Encryption and Decryption of Data Hiding in Audio Signal using LSB algorithm

Kalaiarasi.G [#1]

Assistant professor, Department of Electronics Communication Engineering

Dr.S.Maheswari[#2]

Assistant professor, Department of Electrical &Electronics Engineering

(Sr.Gr)

Snekha.V[#3],Nirmala. T[#3],Suguna. A[#3], Manimegalai. P[#3]

UG Scholars, Department of Electronics and Communication Engineering

JAY SHRIRAM GROUP OF INSTITUTIONS

TIRUPPUR-638660

Abstract-In this recent scenario everyone use multimedia for the conveyance of data. The data we transmit in those social Media should be confidential and highly secure. As the number of users increases the number of intruders also increases. The cryptography and steganography is used to ensure the security of data. Especially they are used in military and defense application to ensure the security. The data is hidden in the image in the existing system, but the data is not unconfined. In the proposed system the data is encrypted using key based algorithm using Linear Feedback Shift Register(LFSR)and the encrypted data is covered in the audio signal using Least Significant Bit (LSB) algorithm in prudent manner and the stego file is formed. The stego file consist of cover audio and encrypted data is transmitted the key produced during encryption is only known to the receive.Decryption is the inverse process of encryption from which the audio signal is extracted and the data is decrypted .Thus the encryption and Decryption has been made using Verilog Hardware Description Language and simulated using ModelSim.The synthesis designs were implemented in Quartus-II software.

Key words - Least Significant Bit (LSB) algorithm, Linear Feedback Shift Register (LFSR) algorithm, Stego file, intruder, modelsim ,Quartus-II software, hex editor neo software

I.INTRODUCTION

Data hiding is the recent technique for ensuring the privacy of data transmitted over multimedia. As the usage of internet as transmission mode is highly developed .We also realize the rose of unauthorized access. Due to this the need for security of data is also increased. There are various method used to encrypt and compress the data to maintain thesecrecy, but the encryption of data alone will not be very efficient to protect confidentiality.

The steganography and cryptography are used in this paper for protecting the security and also the confidentially of data. Cryptography is used for enciphering of data. [2]

Steganography means concealing of data. The pro of the steganography over cryptography is the text will not be noticeable .The need for steganography arouse because of the significant increase of malicious users.

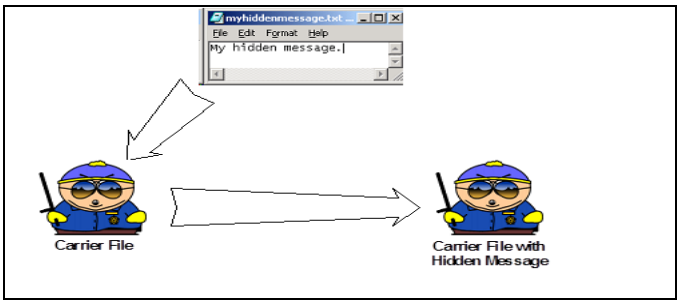

FIG 1.0 STRUCTURE OF STEGANOGRAPHY

In the proposed system there are four actions performed they are represented as[3-6]]

1. Encryption
2. Encoding
3. Decoding
4. Decryption

The text is encrypted with the use of keys and represented as unreadable code. The audio signal is converted into binary format and the encrypted data is encoded using LSB (Least Significant Bit) encoding Algorithm and transmitted over the network in imperceptions manner. In the decoding and decryption the inverse process of previous steps are followed. Thus the Audio signal is decoded and data can be retained without any damages.

According to the Encryption and data hiding are two effective means of data protection. While the encryption techniques convert plaintext content into unreadable cipher text, the data hiding techniques embed additional data into cover media by introducing slight modifications.[1]

The image is encrypted with key and thus the cover image is formed the text is hidden in the encrypted image using Least Significant Bit algorithm then it's conveyed to receiver. In receiver the data is extracted and the image is be decrypted by the reverse operation of encryption .The block diagram of existing system is given below.

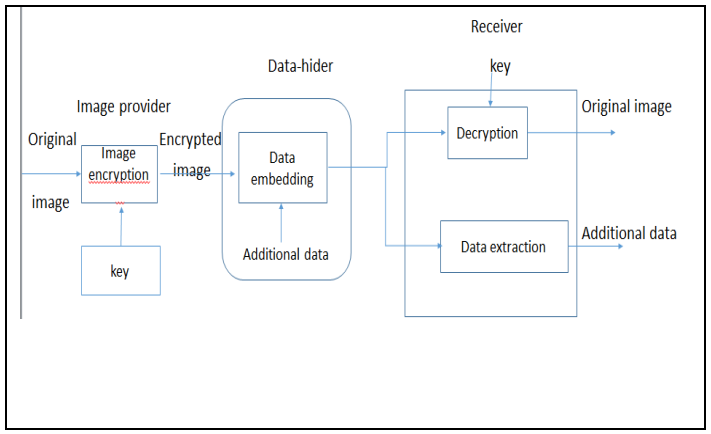

FIG1.1 EXISTING SYSTEM

The difficulties faced in practical implementations are:-
1. The quality of decrypted image is significantly degraded due to the disturbance of additional data.
2. The existing system loss the cipher text data during decryption process
3.An attacker can easily decrypt all cipher text blocks that were weakened.

II.PROPOSED SYSTEM

In order to overcome the cons of the existing system the proposed system uses the audio signal to conceal the text data in it .The audio signal is converted into its binary form using the Hex editor software. The text is encrypted with the use of key. Then the encrypted data is hidden is hidden in audio signal using Least Significant Bit algorithm.

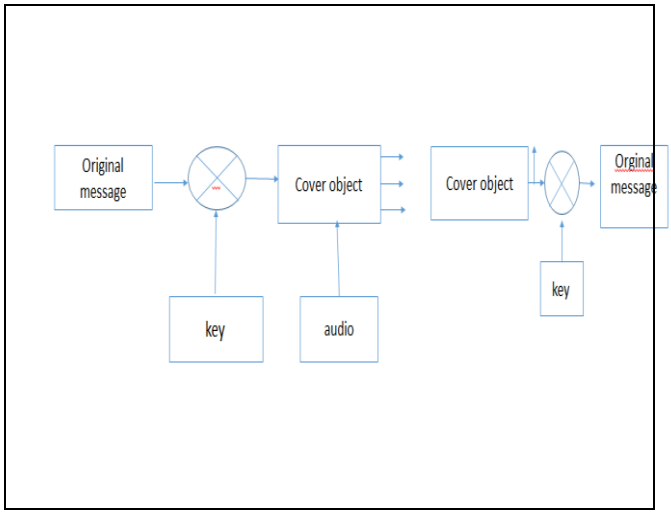

FIG: 2.0 PROPOSED SYSTEMS

The main goal of Text data hiding in Audio signal is to hide messages inside the audio in a way that does not allow any enemy to even detect that there is a second secret text message present in the audio using LSB encoding technique.

It can also be used for inserting hidden data into audio files for the authentication of spoken words and other sounds and for monitoring of the song over broadcast radio.

Text data is hidden in audio file without disturbing the quality of the audio file.

II.A. ENCRYPTION AND DECRYPTION

The encryption is the method of enciphering the original text data in obscurity manner. The enciphered data is called as the chiper data.Then the data cannot be read by the attackers. It is one of the methods in cryptography[3-8]

There are two types of keys symmentrickey and asymmentric key .The asymmentric keys are the public keys .the symmentric keys are the private keys.

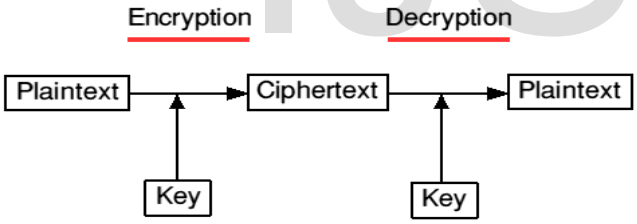

FIG 2.1 STRUCTURE OF ENCRYPTION & DECRYPTION

There are various algorithm used for text encryption like ADVANCED ENCRYPTIION STANDARD (AES). DATA ENCRYPTION STANDARD (DES), SHA 256 Algorithm etc.

Then in the reception the deciphering operation is performed by the receiver to read the text transmitted by sender. This ensures the security of data conveyed

II.A.1 TEXT ENCRYPTION.

In the proposed system we use key based encryption algorithm. The original data is of size 32 bit “SUGU” is performed EXCLUSIVE OR operation with key of same 32 bit. Then the unreadable format of the script is obtained at output as encrypted data.

This is the shown in the figure below

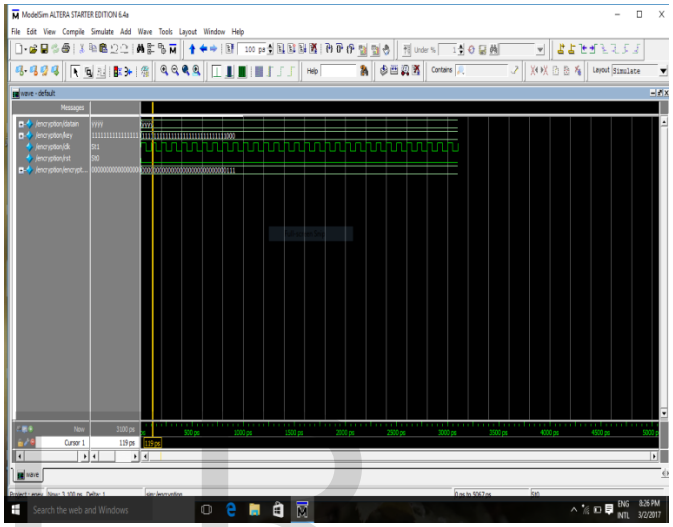

FIG: 2.2 SIMULATIONS OF ENCRYPTED DATA

The text is obtained as unreadable code at the output. Therefore it ensures the security of data conveyed over internet from eavesdropper.

The LFSR(linear feedback shift register) algorithm is a shift register used for performing the EXCLUSIVE-OR operation

III. BINARY REPRESENTATION OF AUDIO SIGNAL

The audio signal is the representation of sound so it is also called as speech signal as they are audible to human beings It is continuous according to the vibration frequency.

The audio signal in the mp3 format is taken as sample original signal and it is at the size of 3MB.The audio signal is analog and continuous signal.

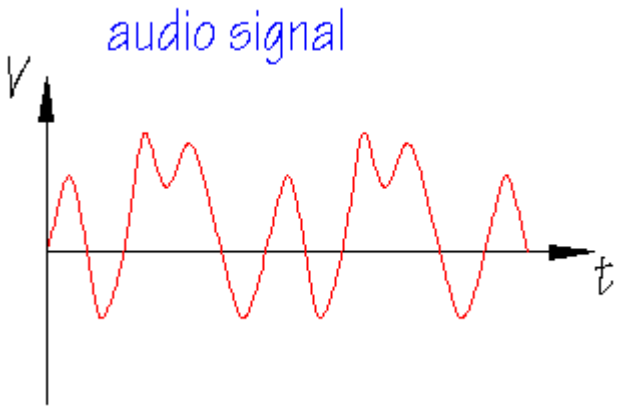

FIG: 3.0 REPRESENTATION OF AUDIO SIGNAL

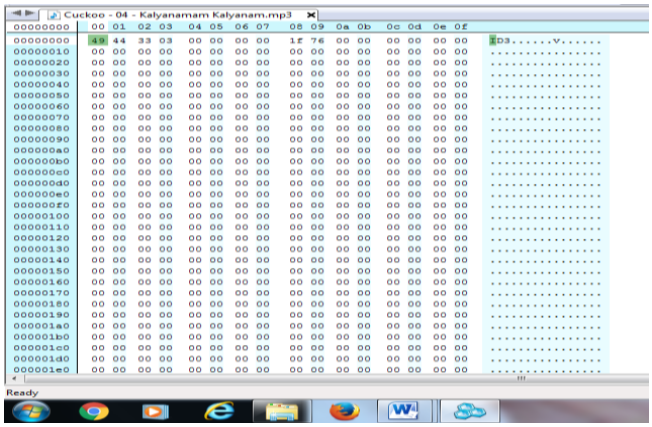

FIG 3.1 BINARY REPRESENTATION OF AUDIO SIGNAL

The audio signal is converted into its digital form using hex editor software. Then the encrypted data is concealed in the audio signal using Least Significant Bit encoding algorithm.[6]

The audio signal is represented in the bit pattern of 16 bit. The least or the first bit of an audio signal is compressed at that space the encrypted data is concealed and conveyed in the imperceptions manner.

The least bit of an audio signal is choosen because the least bit of an audio signal does not contain many information of audio signal.

So the signal may be recovered without any loss of an audio signal in the destination

Then an audio signal is converted into its binary bit form using the software hex editor .

The audio selected here is in the mp3 format .the binary bit pattern of the audio signal is given in the picture.it is the hexacode representation of an audio signal which is given as input to the software hex editor neo.

IV LEAST SIGNIFICANT BIT ENCODING ALGORITHM

It is the most efficient method of the steganography this is used for "concealed writing " that is the encrypted data will be hidden in the least and first bit of the audio signal in the imperceptions manner .the example is given below [6,9]

01011101 11010000 00011100 10101100

11100111 10000111 01101011 11100011

Becomes

01011100 11010001 00011100 10101100

11100110 10000110 01101010 11100011

FIG: 4.0 EXAMPLE OF REPRESENTATION LSB ALGORITHM

The data transmission is not visible to the other intruder except the authorized receiver with the key. When the conveyance of data is not visible to others. .It ensures the confidentiality and secrecy of data conveyed from intruder over the internet in multimedia, as the data is represented in imperceptions manner.

The audio signal of 3 MB in size is selected and it is in the MP3 format as mentioned above the 32 bit of encrypted data is embedded in the binary representation of audio signal is it .(i.e..) ”11111111000000001111000011100 0” is substituted in the least bit of the audio signal in the imperceptions manner. It is explained in the picture below.

The audio signal will not be degraded as the encrypted data is substituted in the least bit of the audio signal.so the signal can be obtained without any degradation .

The picture red colour representation of binary pattern represents the encrypted data in the binary bit patterns of audio signal which is substituted in the least significant bit of audio signal using Least Significant Bit encoding algorithm

It is represented clearly in the image below that the least bit of the first 512 samples are encoded.

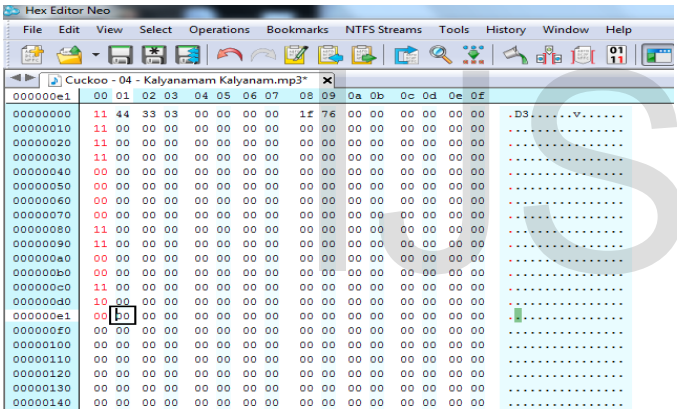

FIG: 4.1 ENCRYPTED DATA IN AUDIO SIGNAL

V.DECODING AND DECRYPTION

The receiver receives the signal and perform the inverse operation of the encryption and Least Significant Bit encoding algorithm.

The receiver first decodes the audio signal using Least Significant Bit decoding algorithm, as the audio signal can be extracted from the encrypted data.

Then decryptions process is carried out to obtain the original text data at the receiver. Thus the enciphered data in obscurity manner is deciphered into readable text.

Hence the challenge of the transmission of data over the multimedia in confidential and highly secured manner using integration of two effective concepts of cryptography and steganography is conquered and enhanced in the convincing manner..

VI.CONCLUSION

This project is the combination of both steganography and cryptography algorithm. This is used to ensure protection of privacy of data conveyed in multimedia over internet.

The cryptography is based on the Linear Feedback Shift Register(LFSR)which is a shift register that performs one bit EXCLUSIVE-OR operation of data and key represents encrypted datawhich is enciphered data and appears to be in obscurity manner.

The audio signal is converted into its binary bit pattern with the help of the software hex editor neo

In steganography, Least Significant Bit encoding algorithm is used to conceal the encrypted data in the least bit of an audio signal.

The inverse process is performed in receiver and then an audio signal is decoded and text is decrypted to obtain an original text and an audio signal.

Hence the key based encryption in cryptography methods and Least Significant Bit encoding algorithm.in steganography methods are very efficient method to ensure the privacy of data conveyed over the multimedia using the internet.

REFERENCES

[1] Xinpeng Zhang, Jing Long, Zichi Wang, and Hang Cheng” Lossless and Reversible Data Hiding in Encrypted Images with Public Key Cryptography” IEEE Transactions on Circuits and Systems for Video Technology 10.1109/TCSVT.2015.2433194,

[2] Bankarpriyanka R. Katariyavrushabh R. Patilkomal K. Shashikant M. Pingl E and Sanghavimahesh R" AUDIO STEGANOGRAPHY USING LSB" 1st International Conference on Recent Trends in

[3] K.P.Adhiya Swati A. P" Hiding Text in Audio Using LSB Based Steganography" Information and Knowledge Management Vol 2, No.3, 2012

[4] M. Sumathi*, D. Nirmala**, R. Immanuel Rajkumar" Study of Data Security Algorithms using Verilog HDL" International Journal of Electrical and Computer Engineering (IJECE)
Vol. 5, No. 5, October 2015,

[5] Nishu Gupta1, Mrs.Shailja2" A Practical Three Layered Approach of DataHiding Using Audio Steganography"International Journal of Advanced Research in Computer and Communication EngineeringVol. 3, Issue 7, July 2011

[6] AbikoyeOluwakemi C. AdewoleKayodeS.andOladipupoAyotunde J."Efficient Data Hiding System using Cryptography and Steganography"International Journal of Applied Information Systems (IJAIS) – ISSN : 2240868 Foundation of Computer Science FCS, New York, USA Volume 4– No.11, December 2012

[7] Gunjan Nehru1, Puja Dhar2" A Detailed look of Audio Steganography Techniques usingLSB and Genetic Algorithm Approach" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, January 2012

[8] AartiMehndiratta , " Data Hiding System Using Cryptography & Steganography: A Comprehensive Modern Investigation" International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 Volume: 02 Issue: 01 | Apr-2015

[9] Padmashree G, Venugopala P S, "Audio Stegnography and Cryptography: Using LSB algorithm at 4th and 5th LSB layers" International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 4, October 2012

[10] S. Raveendra Reddy1, Sakthivel S M2 , "A FPGA IMPLEMENTATION OF DATA HIDING USING LSB MATCHING METHOD" International Journal of Research in Engineering and Technology Volume: 04 Issue: 03 | Mar-2015,

[11] Navnath S. Narwade, VikasBhagasara, Mahesh Kanthali, and RushikeshPailwar , " Enhanced Data Hiding Model in Audio to Ensure Secrecy" International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 9, March 2013

[12] ChhayaVarade, Danish Shaikh, Girish Gund, Vishal Kumar, and Shahrukh Qureshi , "A Technique for Data Hiding using Audio and Video Steganography" International Journal of Advanced Research in Computer Science and Software EngineeringVolume 6, Issue 2, February2016

[13] Rituraj Rusia1, Munendra Kumar Mishra2, R.andK.Tiwari , "
Data Hiding using LSB Steganography technique" RiturajRusia et al, Int.J.Computer Technology &Applications,Vol 5 (4),1495-1505July-August 2014

.