ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 7, July 2014

A Practical Three Layered Approach of Data Hiding Using Audio Steganography

Nishu Gupta[1], Mrs.Shailja[2]

Student (M.Tech), CSE, CDLU, Sirsa, India[1]

Assistant Professor, CSE, CDLU, Sirsa, India[2]

Abstract: This paper is about the study of cryptographic and steganography techniques and provides the approach of security with the combination of these techniques .Security and confidentiality is a big challenge for computer users. This paper proposed the three layer approach for security of information which includes hashing (MD5), encryption and decryption algorithm (DES) and LSB techniques. LSB stands for least significant bit (LSB) coding is the simplest way to embed information in a digital audio file. Hashing for maintain the confidentiality of information, DES cryptographic algorithm has been used with Hashing algorithm. Audio steganography is a techniques used to transmit hidden information by modifying an audio signal is an imperceptions manner. This Paper provides a new way of securing the information to avoid hassle in transmission over network and implemented in MATLAB. The results show the security of workflow.

Keywords: Steganography, Cryptography, Hashing, Audio, LSB.

I. INTRODUCTION

Security of information is crucial part of any organization and it provides confidentiality and authentication as well. The information should be hidden from intruder and by steganography techniques, the confidential information can be communicated over the network. The encrypted information can retrieve by cryptanalysis attack but on the contrary side, the hiding information difficult to retrieve. Information security is essential for confidential data transfer. Steganography is one of the ways used for secure transmission of confidential information. Data hiding techniques have been widely used for transmission of hiding secret message for long time.

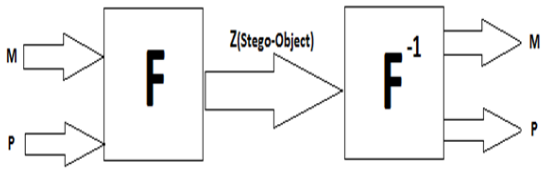

Fig 1 Steganography Scenario.

Steganography is an art and science of writing hidden message in such a way that no one apart from the intended recipient knows the existence of the message .In steganography, the message used to hide secret message is called host message or cover message. Once the content of the host message or cover message are modified the resultant message is known as stego message is known as stego message. Cryptography scrambles messages so it can't be understood. It defines the art and science of transforming data into a sequence of bits that appears as random and meaningless to a side observer or attackers. Cryptography is the study of methods of sending message in disguised from so that only the intended recipients can remove the disguise and read the messages. Audio steganography is the techniques of hiding data in audio files such as e.g. wav file. In computer –based audio steganography system, Secret messages are embedded in digital sound. The secret messages are embedded by slightly altering the binary sequence of a sound file. Existing audio steganography software can embed messages in WAV, AU and even MP3 sound.

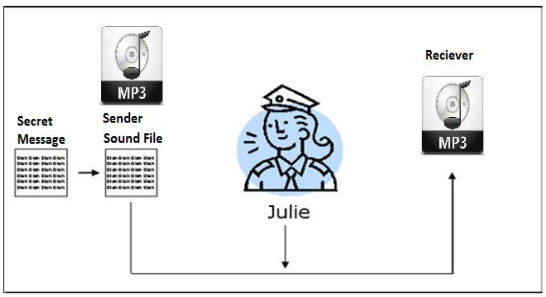

Fig 2 Secret message behind MP3.

II. LITERATURE REVIEW

In steganography, the possible cover carrier's are images, audio, video, text, or some other digitally representative code, which will hold the hidden information. A message can be information and it can be plaintext, hidden, image and it can be embedding in bit stream. Mutually, the wrap carrier and the embedded message create a stego-carrier. Hiding information may require a stego key which is additional secret information, such as a password, required for embedding the information [4].

In today's Research scenarios, there are many techniques, which have been discussed for security of the content. The data is converted in stegano-object, then communicated and on receiver side, this object is processed and retrieves the original information as described in the flowchart [5]. Author used two layers of security to secure the data. The Flow Diagram is described in which the data is to be decrypted, which has been embedded into the audio file. In next step, the Wave information and expected parameters is analyzed which includes the data-length, step-Size and frequency. Now, on receiver side, the de-steganography is

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 7, July 2014

need to be implement for extraction of cipher data and voice and this procedure will convert the cipher information in to original form [5]. The cryptography technique is for encryption and hiding of the information in any media file or plain file is Steganography [3]. There are LSB audio steganography technique and RSA Cryptographic algorithm. Steganalysis is the techniques for hide the information and recover the information from image. The probability of matching data with an image data is less and attacker not able to identify the correct data and difficult to implement Steganalysis technique and for more security, firstly encrypt and then hide in image [1]. The message hidden in the selected media is transmitted to recipient. At receiver end, reverse process is implemented to recover the original message. Author has described the different techniques for hiding the information [3].

The steganography algorithms tradeoffs are between the amount of covert information being embedded, called stego-data, and that the insurance for its presence to remain undetected. The recent advances allow more and more the use of advanced watermarking techniques to embed large amount of covert information that is also robust against removal and detection [4].

III. PROPOSED METHODOLOGY

The prime objective needs to be known initially before implement the techniques. The different layer data securing technique will be implemented. These layers will secure the content from intruders.

This technique will secure the confidential content over the network. A flowchart is a type of diagram that represents an algorithm, workflow or process, showing the steps as boxes of various kinds, and their order by connecting them with arrows.

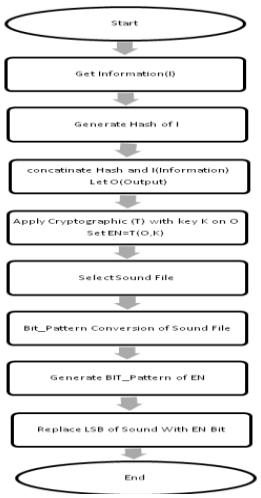

Fig 3 Flow Chart

These layers are (i) First layer will convert the data using Hashing algorithm (ii) The output of the first step will be encrypted using cryptography technique (iii) The outcome of these two layers will be embedded to Sound files (iv)These three layers will work fine from the sender side and sound file will be transmitted over the network.

IV. ALGORITHM

The number of steps has been analysed to secure the information. The DES cryptography and LSB steganography techniques has been implemented for encrypt, decrypt information and steganography for hiding of information. Along with this, the hashing method MD5 is used for confidentiality of information. The proposed approach has the multi-layers. The hash and message encrypted and then hide in audio files such as wav format. The Lease Significant bit (LSB) replaces the wav LSB with the encrypted Information. The advantage of these steps, the HAS (Human Auditory system) cannot identify the audio file information. The results have been generated using a MATLAB 7.11.0 version.

Table 1Proposed Algorithm

Get Confidential Information(I)
Let Hash Output S
Initialize Hash Algorithm-Denoted H
Generate Hash of I
For each Character(C_i) in I
$\sum_{i=0}^{lengt\,h(I)} S = H(Ci)$

If(Hash Successful) then
Let Output O
Concatenate Hash(S) and I(Confidential Information)
Set O =concatenate(S,I)//First Layer Completed
Cryptographic technique selection, Technique (T) and Key (K)
Let EN (Encrypted Information)
Set EN=Encrypt T(O from Step 9,K)//Second Layer Completed
Select Sound File (Let name is SO)
Repeat below Steps until Low-Bit Encoding Complete
Convert SO in Bit Pattern
Initialize of EN Bit Conversion
Let BS(Bit Sequence)
Set C Character in EN
For Each(C in EN)
$\sum_{i=0}^{lengt\,h(EN)} BS = Bit(Ci)$
If BS Completed Successfully then
Replace LSB (Step: 15) with BS Bytes//Third Layer Completed.
Else Move to Step 19.
Stop

In first Layer, the confidential information denoted as (I) will be taken as Input and the hash will be generated of the Information (I). For generate hash of (I), the every character will be taken from information (I) and the hash will be generated. After completion of this step, the hash will be concatenate with information (I) and this result will be encrypted by cryptographic technique and with key K for secure the resulted output. Furthermore, In Final Layer, The bit level manipulation to encode the message is shown in Figure. The following steps are

a. Receives the audio file in the form of bytes and converted in to bit pattern.
b. Each character in the message is converted in bit pattern.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 7, July 2014

c. Replaces the LSB bit from audio with LSB bit from character in the message.

V. RESULTS

The cryptography and steganography techniques has been implemented in the MATLAB tool with input of confidential information, Sound File, Image and hashing has been implemented for confidentiality of information in transmission. The graph has been shown of audio steganography shows that there is no loss in quality of sound and resulted sound file will be accurate in terms of memory. In first step, the hash has been generated of input text. The input text is nishu1. The hash will be generated and concatenated.

```
>> msg='nishu1';
%22 length max
hash = DataHash(msg);
subHash=hash(1:2); % add hash of length 2.
msg=strcat(msg,subHash);
%process 1st 8 bytes
msg1=msg(1:8);
str = reshape(dec2bin(double(msg1),8).',[],64)
input64 = str;

str =

0110111001101001011100110110100001110101001100010110001000110000
```

Fig 4 Binary Conversion of Concatenated Information and Hash

The concatenated result is nishu1b0. This layer1 has been completed. In the second layer, this information will be as input to the cryptographic technique which will generate the encrypted information. The information will be converted to binary and then, encrypts by the key. The resulted output will gives the sequence of bits.

0110111001101001011100110110100001110101001100010110001000110000

At this stage, the number of bits will be hidden in the audio wav file by LSB Technique by replacing the LSB of wav file with the resulted bits and HAS (Human Auditory System) will not be able to detect the wav file. The wav file before hide and after hide should remain same along with the properties of the wav. This can be visualized by comparing the wavforms of original and modified wav file.

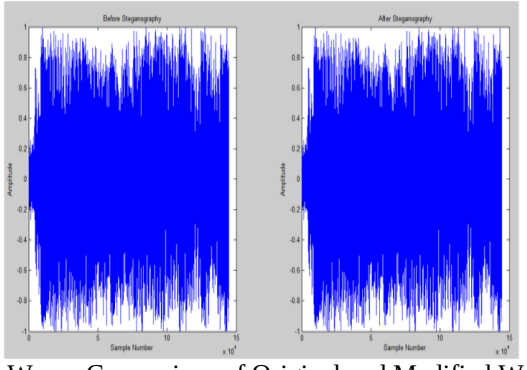

Fig 5 Waves Comparison of Original and Modified Wave

This figure depicts that the files being remain same after hiding of information and before hiding and it ensures that the wave forms has been altered with proper LSB technique.

VI. CONCLUSION AND FUTURE WORK

The data encryption and hiding of information is techniques for securing the information and can be communicated over the network. In this paper, we have presented an Audio Steganography concept for hiding the information in audio file such as mp3 or wav file. The Storage of secret information is a constant security concern, and the reliability and integrity of this information is important. The key idea of our proposed algorithm is to avoid embedding in a silent periods of host audio signal or any point that near from this silent periods due to sensitivity of Human Auditory System (HAS) for these periods so it will affect the perceptual transparency or noticeable perceptual distortion in a certain manner. In existing work, the hash was not used along with the cryptography and steganography concept. Hash generate is useful for check the confidentiality of information. This means, if the security breaches at single point, the hash comparison can give that information. The proposed work will compute the hash and then recreate the message using has and then cryptography algorithm will be used to encrypt the whole data, then LSB technique will hide the information in audio file. The hashing method is used for identification of confidentiality of information. The corruption of the secret data's host means the corruption of the secret data. This article proposed a simple application of threshold sharing and information hiding in mp3 audio files. The sound file will be modified and keep the information inside it. The experimental results show the accuracy of system and will be beneficial for organization. Finally high perceptual transparency is accomplished by LSB of host audio signal which are used for data hiding and method has improved the capacity and robustness of data hiding in the audio file.

In future, the depth of the Sound file can be improved by some methodology and techniques for hide the maximum data in audio files. The techniques should be feasible in such as way that the HAS (Human Auditory System) cannot detect the hidden information or any kind of information and SNR (Signal to Noise ratio) factor can be considered for measure the performance of methods.

REFERNCES

[1] Zaidoon Kh. AL-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan.O.Alanazi (2010)," Overview: Main Fundamentals for Steganography".

[2] Usha, S. (2011), "A secure triple level encryption method using cryptography and steganography", Computer Science and Network Technology (ICCSNT), 2011 International Conference, Page(s):1017 - 1020

[3] Djebbar, F. ; Ayad, B. ; Hamam, H. ; Abed-Meraim, K, "A view on latest audio steganography techniques", Innovations in Information Technology (IIT), 2011 International Conference on 2011 , Page(s): 409 - 414

[4] Nugraha, R.M., "Implementation of Direct Sequence Spread Spectrum steganography on audio data", Electrical Engineering and Informatics (ICEEI), 2011 International Conference 2011 , Page(s): 1 – 6

[5] Asad, M. ; Gilani, J., "Khalid, A, "An enhanced least significant bit modification technique for audio steganography", Computer Networks and Information Technology (ICCNIT), 2011 International Conference, 2011 , Page(s): 143 - 147
[6] Shahadi, H.I. ; Jidin, R., "High capacity and inaudibility audio steganography scheme Information Assurance and Security (IAS)", 2011 Page(s): 104 - 109
[7] Balgurgi, P.P. ; Jagtap, S.K., "Intelligent processing: An approach of audio steganography", Communication, Information & Computing Technology (ICCICT), 2012, Page(s): 1 – 6
[8] Kumar, H. ; Anuradha, "Enhanced LSB technique for audio steganography", Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference, 2012 , Page(s): 1 - 4
[9] Ankita Agarwal(2012)," Security Enhancement Scheme for Image Steganography using S-DES Technique".
[10] Sandeep Singh, Aman Singh(2013)," A Review on the Various Recent Steganography Techniques".
[11] Vipul Sharma, Sunny Kumar (2013), "A New Approach to Hide Text in Images Using Steganography".
[12] Ajit Singh, Swati Malik(2013), "Securing Data by Using Cryptography with Steganography".
[13] Jagbir Singh, Savina Bansal, R.K. Bansal (2013), "Performance Analysis of Data Hiding Using Adjacent Pixel Difference Technique".
[14] Sonam Pathak, Rachana kamble(2013), "A Review: Chaotic System with DES (Data Encryption Standard) Image Encryption Technique".
[15] Dr.K.Sathiyasekar, S.Karthick Swathy Krishna K S (2014), "A Research Review On Different Data Hiding Techniques".
[16] Krati vyas1, B.L.Pal2 (2014) , "A Proposed Method in Image Steganography to Improve Image Quality with LSB Technique", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 1.
[17] Roy, S. (2014), "Online payment system using steganography and visual cryptography", Electrical, Electronics and Computer Science (SCEECS), 2014 IEEE.

BIOGRAPHIES

Nishu Gupta pursuing her M.Tech in Computer Science from Choudhary Devi Lal University, Sirsa (Hry). She is presently the Student of Computer Science Branch. Her Research interest in Steganography and Hashing. She published the Research Papers in related steganographic techniques.

Mrs. Shailja kumari earned his M.Tech degree in Computer Science from Choudhary Devi Lal University (C.D.L.U), Sirsa (Hry). She is presently the assistant professor in C.D.L.U. Sirsa under C.S.A. deptt and having the experience of two years. Her research interest includes the DBMS and Computer Architecture.