International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 1 | Issue – 6

A Novel Approach: An Advanced Security Mechanism for Sending Messages using Steganography

R. Jayavadivel
Assistant Professor, Department of IT,Paavai Engineering College, Namakkal, Tamilnadu, India

B. Prabhushankar
Associate Professor, Department of IT, Paavai Engineering College, Namakkal, Tamilnadu, India

S.Rajesh
Associate Professor,Department of CSE, Paavai Engineering College, Namakkal, Tamilnadu, India

ABSTRACT

Steganography is the art of concealing information in ways that prevents the detection of hidden messages. Providing security for sending messages and confidential information via internet has been a challenging task for ages. Steganography provides a method to hide the data inside an image called cover object, while communication takes place between the sender and the receiver. Several techniques have been developed by the researchers to provide secured transmission of data. Hiding text messages inside an image using various methods in steganography is one of them. In this paper, we have proposed a new technique of file steganography and audio steganography. Here, the image and audio files are used as the carrier medium which adds another step in security. Only encrypted data is embedded in the image or audio file. Therefore, the intruders cannot access the original data from cover object as it will be available only in its encrypted form.

Keywords: *Cryptography, Steganography, LSB, Hash-LSB, RSA Encryption –Decryption, Low bit encoding*

I. INTRODUCTION

In today's information technology era, the internet has become an essential part for communication and information sharing. The number of data exchange has been increasing and therefore it is important to ensure the secure transmission of data between the sender and receiver.

Cryptography is a technique that deals with the science of coding and decoding secret messages, with the help of various encryption and decryption algorithms, integrity check functions and digital signature schemes.

Another technique called, Steganography that deals with the methods of hiding or covering secret and confidential data within other data or files.

The steganography can be used to hide objects such as:

a. Text
b. Image
c. Audio/video

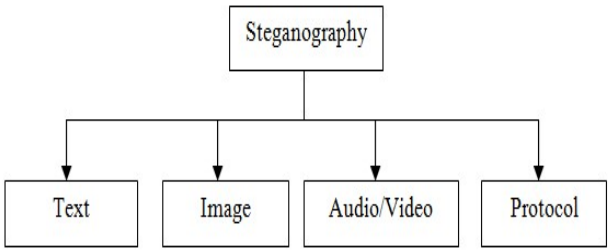

Figure 1: Steganography

Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display [6]. Because of this property, the alterations in the cover object is done

without damaging it and the embedded message will not be revealed easily. In this project, the image steganography and audio steganography are done with the help of LSB insertion and Low bit coding techniques respectively.

II. RELATED WORK

Several methods and techniques have been developed to hide text messages inside image files. For example: RSA algorithm and LSB insertion method can be used in embedding the messages inside an image. The most widely used technique to hide data is the usage of the LSB [1]. The existing techniques are mainly based on LSB (Least Significant Bit) where LSBs of the cover file are directly changed with message bits. In [3], two steganography techniqueshad been proposed for hiding image in an image using LSB method for 24 bit color images. Mohmmad A.Ahmed et al, in [2], proposed a method in which a message hidden inside an image by using the Least Significant Bit (LSB) technique and after creation of the hidden message, the image will pass it in hash function to obtain hashing value using the MD5 technique. In [4], [5], [7], [8] and [10], designing of robust and secure image steganography based on LSB insertion and RSA encryption technique has been used. In[6],Obaida Mohammad Awad Al-Hazaimeh, proposed that the inserting of message bits into the image is not only in the least bit but also the other bits in the pixel in the random manner. This can be done by comparing the message bit to the pixel bit randomly chosen from second to the last bit.

III. EXISTING TECHNIQUE USED

A. LSB Insertion Method

LSB insertion method is the simplest and the secure method used in steganography to embed message content inside a cover image. It embeds the bits of the message directly into least significant bit plane of the cover-image in a deterministic sequence. In this technique, the embedding capacity can be increased by using two or more least significant bits.

At the same time, not only the risk of making the embedded message statistically detectable increase but also the image fidelity degrades. The advantage of the LSB - based method is easy to implement and high message payload. And also, LSB hides the message in such way that the humans do not perceive the hidden content.

IV. PROPOSED TECHNIQUE

The Proposed system is intended to give an overview of image Steganography and Audio Steganography. It also attempts to identify the requirements of a good Steganography algorithm and briefly reflects on identifying which steganography techniques are more suitable for which applications.

A. Image Steganography

Hiding secret information using images is one of the most popular choices for Steganography. There have been many techniques for hiding information or messages in images in such a manner that alteration made in the image is perceptually indiscernible. Common approaches include LSB insertion method, Masking and filtering and Transform techniques.

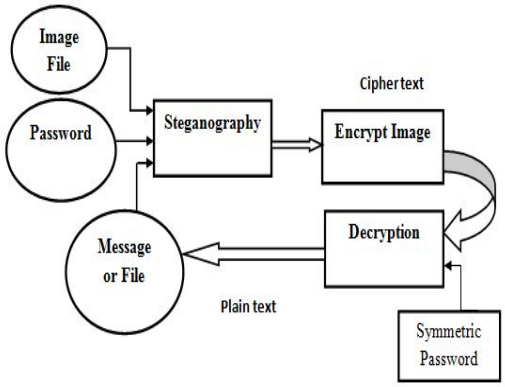

IMAGE STEGANOGRAPHY

Figure 2: Image Stegnography

B. Audio Steganography

Data hiding in audio signals is especially challenging, because the Human Auditory System (HAS) operates over a wide dynamic range. The HAS perceives over a range of power greater than one billion to one and a range of frequencies greater than a thousand to one. Sensitivity to additive random noise is also acute.
The perturbations in a sound file can be detected as low as one part in ten million which is 80dB below ambient level. However, there are some 'holes' available. While the HAS has a large dynamic range, it has a fairly small different range.

As a result, loud sounds tend to mask out the quieter sounds. Additionally, the HAS is unable to perceive absolute phase, only relative phase. Finally, there are some environmental distortions as common as to be

ignored by the listener in most cases.

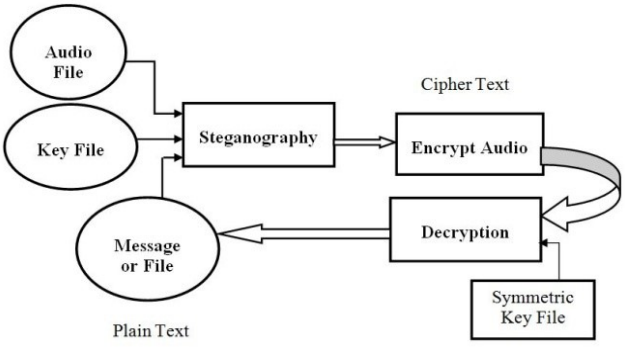

Figure 3: Audio Stegnography

C. Low Bit Encoding

Low-bit encoding is the one of the simplest way to embed data into other data structures. By replacing the least significant bit of each sampling point by a coded binary string, it can encode a large amount of data in an audio signal. Sampling technique followed by Quantization converts analog audio signal to a digital binary sequence. In this technique LSB of binary sequences of each sample of digitized audio file is replaced with the binary equivalent of a secret message.

V. IMPLEMENTATION AND REPORT ANALYSIS

The File Stegano module is used to hide files into the image no one can see that file. It has two options encrypt and decrypt. First select encrypt tab, the application gives the screen to select the image file, information file and option to save the image file. For encryption LSB bit are used to write our security information inside image. So use the last layer (8st layer) of information, change the last bit of pixels. In other hands 3 bits in each pixel, so 3*high*width bits memory to write our information. But before writing our data write name of the data (file), size of name of data & size of data, by assigning some first bits of memory (8st layer) using each 3 pixels of picture to save a byte of data.

The decrypt is used to get the hidden information in an image file. It takes the image file as an output, and give two files at destination folder, one is the same image file and another is the message file that is hidden it that. If the user selects decrypt, the application gives the screen to select only image file and ask path where user want to save the secrete file. Before encrypting file inside image must to save the name and size of files in a definite place of the image. Save file name before file information in LSB layer and save file size and file name, size in most right-down pixels of the image. Writing this information is needed to retrieve files from an encrypted image in decryption state.

Original image

Stego image

An audio format is a medium for storing sound and music. It is a container format for storing audio data on a computer system. There are numerous file formats for storing audio files. WAV is a flexible file format designed to store more or less any combination of sampling rates or bit rates. This makes it an adequate file format for storing and archiving an original recording**.**

In audio Stegano module, during encryption, the first step is selecting an input audio file. The selection is made through opening a new dialog box and the path selected is displayed through a textbox. The second step is selecting a key file. The third step is choosing a text file or typing any text message for embedding. In the fourth step, whatever the files that selected are viewed and verification of the path is done. In the fifth process data is embedded into the audio file using low bit encoding technique. After embedding the content, both the audio files are played and a listener cannot find any difference between the audios.

In decryption, the first step is the process of selecting the encrypted audio file. This is the file that a user has to extract information from the output audio. The

symmetric encryption method is used here, so the key selected during the embedding process is used in decrypting the message. Second process involved in selecting a new text file to display the embedded message. All the process done embedded message are displayed on a list box and finally the embedded message can be viewed with the help of a file or in a textbox.

CONCLUSION

In this paper, new Steganographic systems are proposed to enhance the security of Steganographic system by using both the image and audio as carrier medium to hide the contents. Thus, we expect that the proposed technique will be efficiently used in Steganographic systems or considered as a good alternative to other technique because of the high level of security.

REFERENCES

1) ien Hong, Tung-Shou Chen, "A Novel Data Embedding Method Using Adaptive Pixel Pair Matching", IEEE Transactions on Information Forensics and Security, Vol. 7, Issue No. 1, Pages No. 176 - 184, Feb., 2012.

2) Mohammad A. Ahmad, Dr. ImadAlshaikhli, Sondos O. Alhussainan, "Achieving Security for Images by LSB and MD5", Journal of Advanced Computer Science and Technology Research, Vol. 2, Issue No.3, Pages No. 127-139, Sept., 2012.

3) DeepeshRawat, VijayaBhandari, "ASteganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image", International Journal of Computer Applications, Vol. 64, Issue No. 20, Feb., 2013.

4) MamtaJuneja, Parvinder Singh Sandhu, "Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption", International Conference on Advances in Recent Technologies in Communication and Computing, Pages No. 302 – 305, 27-28 Oct., 2009.

5) Swati Tiwari, R. P. Mahajan, "A Secure Image Based Steganographic Model Using RSA Algorithm and LSB Insertion", International Journal of Electronics Communication and Computer Engineering (IJECCE), Vol. 3, Issue No. 1, 2012.

6) Obaida Mohammad Awad Al-Hazaimeh, "Hiding Data in Images Using New Random Technique", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue No. 4, No 2, July 2012.

7) Samir Kumar Bandyopadhyay, SarthakParui, "A Method for Public Key Method of Steganography", International Journal of Computer Applications, Vol. 6, Issue No. 3, Sept., 2010.

8) Shailender Gupta, AnkurGoyal, Bharat Bhushan, "Information Hiding Using Least Significant Bit Steganography and Cryptography", I. J. Modern Education and Computer Science, Vol. 6, Pages No. 27-34, 2012.

9) Anil Kumar *, Rohini Sharma, "A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique",International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, July 2013.

10) Deepali, "Steganography with Data Integrity", International Journal of Computational Engineering Research, Vol. 2, Issue No. 7, 2012.