"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 a part 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. Cryptography techniques are based on rendering the content of a message garbled to unauthorized people. 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. Modern cryptography works on the 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 signal data bits in cover signal data bits. In this paper 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 adays, every person access information from Internet and today's requirements from internet world is the data transmission should be fast and secured. There are some specific security requirements includes:
1) Authentication 2) Privacy/Confidentiality 3) Integrity 4) Non-repudiation.
The secret signal data may get hacked by breaking the password assigns to the system.

Thus it is very important designing a robust encrypted method for robust data security. Many public places such as Banking sectors, Share markets, Educational sectors, IT industries, Government sectors and Medical sectors required secured secret data transmission. There are many softwares developed by the hackers to attack on any weak secret key (password) [3]. It means only user ID and password are not enough to protect the secret message. The confidential data must be saved in the encrypted form. There are

two types of cryptography algorithm, first is symmetric-key cryptography used for the encryption process in which sender and receiver uses the secret key and another one is public-key cryptography used where the various keys are used for encryption and decryption. The various types of secret key encryption schemes are designed for implementation in software. The secret key cryptography techniques are categorized as stream ciphers or block ciphers [6], [8].

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.

Existing System

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 un 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].

Drawbacks of Existing System

1. Can easily decode due to use of standard algorithms.

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

Proposed system

In this section we describe a new proposed system for audio signal encryption for robust data hiding. In this technique, we will use the secret key for encrypting the input secret audio file. With the same cover file the secret message can be encrypt with different secret key. For the same secret message every time a new secret key is generated. By using this technique secret message encrypting procedure is done multiple times[11]. The proposed key blocks contains possible combinations of all characters ASCII code between 0 to 255 in random order. The pattern of the key blocks find out by using secret key entered by the user. The proposed system consists of $256 * 2 = 512$ bits key size to encrypt a speech message. To decrypt the secret file one has to know the exact secret key which find out position of the secret blocks. To find the position of the secret data one has to apply 2512 trial run which is very difficult for hackers. The secret

key generation is on the basis of 256 * 2 =512 bit key which will be decided at transmitter end so proposed method is very secure from network attacks [4], [7]. In the proposed system a common key is used between transmitter and receiver which is called as secret key.

In this system we use following algorithms:

1. Proposed algorithm for secret key generation
2. Proposed algorithm for secret key hiding in cover image at transmitter end
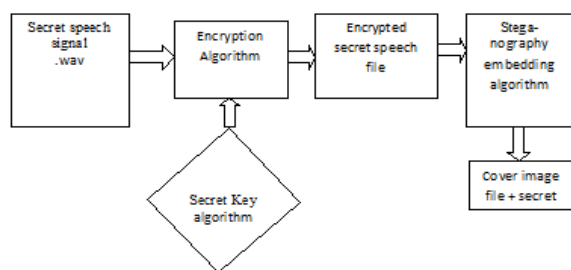3. Proposed algorithm for encryption of speech file

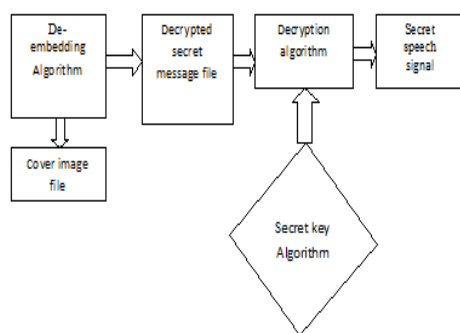Fig . Encryption at transmitter end.

Fig. Decryption at Receiver end

Advantages of Proposed System

1. **Hiding Encrypted data in audio wave file:**
   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:**
   In this method cryptography technique is applied on audio to increase the security of audio data during transmission

Hardware Interfaces

1. Processor – Intel Core2Duo, Pentium –III/i3
2. Speed – 2.4 GHz
3. RAM - 1 GB (min)
4. Hard Disk - 50 GB
5. Keyboard and Mouse

Software Interfaces

1. Operating System : Windows 7
2. Front End : Java 7
3. Back End : nil
4. JDK 1.7
5. Eclipse Indigo

Conclusion

This encryption method generates a robust encryption secret key which provides optimized security for hiding the secret speech data within 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.