International Journal of Research
ISSN: 2348-6848 Vol-3, Special Issue-6
National Conference on Recent Engineering Trends
NCRET- 2016
Held on 16th March 2016 organized by Institute of Knowledge College of Engineering, Pune, India.

"A Novel System to Increased Security of Audio Data Using Digital Images"

Neeta Pingale
npingale27@gmail.com
Shweta Khedkar
shwetakhedkar1012@gmail.com
Bhau Gawade
mailmebhau.gawade@gmail.com
Prof. Ritesh Thakur
hod_comp_iok@yahoo.com

SP's Institute of Knowledge College Of Engineering, Department of computer engineering, Pimple Jagtap, Pune-412208.

Abstract:
Steganography is an art of hiding information in a host signal. The goal of steganographic systems is to obtain secure and robust way to conceal high rate of secret data. It is very important to hide the secret data efficiently, as many attacks made on the data communication. The host signal can be a still image, speech or video and the message signal that is hidden in the host signal can be a text image or an audio signal.
The cryptography concept is used for locking the secret message in the cover file. The cryptography makes the secret message not understood unless the decryption key is available. It is related with constructing and analyzing various methods that overcome the influence of third parties. A symmetric key is developed which consists of reshuffling and secret arrangement of secret signal data bits in cover signal data bits. We have performed the encryption process on secret speech signal data bits-level to achieve greater strength of encryption which is hidden inside the cover image. The encryption algorithm applied with embedding method is the robust secure method for audio data hiding.
Keywords:—Cryptography; Encryption; Secret signal; Cover signal; Secret key.

Introduction:

Now a days, every person access information from Internet and today's requirements from internet world is the data transmission should be fast and secured. Steganography is the process of hiding a secret message within a larger one in such a way that someone cannot know the presence or contents of the hidden message. Although related, Steganography is not to be confused with Encryption, which is the process of making a message unintelligible Steganography attempts to hide the existence of communication.

The basic structure of Steganography is made up of three components: the "carrier", the message, and the key1. The carrier can be a painting, a digital image, an mp3, even a TCP/IP packet among other things. It is the object that will 'carry' the hidden message. A key is used to decode/decipher/discover the hidden message. This can be the password.

In this our main focus is on the use of Steganography within digital images (BMP) using LSB Substitution, although the properties of Image Steganography may be substituted with audio .wma and .wav digital document format relatively easy.

Problem Statement:

1. To develop symmetric key which consists of reshuffling and secret arrangement of secret signal data bits in cover signal data bits.

2. To develop the encryption process on secret speech signal data bits-level to achieve greater strength of encryption which is hidden inside the cover image.

An overview of speech encryption techniques, in this paper speech scrambling techniques are used to scramble the secret speech data. In this method the speech signals are encrypted by using different pseudo-noise sequences is compared by informal listening tests and signal inspection method in time and frequency domains. Pseudo-noise sequence have random like properties used in reducing the correlation among the speech samples. The speech encryption techniques using pseudo-noise sequences make the speech signal understood by removing the correlation between the samples of the speech signal [9]. Hiding Encrypted data in audio wave file, in this method data encryption standard asymmetric algorithm is used to design encipher and decipher blocks of data consisting of 64 bits under control of 64 bits key. Cryptography in speech processing are multi hash and repositioning of speech elements, in this paper cryptography technique is applied on audio to increase the security of audio data during transmission. The encrypted message consists of background noise, hiss and clicking noise which represents meaningless to the unauthorized person. In this method even if one level of encryption is broken the rest of levels prevent the actual audio data [5].

Existing System

- **An overview of speech encryption techniques:**

  – Speech scrambling techniques are used to scramble the secret speech data.
  – The speech encryption techniques using pseudo-noise sequences make the speech signal un-understood by removing the correlation between the samples of the speech signal.

- **Hiding Encrypted data in audio wave file:**

  – In this method data encryption standard asymmetric algorithm is used to design encipher and decipher blocks of data consisting of 64 bits under control of 64 bits key.

- **Five level Cryptography in speech processing in multi hash and repositioning of speech element:**

– Cryptography technique is applied on audio to increase the security of audio data during transmission.

– The encrypted message consists of background noise, hiss and clicking noise which represents meaningless to the unauthorized person.

Drawbacks of Existing System

1. Can be easily decoded because of Scrambling (Inverted)

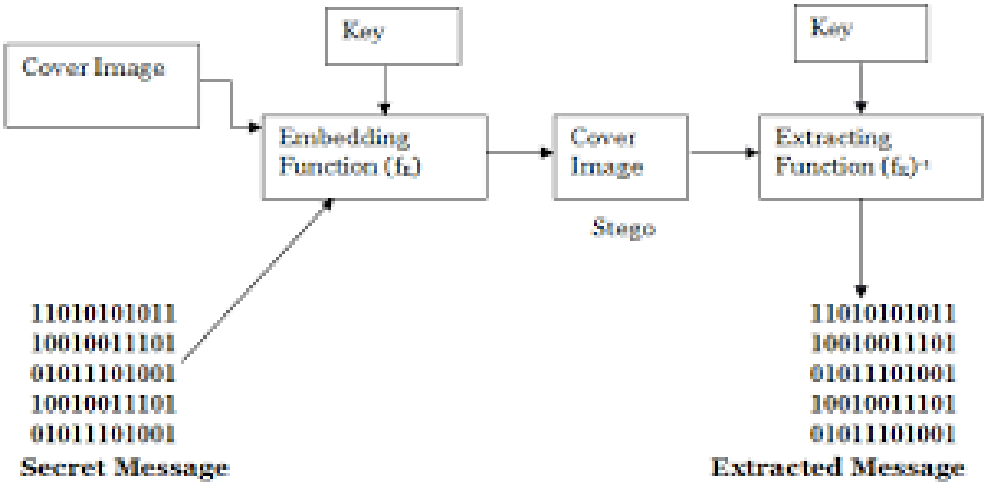
2. Decrypted Audio has background noise, hiss and clicking noise.

3. Only 64 bit key is used in encryption/decryption.

4. In this method even if one level of encryption is broken then rest of levels also failed.

Objectives and goals

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



Proposed system

1 A new proposed method for audio signal encryption for robust hiding.
2 The secret key will use for encrypting the input secret audio file.
3 The proposed system consists of 512 bits key size to encrypt a speech message.
4 To decrypt the secret file one has to know the exact secret key which find out position of the secret blocks.

5 The proposed method is very secure from network attacks as secret key generation is on the basis of 512 bit key which will be decided at transmitter end.

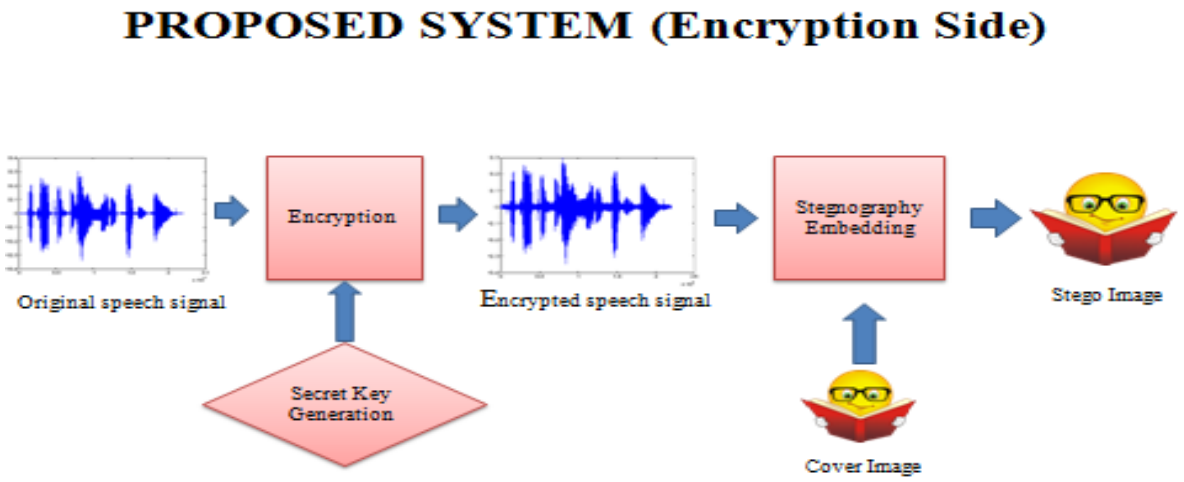


Fig. Encryption Side

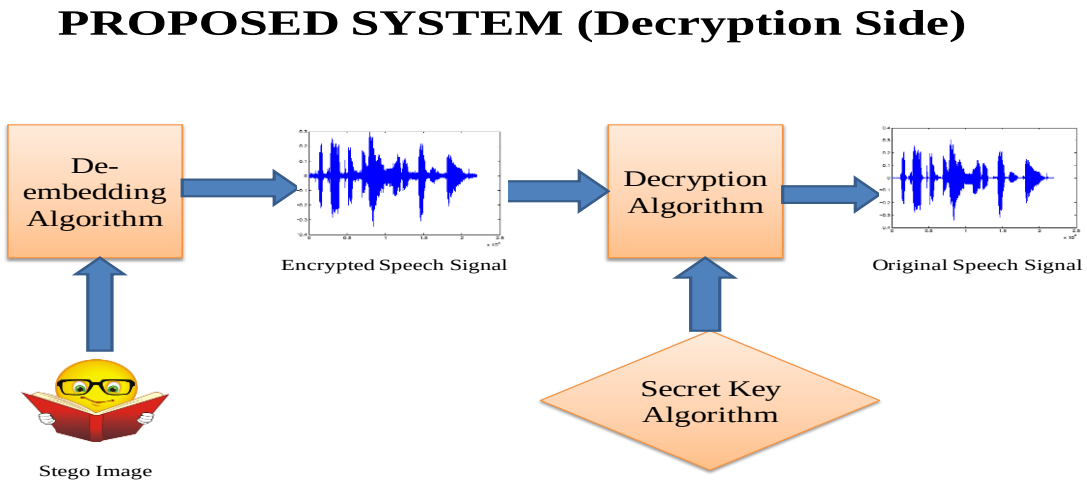


Fig. Decryption Side

Architecture of Project

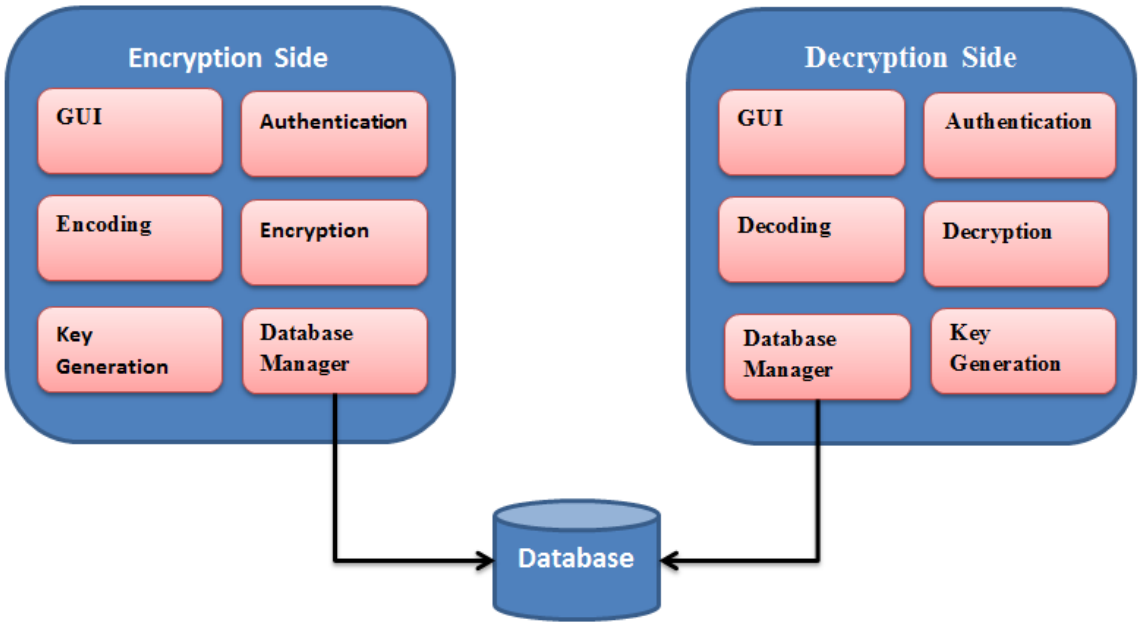


Fig. Architecture of Project

Advantages of Proposed System

- 512 bit key used.
- Custom key is used to make system more harder .
- Encryption and Encoding both technique used.

Algorithms Used for Proposed System

- In this Proposed system we use following algorithms:
  - Secret key generation.
  - Encryption of speech file.
  - Secret key hiding in cover image at transmitter end.

1. SECRET KEY GENERATION ALGORITHM

- Ask User to enter random combination of letters, numbers and special characters as a random number of size 16 to 128.
- Make secret key is 256 binary bits by converting the users ASCII value.
- Make 4 blocks of 8 bytes likes key block 1, key block 2, key block 3 and key block 4.

- Apply XOR operation between block 2 and block 4, result has to store in new key_ block I.

- Apply XOR operation between block 1 and 3, result has to store in new key_ block II.

- Apply XOR operation between key _block I and, key _block II result has to store in new Key _block III.

- Store the key_ block III as secret key into database at transmitter end.

2. ALGORITHM FOR ENCRYPTION OF SPEECH FILE

- User will enter the input speech signal.
- We have encrypt this speech signal using secret key.
  - Add high frequency noise bits at low frequency components of the signal.
    - Each bit value of speech signal is added using secret key bit value for positive signal in positive direction .
    - Each bit value of speech signal is added using secret key bit value for negative signal in negative direction.

1. ALGORITHM FOR SPEECH DATA HIDING IN COVER IMAGE

- Take Encrypted Speech data as input.
- Apply LSB Stego method to encode speech data into provided cover image.

2. ALGORITHM FOR DATA HIDING

- Use of Least significant bits embedding method to hide the data.
- All below 3 values.
  - Secret key.
  - Noise random number .
  - And Encrypted speech WAV file.

  Will get hidden into cover image.

Applications of System

- One of the main use of our project is for the transportation of high-level or top-secret documents between international governments.
- This can be used anytime when you want to hide data.
- In the business world our project can be used to hide a secret chemical formula or plans for a new invention.
- Terrorists can also use to keep their communications secret and to coordinate attacks.

Future Scope

We hope to add support to hide all file formats. This allows for a much broader spectrum of uses: one would be able to encode .txt, .exe, .doc, .pdf, .mp3, .mp4 etc.

We eventually plan to port the program to use C/C++/java so that we may take advantage of bit-fields in C/java and learn to code GUI's as well. We have a plug-in handler developed for C++/java that we would like to use in this project so that third-party developers may contribute to the project.

Conclusion: The original image and stego image with encrypted secret speech file hide inside the cover image.

References:

[1] "A Robust Encryption Method for Speech Data Hiding in Digital Images for Optimized Security", Sheetal A. Kulkarni ,

Shubhangi B. Patil International Conference on Pervasive Computing (ICPC)(2015).

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

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

[4] "A four level speech signal encryption algorithm", Harjinder Kaur, Gianetan Singh Sekhon IJCSC, Vol. 3, No. 1, PP. 151-153, January 2012.

[5] "Five level cryptography in speech processing using multi hash and repositioning of speech elements", Divya Sharma, International Journal of Engineering Technology and Advanced Engineering, Vol. 2, No. 5, PP. 21-26, 2012.

[6]"Real Time attacks on Audio Steganography", M. Nutzinger, Journal of Information Hiding and Multimedia Signal Processing, Vol. 3, No. 1, PP. 47-65, 2012.

[7] "An Enhanced Symmetric Key Cryptography Algorithm to Improve Data Security", Krishna Kumar Pandey, Vikas Rangari, Sitesh Kumar Sinha, International Journal of Computer Applications, Vol. 74, No. 29, PP. 29-33, July 2013.

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

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

[10] "A new symmetric key cryptography algorithm using extended MSA method: DJSA symmetric key algorithm", Dripto Chatterji, Joyshree Nath, Suvadeep Dasgupta, Asoke Nath, International conference on Communication systems and network technologies, 2011.

[11] "Encryption of speech signal with multiple secret keys in time and transform domains", E. Mosa, N. W. Messiha, O. Zahran, F.E. Abd El-Samie, International Journal of speech technology, Vol. 13, No. 4, PP. 231-242, December 2010.