ISSN (Online): 2456-5717

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Issue.4, April 2017

Audio Steganography: An Approach towards Secure Information Transmission System

S.Jayaprakash[1], P.Mohanavalli[2], R.Priyadharshini[3], R.Swathi[4], S.Deivanai[5], A.Roselinmary[6].
HOD/CSE[1], AP/CSE[2], UG Scholar/CSE [3,4,5,6]
Idhaya Engineering College for Women, Chinnasalem, TN, India.

Abstract - **This paper proposes a novel reversible audio data hiding scheme over encrypted domain. Data embedding is achieved through a public key modulation mechanism, in which access to the secret encryption key is not needed. At the decoder side, a powerful decoder is designed to distinguish encrypted and non-encrypted audio patches, allowing us to jointly decode the embedded message and the original audio signal. Compared with the state-of-the-art methods, the proposed approach provides higher embedding capacity and is able to *perfectly* reconstruct the original audio as well as the embedded message. Extensive experimental results are provided to validate the superior performance of our scheme.**

I. INTRODUCTION

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. Steganography works by replacing bits of useless or unused data in regular computer Files (such as graphics, sound, text, HTML, or even floppy disks) with bits of different, invisible information. This hidden information can be plain text, cipher text, or even images.

In a computer-based audio Steganography system, secret messages are embedded in digital sound. The secret message is embedded by slightly altering the binary sequence of a sound file. Existing audio Steganography software can embed messages in WAV, AU, and even MP3 sound files. Embedding secret messages in digital sound is usually a more difficult process than embedding messages in other media, such as digital images. These methods range from rather simple algorithms that insert information in the form of signal noise to more powerful methods that exploit sophisticated signal processing techniques to hide information.

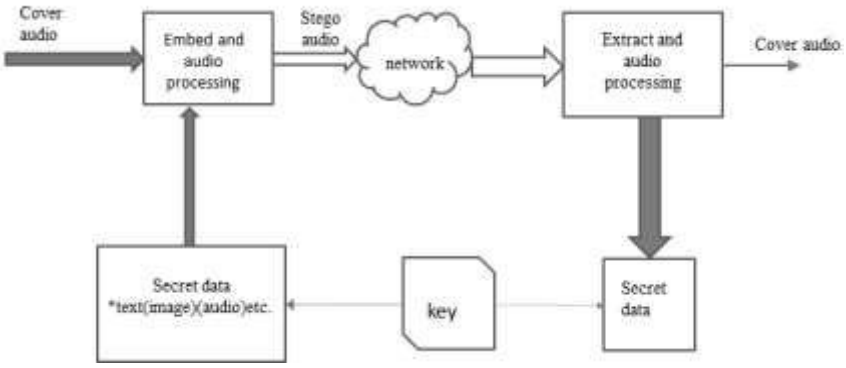
Thus the main purpose of this seminar is to explain Audio Steganography and algorithms commonly employed for Audio Steganography and its applications.

II. AUDIO STEGANOGRAPHY

Audio is sound within the acoustic range available to humans. An audio frequency (AF) is an electrical alternating current within the 20 to 20,000 hertz (cycles per second) range that can be used to produce acoustic sound. Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing” defining it as “covered writing”. In image steganography the information is hidden exclusively in images. Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a

message secret. Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised.

III. ARCHITECTURE



IV. MODULES

a. Audio File Selection and Graphical User Interface.
b. Least Significant Bit.
c. Text Encoding
d. Text Decoding

a) *Audio File Selection and Graphical User Interface*

GUI Creating Using MATLAB, Audio File Selection, Select Message Creation, Conversation to Bits (audio And Text)

b) Least Significant Bit

We have to use the range of audio signals which lies between -1 to and1.As per the range it will be converted into values. Apply formula A>$3WH/8$

c) Text Encoding

Encode the text code like"1010110" in code of audio as text code is much smaller than audio. It uses the least significant bit to hide text messages.

d) Text Decoding

Reverse the process and convert the audio with hidden text to codes. Then MATLAB automatically detects the location where text was hidden then it decodes and gets the message as original.

ISSN (Online): 2456-5717

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Issue.4, April 2017

V. EMBEDDING PHASE

Step 1: Audio Processing Read the cover audio file. Audio samples are stored in a vector and are signed floating point values.

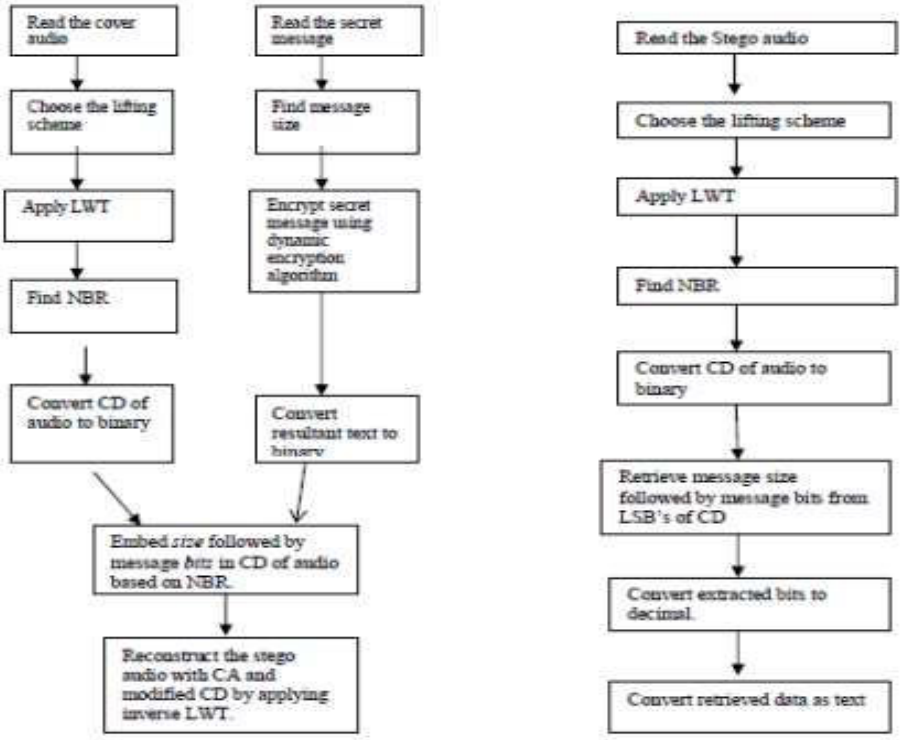
Step 2: Apply LWT based on lifting scheme, this algorithm uses integer to integer transformation which is implemented using lifting wavelet transformation (LWT). LWT uses Lifting Scheme (LS).

Step 3: Calculate number of bits to be replaced.

Step 4: Read text file and encrypt it. Read the text file. Find the size of the text to be hidden. The text is encrypted by subtracting ASCII value of each character by message size. Cipher text is then converted to binary string.

Step 5: Embed the encrypted text this step is sub divided into two parts: Hiding the size of the text and hiding the actual text.

Step 6: Reconstruction of stego-audio signal. Stego-audio signal is reconstructed by applying inverse LWT. This stego-audio sounds same as the cover audio.



VI. EXTRACTION PHASE

Step 1: Audio Processing Read the stego audio file. Then convert the audio samples into integers. This step is same as step 1 in the embedding phase.

Step 2: Apply LWT based on lifting scheme.Select the same lifting scheme which is used in the embedding phase.

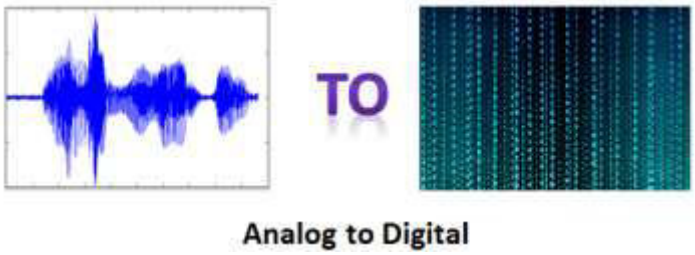
Step 3: Calculate number of bits to be replaced.

Step 4: Extract the hidden message.

Step 5: Decryption of message and writing it into a file After retrieving, the encrypted secret message bits are converted to decimal.

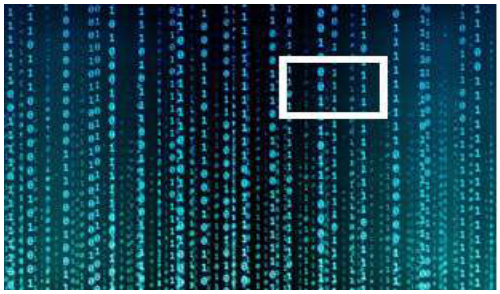
VII. IMPLEMENTATION PLAN

Host Audio Selection and its conversion to matrix digital numbers



Secret Message Selection and its conversion to matrix digital numbers.

LSB Selection and Implementation



Conversion to Audio (with secret message)

VIII. CONCLUSION

Thus we create a stenographic system of message hiding in audio files .It is checked for used in any type real time system. It can be implemented in several fields to maintain data integrity for example in the field of Engineering, Army, Banking, Finance, Treaty, Personal and privacy. The system is specially designed for real time usage. It is 100% secure and flexible. As our future enhancement we will add different techniques of encryption including image, audio and video all together to accept any type of input. If the system is implemented practically it can bring great ease to protect data integrity against corruption and data stealing.

ACKNOWLEDGMENT

The authors are thankful to the reviewers for their valuable comments and suggestions for improving this paper.

REFERENCES

[1] C. Yeh, C. Kuo, (October 1999) Digital Watermarking Through Quasi M- Arrays, Proc. IEEE Workshop On Signal Processing Systems, Taipei, Taiwan, Pp. 456-461.
[2] Dr. D Mukhopadhyay, A Mukherjee, S Ghosh, S Biswas, P Chakarborty (2005.) An Approach for Message Hiding using Substitution Techniques and Audio Hiding in Steganography, IEEE
[3] E. Zwicker, "Psychoacoustics", Springer Verlag, Berlin, 1982.
[4] Mazen Abu Zaher Modified Least Significant Bit (MLSB) Published by Canadian Center of Science and Education Vol. 4, No. 1; January 2011
[5] Nedeljko Cvejic, Tapio Seppben (,IEEE 2002) Increasing The Capacity Of LSB-Based Audio Steganography

[6] Steganographic Techniques and their use in an Open-Systems Environment- Bret Dunbar, The information Security reading Room, SANS Institute 2002 http://www.sans.org/reading room/whitepapers/covert/677.php

[7] Mansour Sheikhan et al, High Quality Audio steganography by Floating Substitution of LSBs in Wavelet Domain, world applied science Journal IDOSI publications, 2010

[8] Y.V.N.Tulasi et al.,Steganography -Security through Images On Embedding of Text in Audio – A case of Steganography Pramatha Nath Basu, 2010 International Conference on Recent Trends in Information, Telecommunication and Computing