International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 01 | Jan -2017 www.irjet.net p-ISSN: 2395-0072

Secure Audio Data Transfer over Internet Using Steganography

Shweta Hallale[1], Nikita Gaikwad[2], Aayushi Kachole[3], Shivanee Kamble[4],

S.P.Pingat[5] (Assistant prof.)

Department of Computer Engineering,

Smt. Kashibai Navale College of Engineering,

Pune, India.

***Abstract*–-** *Steganography is an art of hiding information in a host signal. It is very important to hide the data efficiently, as many attacks made on the data communication. The host signal can be an image, speech or video and the message signal that is hidden in the host signal can be a text, image or an audio, video signal. The cryptography concept is used for locking the secret message in the cover file. Due to cryptography the secret message will not get decrypted easily. It is related with constructing and analyzing various methods to overcome the influence of third parties. Modern cryptography works in many disciplines like mathematics, computer science and electrical engineering. In this paper a symmetric key is developed which consists of reshuffling and secret arrangement of secret data bits in cover image data bits. In this paper the authors have performed the encryption process on secret speech signal data bits-level to achieve greater strength of encryption which we have hided inside the cover image. The encryption algorithm applied with embedding method is the robust secure method for data hiding.*

Key words: Steganography, Encryption, Secret key generation,Decryption.

1. INTRODUCTION

1.1 Problem Statement

In today's internet world the data transmission should be fast and secured. The secret signal data gets hacked by breaking the password assigned to the system. Thus it is very important to design a secure encryption method for perfect data security. Many public places such as Banking sectors, Share markets, different Industry sectors, Educational sectors, IT industries, Government sectors and Medical sectors required secured secret data transmission. There is much software developed by the hackers to attack on any secret key (password). It means only user ID and password are not enough to protect the secret data. The confidential data must be hidden in encrypted form. There are two types of cryptography algorithm. symmetric-key cryptography used for the encryption process in which sender and receiver uses the secret key. Public key cryptography used only for encryption and decryption. There are various types of secret key encryption schemes are designed for implementation in software. The secret key cryptography schemes are categorized as stream ciphers or block ciphers. The stream ciphers works on single bit or byte at a time and implement some form of feedback mechanism so that the key is constantly changing. A block cipher is used to encrypts one block of data at a time using the same key on each block.

2. LITERATURE SURVEY

SRN 0.	REFERENCES	PUBLICATION	TECHNIQUES
1	Hiding Encrypted data in audio WAV file.[1]	IEEE 2014	In this method data encryption standard asymmetric algorithm is used to design encipher and decipher blocks.
2	Five level cryptography in speech processing in multi hash and repositioning of speech elements.[2]	IEEE 2015	In this paper cryptography technique is applied on audio to increase the security of audio data during transmission.
3.	Universal steganography model for low bit-rate speech code[5]	IEEE 2015	One level security provided. No secret key has been used.
4.	A challenge in hiding encrypted message in LSB and LSB+1 bit positions in various cover files.[4]	IEEE 2012	In this paper the secret message is encrypted by MSA algorithm and further encrypted message hide inside the cover file by changing ths LSB and LSB+1 Bits of cover file.

3. PROJECT SCOPE

3.1 Introduction

Robust method to encrypt a secret speech signal message inside cover image will be developed. The secret key will be generated within the encryption algorithm directly according to the entered letters and numbers at transmitter end. For the decryption of hidden file one has to go through 2 raise to 512 combinations of characters and numbers which is very difficult for attackers to hack the secret data. The secret data will be received by the authorized person at receiver end only when the secret key is entered correctly. This proposed method is very secure from hackers as 256 * 2 bit maximum key length can be used. Every time a new secret key will be generated even though the same secret signal entered as the key developed is stored in the database and compared with key which is at transmitter end. This encryption method generates an encrypted secret key which provides optimized security for hiding the secret speech data inside the cover image.

3.2 The Aim:

- To develop a symmetric key which consists of reshuffling and secret arrangement of signal data bits in cover image data bits.
- To develop the encryption process on secret speech signal data bits level to achieve greater

strength of encryption which gets hidden inside the cover image.

3.3 The Objective:

- To embed the audio file inside the cover image using different techniques of steganography.
- To hide audio as well as text message inside cover image.
- It is used to be as a supplement encryption process to prevent unauthorized access from being detected.

4. SYSTEM DESIGN

4.1 Proposed System: The proposed method for audio signal encryption we are generating a secret key. The system consists of 512 bits key size to encrypt a speech message. For more security we are adding noise in audio file and hiding this inside a cover image.

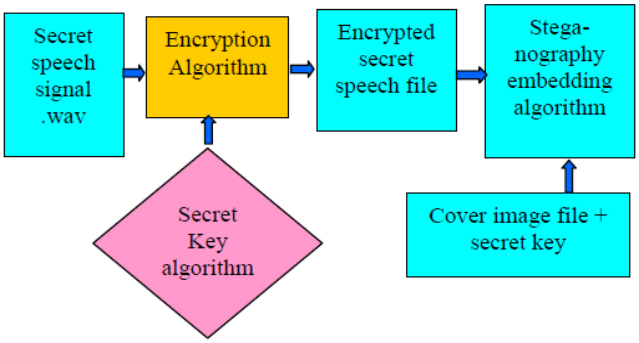

Fig 4.1.1 Proposed System (Transmitter end)

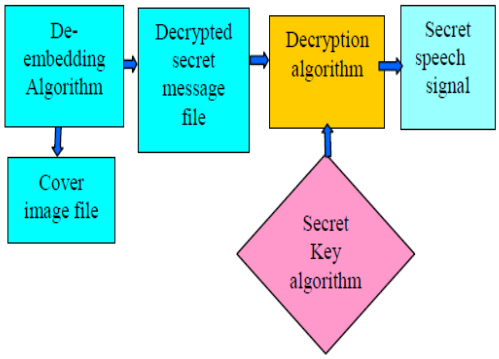

Fig 4.1.2 Proposed System(Receiver end)

4.2 Main Modules:

GUI: It is used to interact with the user. GUI reflects the basic appearance of the application.

Encryption: For audio file encryption enter the secret speech signal. This process involves adding high frequency noise bits at low frequency components of the signal. Use of Least significant bits embedding method to hide the data thus audio WAV file used for encryption. This can be achieved by XORing secret key with binary data.

Secret Key: Enter random combinations of letters and convert it into its ASCII value.Secret key size must be of 8 digits. Make 4 blocks of 8 bytes each. Apply XOR technique.Final generated key is a secret key stored into the transmitter end.

Steganography: In this use of least significant (LSB) bits embedding method to hide data. In this algorithm

LSB of each pixel is replaced by data to be hidden.

Decryption: This algorithm is used to retrieve the secret speech file. The authorized person who entered the correct secret key can decrypt the secret audio signal.

5. SYSTEM ANALYSIS

5.1Data flow diagram:

A data flow diagram (DFD) is a graphical representation of the "flow" of data through an information system, modelling its process aspects. A DFD is used as a primary step to create an overview of the system, which can later be elaborated.

Level 0:-

User gives the input into the form of image file, this file contains audio data which is hidden inside this cover image file. Then apply encryption algorithm on input file for the required output image.

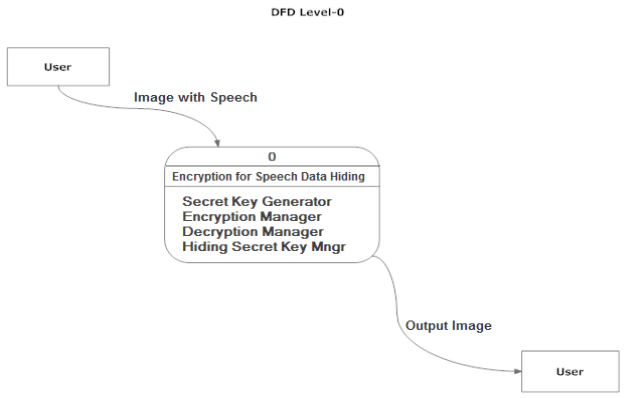

Fig 5.1.1

Level 1:-

Input is given by user in the form of image file with speech data. Secret key is generated. Using secret key manager this key gets hidden inside input file.

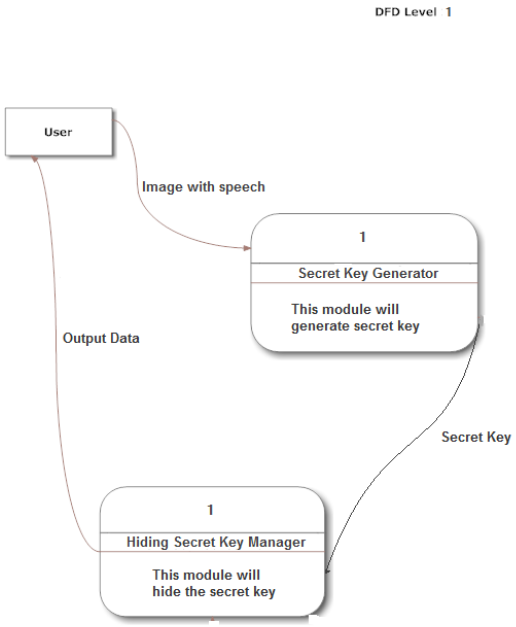

Fig 5.1.2

Level 2:-

Encryption and decryption is performed according

To the algorithm.

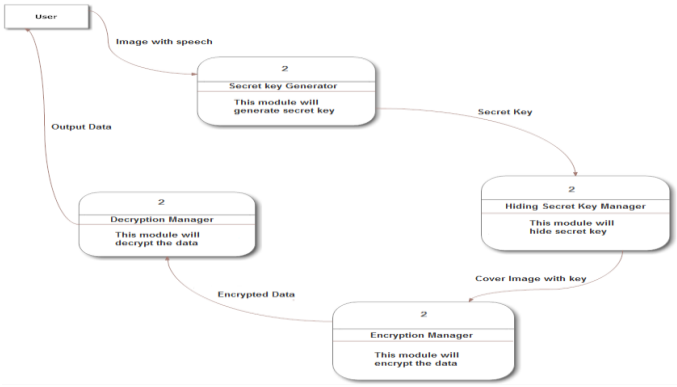

Fig 5.1.3

5.2 Use Case Diagram

This diagram consists of Actors. Our system consists of only 1 Actor. Following functionalities are handled by application: Login, image file, audio file, video file, Logout.

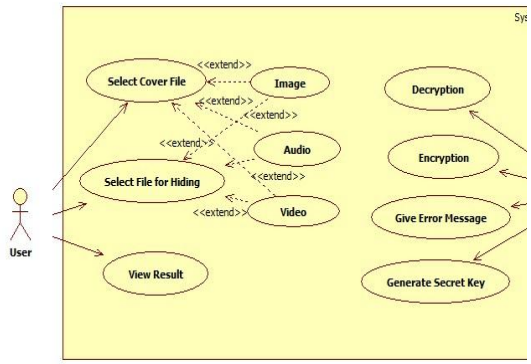

Fig 5.2

5.3 Activity Diagram

This diagram helps us to understand the activities are performed.

Login: - We **verify** the user by login id and password and if it is correct then its logins **successfully**.

After the successful login user selects cover image and audio file is selected. The system generates the secret key.

Check whether it is correct or not. Now hide that key inside image. Then data get encrypted. At receiver side it is get decrypted and original secret speech is retrieved.

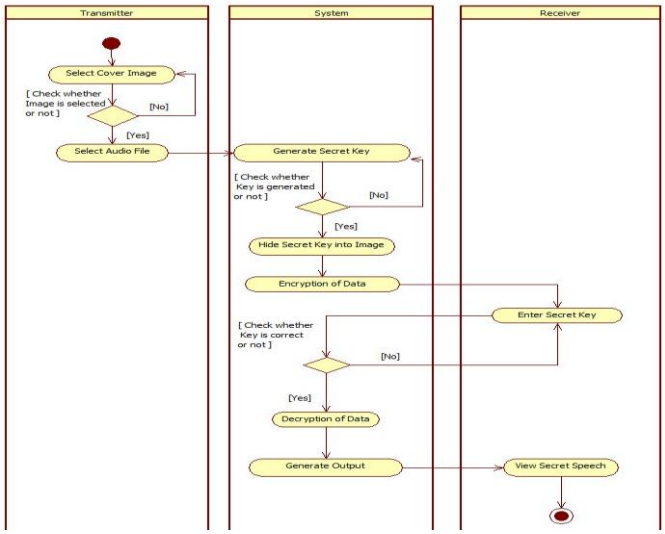

Fig 5.3.1

6. FEASIBILITY AND MATHEMATICAL MODEL

Set Theory Analysis

1. Let 'S' be the "Robust Steganography"

   S= {S1, S2, S3….., Sn}

   Set S is divided into5 modules

   S1= Authentication (AT)

   S2= Encryption (ENC)

   S3= Decryption (DEC)

   S4= Key Generator (MB)

   S5= Graphical User Interface (GUI)

2. Identify the inputs as I.

   Inputs = {X1, X2, X3, ……..Xn}

   X1= Message

   X2= Cover Image

   X3= key

3. Identify the output as O.
   a. Outputs = {Y1, Y2, Y3, ……..Yn}
   b. Y1= Original Message

Let S1 be a set of login request.

S1= {username, password}

If (username/password incorrect)

Discard request

Else

Success

F1: proceed()

Let S2 be a set of encryption having following parameters:

S2={message, cover_image, key}

Where,

Message: message to be encoded

Cover_ image: Cover image in which message is going to encoded

key: encoded key

Let S3 be a set of decryption having following parameters:

S2={message, cover_image, key}

Where,

Message: message to be decoded

encoded_image: Encoded Image from which original to be decoded.

Key: decoding key

As described above in entire Process: Robust Stenography

Input: Message to be hidden

Output: Original Message

7. CONCLUSION

This paper has looked in detail at the major techniques used for data hiding in audio files. This paper gives particularly the concept of audio steganography. We used steganography algorithm LSB coding for audio data. At the end feasibility of audio steganography was evaluated by considering its pros and cons.

8. REFERENCES

[1]. Joyshree Nath Sankar Das Shalabh Agarwal and Asoke Nath "A challenge in hiding encrypted message in LSB and LSB +1 bit positions in various cover files" Journal of global research in computer science vol. 2 no. 4 pp. 180-185 April 2011.

[2]. Satyaki Roy Joyshree Nath A. K. Chaudhari Navajit Maitra Shalabh Agarwal and Asoke Nath "Ultra Encryption Standard (UES) Version-IV: New Symmetric Key Cryptosystem with bit-level columnar Transposition and for Reshuffling of bits" International Journal of Computer Applications vol. 51 no. 1 pp. 28-35 August 2012.

[3]. Harjinder Kaur and Gianetan Singh Sekhon "A four level speech signal encryption algorithm" IJCSC vol. 3 no. 1 pp. 151-153 January 2012.

[4]. Divya Sharma "Five level cryptography in speech processing using multi hash and repositioning of speech elements" International Journal of Engineering Technology and Advanced Engineering vol. 2 no. 5 pp. 21-26 2012.

[5]. M. Nutzinger "Real Time attacks on Audio Steganography" Journal of Information Hiding and Multimedia Signal Processing vol. 3 no. 1 pp. 47-65 2012.

[6]. Krishna Kumar Pandey Vikas Rangari and Sitesh Kumar Sinha "An Enhanced Symmetric Key Cryptography Algorithm to Improve Data Security" International Journal of Computer Applications vol. 74 no. 29 pp. 29-33 July 2013.

[7]. Joyshree Nath Saima Ghosh and Asoke Nath "Advanced digital steganography using encrypted secret message and encrypted embedded cover file" International Journal of Computer Applications vol. 46 no. 14 pp. 1-7 May 2012.

[8]. S. M. Elshoura and D. B. Megherbi "A secure high capacity full-gray-scale-level multi-image information hiding and secret image authentication scheme via tchebichef moments" Journal of signal processing vol. 28 pp. 531-552 2013.

[9]. Hemlata Kohad V. R. Ingle and M. A. Gaikwad "An overview of speech encryption techniques" International journal of Engineering research and development vol. 3 no. 4 pp. 29-32 August 2012.

[10]. Dripto Chatterji Joyshree Nath Suvadeep Dasgupta and Asoke Nath "A new symmetric key cryptography algorithm using extended MSA method: DJSA symmetric key algorithm" International conference on Communication systems and network technologies.