INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

A NOVEL FRAMEWORK FOR SECURE DATA HIDING WITH A ROBUST ENCRYPTION METHOD.

MS. ROSHANI D. GHODESWAR.

Prof. Ram Meghe Institute of Technology & Research Badnera-Amravati, India.

Accepted Date: 15/03/2016; Published Date: 01/05/2016

Abstract: In the recent days internet is becoming most popular mean of data transmission. Many private and public sector such as government sector, medical sector, share markets, IT Industries, educational sectors uses internet for data transmission. The data transmission over internet facing a problem of data security as the confidentiality of is the most important issue. Many researches are going on to solve the problem of data security. Cryptography and steganography are the methods to achieve a data security. In a given paper a method is proposed by combining a steganography with encryption. In a given method the audio signal is used to hide a text data using steganography and then this signal is encrypted to provide a double layer of data security

Keywords: Steganography, Audio Steganography, LSB bit substitution method

PAPER-QR CODE

Corresponding Author: MS. ROSHANI D. GHODESWAR

Access Online On:

www.ijpret.com

How to Cite This Article:

Roshani D. Ghodeswar, IJPRET, 2016; Volume 4 (9): 438-444

INTRODUCTION

Internet is most widely used medium in a day to day life. It plays a vital role in the field of communication, commerce, Banking and various banking, privet sectors. Internet is fastest means of communication as large amount of data can be transferred in short duration of time. The transmission of data over an internet facing problem of security. Most of transactions done using a network require confidentiality of data such as bank transaction, e-commerce activities.

In order to provide the confidentiality to data transmitted over internet various encryption methods are used. Steganography is one of the data hiding technique used for securing data while transmitted over internet. Steganography is method of data encryption in which a secrete data is hidden in cover media. The secrete data that is to be hidden may be text, image, audio, video or animation. Similarly the cover media may be anything such as text, image, audio, video or animation. The Steganography is art of hiding secret information in cover medium.

In steganography the term is used stago -media which represents a cover media with hidden information. In steganography the original media and stago-media are seems to be similar in appearance. For example in case of image steganography both cover image and stago-image are similar in their physical appearance though technically there is deference in both.

I. EXISTING WORK

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 software's developed by the hackers to attack on any weak secret key (password) [1] Thus password is not enough to protect the data; data is to be encrypted while transforming over internet.

There are two methods of cryptography symmetric key cryptography and public key cryptography. In symmetric key cryptography sender and receiver both uses a same secrete key while in public key cryptography different keys are used for encryption and decryption. There secrete key cryptography is categorized as stream cipher and block cipher [2], [3].

Steganography:

Another method to achieve higher level of the security is steganography. Steganography is art and science of hiding file in another file. The terms used most commonly in steganography are given as

Cover Media: The file which is used to hide the information is known as cover media. The cover media may be any text file, audio file, image file or video

Secrete Data: The secrete data that is to be hidden in cover file. The secrete data may be any text, image, audio or video file

Stago-Media: The cover signals with a hidden secrete data is known as stago-Media

Steganalysis: It is process of recovering original data from stago- media.

One of the methods of speech encryption is five level cryptography. Five level cryptography in speech processing in multi hash and repositioning of speech elements, cryptograph 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. [4][5]

Our scenario is that two sides need to communicate with each other securely throughout local network or the internet. They need to ensure confidentiality of information transmitted using cryptography algorithm. While using a concept of steganography with an images, it is performed on binary format of an image in decimal to binary color digital images are made up of pixels and pixels are made up of combination of primary colors red green blue (RGB) [6].

Actually the concept of separate reversible data hiding technique is based on steganography and related with internet security. This technique based on attributes like compression-decompression, encryption decryption, data embedding- data extracting, creating space at LSB of the pixel of the image providing security [7] [8].

LSB Bit Substitution Method

Some modern steganography algorithm inserts the text characters directly in the LSBs of the image pixel's. Usually 24-bit or 8-bit files are used to store digital images. 24-bit images provide more space for data hiding. The color information is retrieved from three primary colors: red, green & blue. 24-bit images use 3 bytes for each pixel, where each primary color is represented by 1 byte. So in 24-bit images each pixel can represent 16,777,216 color values. The lower two bits of these color values are used to hide the data, but this change is so little that is undetectable for the human visual system. This method is known as Least Significant Bit insertion. [9]

II. PROPOSED WORK

A new proposed method for audio signal encryption in combination with data hiding the proposed system use of higher LSB bit replacement algorithm for data hiding. In this technique the secret audio file is encrypted using a secret key. This encrypted audio is again used to hide a secret message. With the help of higher LSB bit replacement the proposed algorithm uses a common key between transmitter and receiver known as positioning key

Methodology for secure data hiding with robust encryption method:

This encryption method provides a security to audio signal the whole process can be best described with following three sections:-

Proposed system uses a method of encryption of image for audio encryption. In image steganography the secrete information is hidden in cover image. The encryption process is then applied to this combination of data. Various methods are used for data hiding; the proposed method uses a higher LSB bit replacement method. Here we hide a secrete message in audio signal/data

A. Proposed method for encryption of secret audio signal

1. The audio signal is to be processed is in the form of wave which consist of samples
2. Each sample of the audio wave is in 8 bit and represented in a binary format
3. In proposed method the secret key is to be generated for encryption of the audio signal
4. The key is generated by permutation of numbers between 0 to 7 as each sample is 8 bit and number between 0 to 7 can be used to indicate position of bits in a sample Data Hiding

- For data hiding the secret data is to be converted into its binary format
- The data is then hide by using higher LSB bit replacement algorithm
- The encrypted output is encrypted stego-audio

B. Encryption Process:-

The encryption of stago-audio signal is done by positioning shifting the bits of sample of audio signal. Using no in a queue the bit at that position in a sample is swapped. After performing key based encryption method the encrypted audio signal is obtained.

C. Decryption Process:

The secret data that is to be hidden in encrypted stago-audio is extracted by using decryption algorithm. At this step stago-audio is obtain secrete data is extracted by data extraction method. Thus original audio signal and the secrete data is obtained. The decryption is carried out as given below:

1. At receiver side the receiver will get encrypted stago- audio which is encrypted from of the Secret audio with hidden secrete message.
2. The decryption algorithm is applied to the stago audio file
3. The decryption algorithm provides a decrypted stago- audio which is combination of audio data and secrete message.
4. Now to separate both secrete audio signal and secrete message signal data extraction method is used.
5. As a result of data extraction method two separate secrete information is obtain original audio signal and secrete message

III. EXPERIMENTAL RESULT

In a given paper an audio signal is used as cover file and secrete message is hidden at the higher LSB bit of an audio signal. After this step we get stago- audio is this stago –audio is then encrypted. Thus the resultant audio signal obtain is provide a double layer of data security by means of data hiding and encryption method used in combination with the steganography. The original audio and stago-audio are found to be same that is difference is not detected by human auditory system the screenshots given in figure 1, 2 and 3 shows the plots of audio after each step

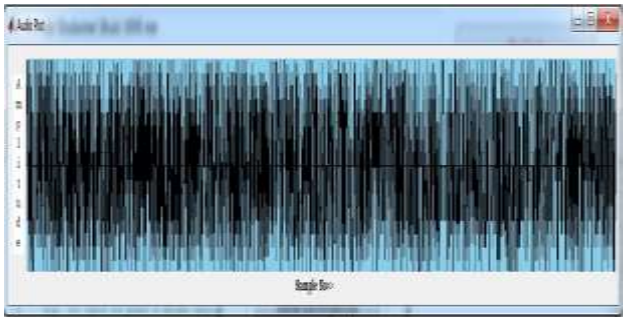

Figure1: Original Audio Signal

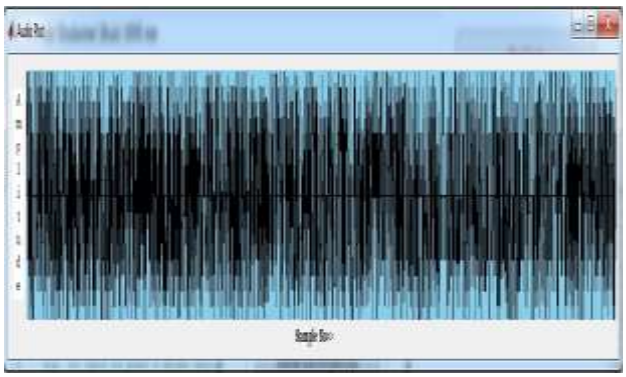

Figure2: Stago- Audio With hidden data

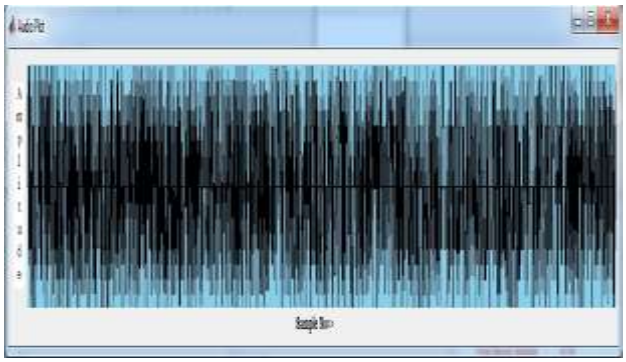

Figure3: Encrypted Stago Audio Signal

It becomes very difficult to distinguish in original audio and encrypted audio. As the security of this method depends on the algorithm used it becomes very difficult to reveal original data during transmission

IV. CONCLUSION

In a given paper an audio steganography is used in combination with encryption to provide a double layer of security. This method provides a double layer of security. The first level of security is achieved by data hiding using a steganography and second level is achieved by encryption method used.

REFERENCE:

1. 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.

2. M. Nutzinger, “Real Time attacks on Audio Steganography, ” Journal of Information Hiding and Multimedia Signal Processing, Vol. 3, No. 1, PP. 47-65, 2012.

3. S. M. Elshoura, 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.

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. Hemlata Kohad, Prof. V. R. Ingle, 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.

6. Tawfiq S. Barhoom, Zakaria M. Abusilmiyeh, “ A Novel Cryptography Method Based on Image for Key Generation,” Palestinian International Conference on Information and Communication Technology, 2013.

7. Vinit Agham, Tareek Pattewar ,” A Novel Approach Towards Separable ReversibleData Hiding Technique,” Internationai Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014.

8. Vinit Agham, Tareek Pattewar ,”Data Hiding Techniques by Using RGBLSB Mechanism ICICES - S.A.Engineering College, Chennai, Tamil Nadu, India,2014.

9. Ms. Megha B. Goel, ,Mr. M. S. Chaudhari, Mrs. Shweta A. Gode” A Review on Data Hiding using Steganography & Visual Cryptography,” © 2014 IJEDR | Volume 2, Issue 1 | ISSN: 2321-9939.

10. Sheetal A. Kulkarni, Shubhangi B. Patil,” A Robust Encryption Method for Speech Data Hiding in Digital Images for Optimized Security,” 2015 International Conference on Pervasive Computing (ICPC) ,2015.