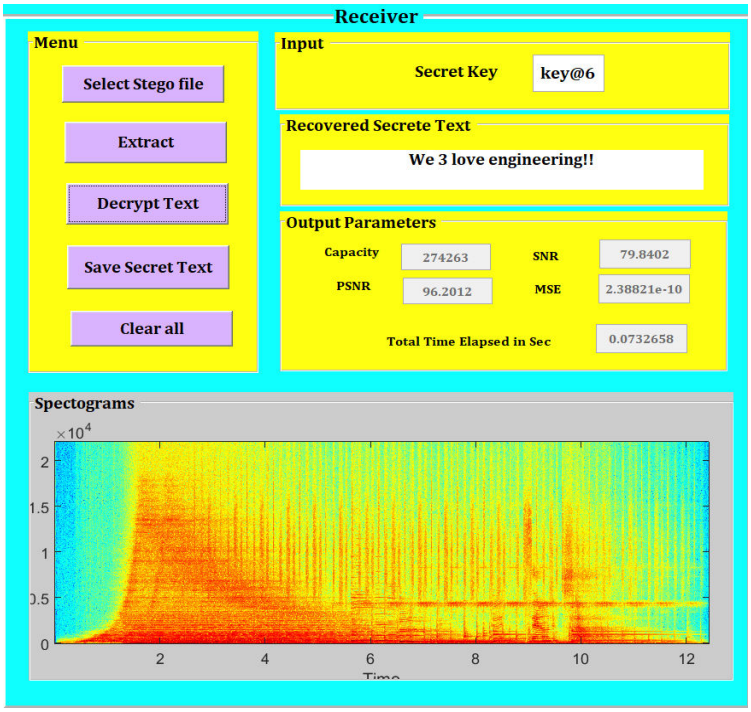

Fig 4. Obtaining original secret text

V. CONCLUSION

The main objective of this project is to provide security in transmitting secret messages. Hence it is achieved using steganography technique. The results obtained from using audio steganography and DWT technique are computed and observed to be good. This algorithm yields zero error extraction, good SNR and capacity. AES technique is the algorithm used for security purposes in many places. Thus also providing security to the message embedded in the audio.

REFERENCES

1. Doshi, R., Jain, P., and Gupta, L., 2012, "Steganography and its Applications in Security", International Journal of Modern Engineering Research (IJMER), 2(6), pp 4634-4638.

2. Djebbar, F., et al, 2012, "Comparative study of digital audio steganography techniques", EURASIP Journal on Audio, Speech, and Music Processing, Springer Open journal, pp 1-16.

3. Weeks, M., "Digital Signal Processing Using MATLAB and Wavelets", Pearson publications, ISBN – 81-297-0272-X.

4. Verma, S. S., Gupta, R., and Shrivastava, G., 2014, "A Novel Technique for Data Hiding in Audio Carrier by Using Sample Comparison in DWT Domain", IEEE conference, pp 639-643.

5. Geethavani, B., 2013, "A New Approach for Secure Data Transfer in Audio Signals Using DWT", IEEE conference.

6. Antony, J., and Sobin, C., 2012, "Audio Steganography in Wavelet Domain – A Survey", International Journal of Computer Applications, 52(13), pp 33-37.

7. ShanYu, T., et al, 2014, "Audio steganography with AES for real-time covert voice over internet protocol communications", Science China Information sciences, 57, pp 1-14.

8. Rekik, S., et al, 2012, "Speech steganography using wavelet and Fourier transforms", EURASIP Journal on Audio, Speech, and Music Processing, Springer Open journal, pp 1-14.

9. Begum, M. B., and Venkataramani, Y., 2011, "LSB Based Audio Steganography Based on Text Compression", International Conference on Communication Technology and System Design, pp 703-710

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 6, June 2021||

DOI:10.15680/IJIRSET.2021.1006042

10. Ballesteros, L. D. M., and Moreno, A. J. M., 2013, "Real-time, speech-in-speech hiding scheme based on least significant bit substitution and adaptive key", Computers and Electrical Engineering 39, pp 1192–1203.
11. Huang, Y., Liu, C. and ShanYu, T., 2012, "Steganography Integration into a Low-Bit Rate Speech Codec", IEEE transactions on information forensics and security, 7(6), pp 1865-1875.
12. Garcia-Hernandez, J. J., et al, 2013, "High payload data-hiding in audio signals based on a modified OFDM approach", Expert Systems with Applications, 40, pp 3055–3064.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details