Secure Data Transmission Using Image Steganography

A.Prema
Department of Information Technology,Velammal Engineering college, Chennai
V.Gowri
Assistant Professor, Department of Information Technology,Velammal Engineering college, Chennai

----------ABSTRACT----------

The internet is used to browse data faster in a secured manner. But just a username and password is not enough to protect the data because softwares are being developed to break weak passwords. So Cryptographic techniques are used to encrypt the data which helps in maintaining its privacy. Encryption is done based on the input given and decryption is done by using the secret key matrix combination. Speech encryption techniques using pseudo noise is implemented to hide the data in an audio file and the hidden data cannot be understood. In the new proposed method a new secret key is generated every time even the same message is sent. This enables multiple times secret message encrypting procedure. The authorized user finds out the secret key which contains the name noise using which the audio was encrypted. The noise name is verified from the noise database which is known to both transmitter and receiver. Then this noise is subtracted from the audio so that the audio will be completely decrypted. This is a much secured form of cryptography because the secret key is based on the input file and every time a new key would be generated for transmission so it is not very easy to guess the key.

Keywords - **Cryptography; Encryption; Secret s i g n a l; Secret key ; Cover image**

I. INTRODUCTION

In current internet phase, the transmission of information should be fast and secured . Confidential data transmission takes place in areas like Banking sectors, Share markets, Educational sectors, IT industries, Government sectors and Medical sectors etc. So data transmitted must be protected from getting hacked or must be protected from physical data damage. Nowadays many hackers develop softwares to attack on any weak secret key (password) [5]. Login credentials alone can't protect the confidential data. The secret information must be saved in the encrypted form using cryptographic techniques. 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 where the different keys are used for encryption and decryption. The various methods of secret key encryption schemes are designed for implementation in software. The secret key cryptography schemes are categorized as stream ciphers or block ciphers [8], [11]. The stream ciphers works on single bit at a time and implement some form of feedback mechanism so that the key is constantly changing. The same key is used to encrypt every single block of data is called block cipher. Cryptography is necessary for communicating over any non-secure medium, like internet. it has the following properties:
Authentication: process of determining whether who or what it is declared to be. Privacy/Confidentiality: the condition of being free from being disturbed by other people. Integrity: the state of being whole and undivided. Non-repudiation: guaranteeing message transmission between parties.
The paper is organized as follows – Section 1 Introduction and importance of cryptography and network security, Section 2 Existing work, Section 3 Proposed Method, Section 4 Experimental Results, Section 5 Conclusion.

II. EXISTING WORK

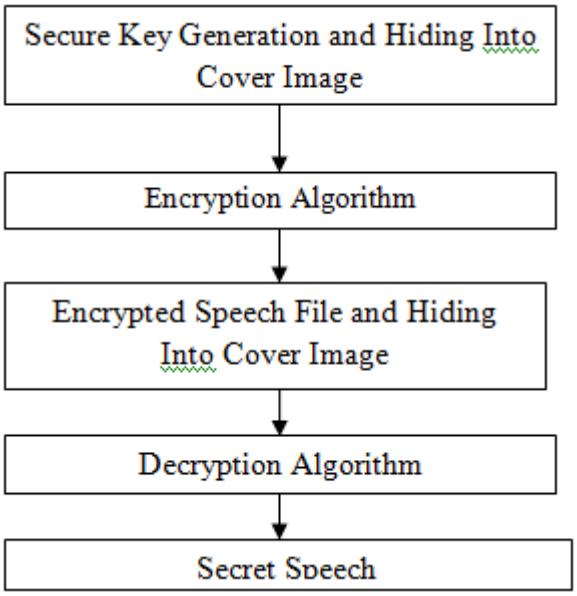
DJSA symmetric key algorithm, in this paper a symmetric key method is described where random key generator used for generating initial key. This initial key is used as secret key for encrypting the given source file. In this method substitution method is used where any four characters from random key matrix has to search similar to input file. For searching the characters, MSA algorithm was used. The pattern of the key matrix will depend on the user entered key characters combination. Randomization number and encryption number can be evaluated. For the decryption of secret file, user must know the secret key matrix combination. In this algorithm consists of all possible words each generated from ASCII code from 0 to 255 in a random order. The author had applied this algorithm on MS word file, MS Excel file, MS access, text file, image file, audio file, PDF file, video file and found correct solution for encryption when file size is 2 MB [13]. LSB and LSB+ 1 bit positions is a challenge to hide in encrypted message of various cover files, in this paper the secret message is encrypted by MSA algorithm by Nath [4] and further the encrypted message hide inside the cover file by changing the LSB and LSB + 1 bits of cover file. This methods is very useful for embedding data in non standard cover files . In this paper the size of the secret key must be less than or equal to 16 characters from any of ASCII characters.

To find the encryption key for the particular secret data, randomization number, encryption number and relative shift is calculated and according to that position of the character get changed. The size of the secret file and secret key is hidden inside the LSB bits of cover file [4].

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 [12].
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 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 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 prevents the actual audio data [7].

III. PROPOSED METHOD

This section describes a new proposed method for audio signal encryption for robust hiding.here the audio file is encrypted using secret key. The different secret key is used to encrypt the speech having the same cover file. Each time the same secret message uses a new secret key. This can be done multiple number of times [14]. all characters ASCII code from 0 to 255 are present in random order. the user uses secret key entered for the key pattern blocks. it has 256 * 2 = 512 bits by which the speech can be encrypted. the exact secret key must be known to decrypt the secret file to find the position of the secret blocks. the hacker find difficult when the position of data is modified by 2 trial run. at the transmitter end 256*2=512 bit secret key generation is used which is very secure from network attacks [6], [9]. The proposed technique uses a common key between transmitter and receiver which is called as secret key. The block diagram shown in Fig. 1.



IV. ENCRYPTION SIDE

Has the following four steps:

- Secret key generation,
- Key hiding in cover image,
- Encryption of speech file,
- Encrypted data hiding in cover image.

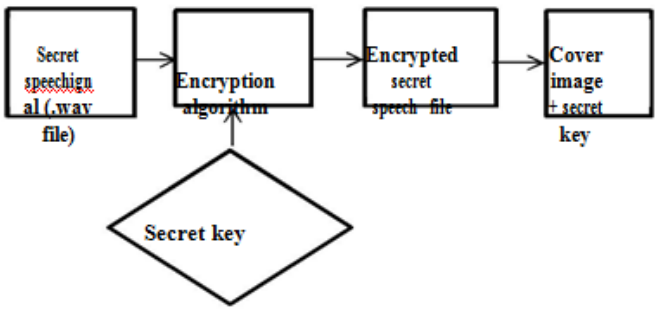


Fig 1: Encryption at transmitter end

4.1 Secret Key Generation

To encrypt the secret message a random secret key has to be generated before hiding it into cover file.Enter random combination of letters, numbers and special characters as a random number of size 16 to 128 .

- Convert the entered each letter and number into its ASCII value and then into binary bits from random number.
- Use total length of secret key is 512 binary bits by converting the ASCII value in either 32 bits to 4 bits binary as per random number.
- 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 [9].Apply Key hiding algorithm which is used for checking the original key and the key entered at receiver end.

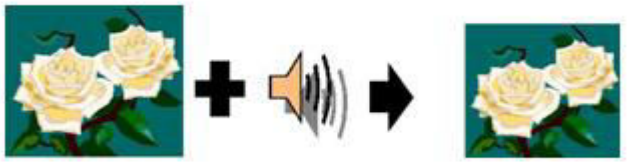
4.2 Hiding Secret Key in Cover Image

- Collect the secret key from the secret speech .wave file at transmitter end.
- Check the secret key is in binary form. right by 4 times and invert string then hide into cover image.
- If first two digits of secret key string is '01' then rotate left by 4 times and invert string then hide into cover image.
- If first two digits of secret key string is '10' then rotate right by 3 times and rotate left by 1 and invert string then hide into cover image.
- If first two digits of secret key is '11' then rotate left by 4 times and rotate right by 1 and invert string then hide into cover image.

4.3 Speech File Encryption

- Enter the secret speech signal.
- Apply Discrete Wavelet Transform on secret message and divide it into low frequency and high frequency components.
- Add high frequency babble noise bits at low frequency components of the signal.
- The random number is generated by using random number generator. Random number generator generates the value between -32767 to 32767 . If signal bit value is positive then the random number is generated between 0 to 32767. If signal bit or byte value is negative then the random number is generated between -32767 to -1.
- Each bit or byte value is subtracted from random number generated.
- Apply amplitude ascending order, the minimum value of the signal bits becomes the first value.
- Apply Inverse Discrete Wavelet Transform and modified the signal again.
- Check the size of original secret speech signal and encrypted signal is same [6]. Thus the encrypted speech signal is ready for hiding inside cover image.
- The original speech signal is shown in Fig. 3 and encrypted speech signal with babble noise is shown in Fig. 4.The decryption of secret speech is shown in block diagram Fig. 2. The reverse encryption algorithm is applied to retrieve the secret speech signal.

4.4 Encrypted Data Hiding in Cover Image



V. DECRYPTION SIDE

As two steps:

- Encrpted speech signal from hidden image,
- Secret speech signal.

The authorized person who entered the correct secret key can decrypt the secret message bits

5.1 Encrypted speech signal from hidden image:

The noise inside the image is taken with the help of the secret key .The secret key mast be the same key while entered during the encryption of speech signal. Fig. 4. Encrypted speech signal with 15 dB street noise [3]

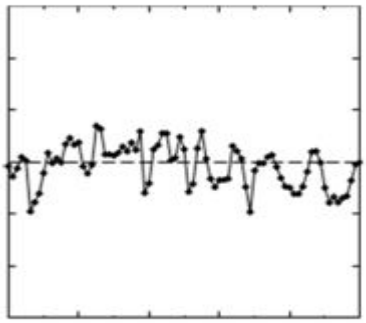


Fig. 3. Original Speech signal at exhibition [1, 2].

5.2 Secret Speech Signal

At this step we retrieve the speech from the cover image.

VI. EXPERIMENTAL RESULTS

The encrypted message with secret key generated also hidden into digital images [10]. The secret key generated by secret key algorithm is again go through secret key hiding algorithm. The authorized person who know the key retrieval procedure able to retrieve the secret key. The position of key hiding is decided at transmitter end by the user . The secret key generated at transmitter end contains the name of noise hidden inside the encrypted speech signal.

The original image and steganographed image with encrypted secret speech file hide inside the cover image shown in Fig. 5. In the above case of both the images we find that both the original image and the steganographed image appears to the same without any modifications .Here it becomes difficult to identify whether any information has been hidden inside the image.

VII. CONCLUSION

In this paper a robust encryption method to encrypt a secret speech signal message inside cover image is developed. The secret key is generated within the encryption algorithm directly according to the entered numbers and letters at transmitter end. For the decryption of hidden file one has to go through 2512 combinations of characters and numbers which is very difficult for attackers to hack the secret data and if the password is entered incorrectly for consecutively 3 times then the entire message available to the hacker is deleted completely. Every time a new secret key will be generated though the same secret signal entered as the key developed is stored in the database and compared at transmitter end .Thus the secret data will be received by the authorized person at receiver end only when the secret key is entered correctly.

REFERENCES

[1] The IEEE database: cs.utdallas.edu/loizou/speech/noiseus http://www.pacdv.com/sounds/voices-2.html www.wavesource.com/people/men.htm

[2] Joyshree Nath, Sankar Das, Shalabh Agarwal, 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.

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

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

[5] 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

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

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