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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015.

Three Layer Protection for Secure Data Transmission using Digital Audio as Carrier

Parul[1], Mr. Vikas Kamra[2]

Student, CSE, JCDM College of Engineering, Sirsa, India[1]

Assistant Professor, CSE, JCDM College of Engineering, Sirsa, India[2]

Abstract: Today In Business Domain, the information is substantial part of enterprise. The data and information present need to be confidential and secure. Secrecy is an essential aspect. So, that no obtruder being able to disturb the information. From the security perspective, the information should not be readable by intruder. The cryptography technique can convert the plain text to encrypted text. The target of steganography is to hide a confidential message within a cover-media in such a way that others cannot discern the presence of the hidden message In this paper, Data will be hidden using Three layers in Audio. Goal of this work is to increase level of security so that data can be gaurded.

Keywords: WAV (Waveform audio file format), HASH, Hidden message

I. INTRODUCTION

The rising rate of usage of internet changed the overall scenario of intercommunication. People are now able to displace large interactive media files through broadband connection. The communication is almost precise. Security is a major factor in the communication system. Data hiding is a approach of providing security to data. Armed forces, intelligence agencies and also in field of spying inconspicuous communication is required.

Steganography is the method of unobservable communication.

This is practiced through hiding data in other data. In Steganography, we use carriers to conceal the data. The carriers may be image, audio, text, video, etc. The confidential information is reserved in some carrier and then transported. The message in steganography is of two types – one is Envelop and other is confidential message .The envelop is used as carrier which envelops the message to be send. .The confidential message is wrapped inside the envelope. Steganography can be applied in numerous regions:

1. Validation: The process of justifying the oneness
2. Solitude: This confirms message reached to accurate receiver.
3. Integrity: This confirms message will not be modified in anyway.
4. Non-repudiation. : It proves that message is authentic .
Wrapping data in audio is much more laborious than wrapping the data in other media. In audio steganography we can wrap messages in WAV, AU, and even MP3 sound files. Encapsulating the data in audio is very efficient technique for safeness of message. In this we are using Audio as a carrier to provide security to data. Steganalysis is a procedure of tracking down the unrevealed messages which have been made private by steganography. Steganalysis generally starts with uncertain data but more knowledge is needed to find out the secret

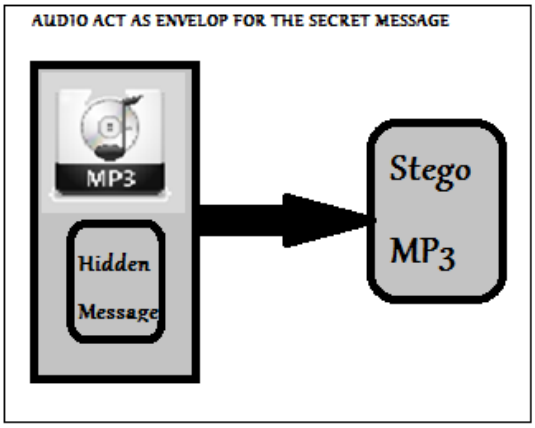

Figure 1 Data Encapsulation in Audio

II. LITERATURE REVIEW

Rohit Tanwar, Bhasker Sharmaand Sona Malhotra proposed a robust substitution technique to implement audio steganography the technique resolves the various inherent problems in using traditional substitution techniques. It improves the data hiding capacity while being robust to various intentional as well as unintentional attacks. [6]

Ms. Nidhi Sharma and NehaGupta introduce a system which aims at providing improved robustness, security by using the concept of DWT (Discrete Wavelet Transform) and LSB (Least Significant Bit) proposed a new method of Audio Steganography. The emphasize will be on the proposed scheme of image hiding in audio and its comparison with simple Least Significant Bit insertion method for data hiding in audio.[1]

Huynh Ba Dieu and Nguyen Xuan Huy present an improved technique for hiding data in audio. The method modifies the amplitude of the cover audio file to embed the secret message. To increase the security of the proposed scheme, we use a key to adjust the hiding

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015.

technique. The suggested scheme does not need the original signal for extracting the hidden bits.[5]

Balgurgi, P.P., Jagtap, S.K., According to us audio steganography is to obtain robust high capacity steganographic systems. We provide implementation of two level encryption of user data by combining two areas of network security, cryptography and steganography. The combination of LSB technique with XORing method is described in this paper, which gives additional level of security. Varieties of techniques for embedding information in digital audio have been established. They attend the general principles of hiding secret information using audio technology, and an overview of functions and techniques.[4]

Arvind Kumar Km. Pooja proposed that steganography serves as a better way of securing message than cryptography which only conceals the content of the message not the existence of the message. Original message is being hidden within a carrier such that the changes so occurred in the carrier are not observable. In this paper we will discuss how digital images can be used as a carrier to hide messages. This paper also analyses the performance of some of the steganography tools. Steganography is a useful tool that allows covert transmission of information over an over the communications channel. Combining secret image with the carrier image gives the hidden image. The hidden image is difficult to detect without retrieval. [10]

Chang-Chou Lin, Wen-Hsiang Tsai States that A secret image is first processed into n shares which are then hidden in n user-selected camouflage images. It is suggested to select these camouflage images to contain well-known contents, like famous character images, well-known scene pictures, etc., to increase the steganographic effect for the security protection purpose. Furthermore, an image watermarking technique is employed to embed fragile watermark signals into the camouflage images by the use of parity-bit checking, thus providing the capability of authenticating the fidelity of each processed camouflage image, called a stego-image. During the secret image recovery process, each stego-image brought by a participant is first verified for its fidelity by checking the consistency of the parity conditions found in the image pixels. The recovery process is stopped if any abnormal stego-image is found.

Otherwise, the secret image is recovered from k or more authenticated stego-images. Some effective techniques for handling large images as well as for enhancing security protection are employed, including pixel wise processing of the secret image in secret sharing, use of parts of camouflage images as share components, adoption of prime-number modular arithmetic, truncation of large image pixel values, randomization of parity check policies, etc. They proposed scheme has three levels of security protection. First, the threshold function is adopted for a group of n participants to share the secret. Only k or more out of the n shares are collected can the original image data be recovered. Then, the concept of data hiding is employed to embed the shares into camouflage images before delivering the shares to the participants. Finally, the proposed scheme is equipped with the capability of authentication, which can detect false participants' shares before the recovery process is executed. Furthermore, the proposed scheme can also handle full color images, and the quality of the recovery result is nearly lossless. This system is thus suitable for the applications where high security and efficiency is required.[20]

III. OBJECTIVES

In contrast to Cryptography, where the informer is allowed to disclose, reveal, obstruct and to reform messages without being able to defy certain safeguard premises guaranteed by a cryptosystem, the target of Steganography is to obscure messages inside other innocuous messages in a way that does not allow any enemy to even detect that there is a second message present. Steganography can be used in a large amount of data configuration in the digital world of today. The most popular data configurations used are .bmp, .doc, .gif, .jpeg, .mp3, .txt and .wav.

1. Problem Statement

Steganography is now becoming considerable area to study. As the demand of safe and secure intercommunication boost up .The need of concealment in secret information is growing. If a user wants to send the discreet information to other persons with security and privacy he can send it by using image steganography. During the last few years lot of different methods of concealing information has been done in this field. Some of the existing methods for hiding information give good results only in case of information get hidden successfully. LSB is the most popular Steganography technique. It hides the secret message in the media file based on it its binary coding. LSB algorithm is used to hide the confidential messages by using algorithm.

LSB changes the quality which clears as well as it is easy to attack. It is clear that LSB changes the media when the least significant bits add in the binary format, so that media quality become burst and there become so much difference in the original media and encoded media in the respect of quality. In two layer security, the data is not much secure because cipher text can be decrypt from the encrypted text by using the cryptanalysis technique. In network scenario, safegaurd of data and transmission of data is main aspect which cannot be taken care by just encryption and stegano techniques and it is critical because information can be revealed or exposed.

2. Objective

The main objective is to provide three layer security to data. The three layers will secure the content from intruders. This technique will secure the confidential content over the network. To make the data more safe and private the three layers would b provided. So the main objectives are:

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015.

1. Gaurd the content from snoopers
2. To obscure messages inside other innocuous messages in a way that does not allow any enemy to even detect that there is a second message present.
3. Make the data extra secure and private

IV. PROPOSED METHODOLOGY

The three layer data security is provided to data using digital audio as carrier. The three layers will secure the content from intruders. This technique will secure the confidential content over the network. These layers are described as:

1. First layer: First layer will convert the data using hashing algorithm.

2. Second layer: The output of the first step will be encrypted using cryptography technique

3. Third layer: The outcome of these two layers will be embedded to Sound files.

4. These three layers will work fine from the sender side and sound file will be transmitted over the network

Various Techniques used in proposed methodology

1. Secret Key Cryptography

With secret key cryptography, a single key is used for both encryption and decryption.

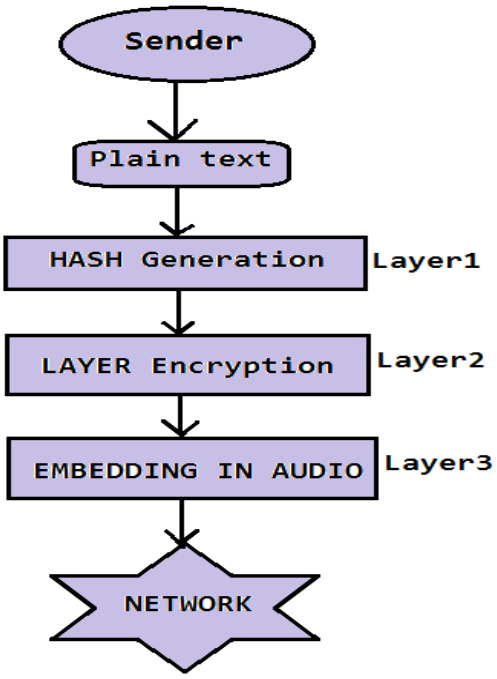

Figure 2 Three layered model

The sender uses the key to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the carbon key to decrypt the message. As a single identical key is used for both functions, secret key cryptography is also called symmetric encryption.

2. Public Key Encryption

In Public Key Cryptograohy, one of the keys is beptised as public key. The other key is beptised as the private key and is never disclosed to other party. The messages are plain –dealed under this scenario.

3. Hash Functions

Hash functions, also called message digests and one-way encryption. These are the algorithms that, in some sense, use no key. Instead, a fixed-length hash value is computed based upon the plaintext that makes it infeasible for either the contents or length of the plaintext to be recovered. Hash algorithms are typically used to provide a digital fingerprint of a file's contents often used to ensure that the file has not been reshaped by an intruder or virus. Hash functions, also provide a measure of the integrity of a file.

V. CONCLUSION AND FUTURE WORK

In this paper three level scheme is proposed for hiding data in audio. This scheme helps to increase the level of security of data. For this purpose hash function is generated and layer encryption is used.

The conventional LSB modification techniques used are prone to steganalysis. A new three layered model for audio steganography is presented in this paper. On the sender side, the first layer maps characters of the secret message to bits.

The compression provided by this layer increases capacity. The second layer applies encryption to secret message bits, thus changing representation of the secret message. The change in representation increases robustness, but the transmission of key decreases capacity. However, the decrease in capacity becomes negligible for longer secret messages. The third layer samples the cover message, embeds the secret message in it and transmits the resultant stego message over the network to the receiver. The third layer increases transparency and robustness, but decreases capacity which can be easily overcome by advance broadband networks. The receiver retrieves the stego message from the network and passes it through all three layers but in reverse order with each layer performing reverse operations. At the end, the same secret message is available to the receiver

REFERNCES

[1] Ms. Nidhi Sharma and NehaGupta "Dwt and Lsb Based Audio Steganography", International Conference on Reliability, Optimization and Information Technology - ICROIT, 2014
[2] Andreas Westfeld "A Steganographic Algorithm High Capacity Despite Better Steganalysis", 2001
[3] Kevin Curran "An Evaluation of Image Based Steganography Methods", 2003
[4] Balgurgi, P.P., Jagtap, S.K., "Intelligent processing: An approach of audio steganography", Communication, Information & Computing Technology (ICCICT), 2012
[5] Huynh Ba Dieu Nguyen Xuan Huy "An Improved Technique for Hiding Data in Audio", IEEE, 2014
[6] Rohit Tanwar Bhasker Sharma Sona Malhotra" A Robust Substitution Technique to implement Audio Steganography ",International Conference on Reliability, Optimization and Information Technology, 2014
[7] Delforouzi, A.; Pooyan, M., "Adaptive Digital Audio Steganography Based on Integer Wavelet Transform", Intelligent Information Hiding and Multimedia Signal Processing. IIHMSP, 2007.
[8] Pooyan, M.; Delforouzi, A., "LSB-based Audio Steganography Method Based on Lifting Wavelet Transform", Signal Processing and Information Technology, 2007

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015.

[9] Shah, P.; Choudhari, P.; Sivaraman, S., "Adaptive Wavelet Packet Based Audio Steganography using Data History", Industrial and Information Systems, 2008, ICIIS 2008, IEEE, 2008
[10] Arvind Kumar, Km. Pooja "Steganography- A Data Hiding Technique," 2010
[11] Gopalan, K., Qidong Shi "Audio Steganography Using Bit Modification - A Tradeoff on Perceptibility and Data Robustness for Large Payload Audio Embedding", Computer communications and Networks (ICCCN), 2010
[12] Sujay Narayana and Gaurav Prasad" Two New Approaches for Secured Image Steganography Using Cryptographic Techniques and Type Conversions", 2010
[13] Hamid.A.Jalab, A.A.Zaidan, B.B.Zaidan "New Design for Information Hiding with in Steganography Using Distortion Techniques", 2010
[14] Zaidoon Kh. AL-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan.O.Alanazi" Overview: Main Fundamentals for Steganography", 2010
[15] Usha, S. "A secure triple level encryption method using cryptography and steganography", Computer Science and Network Technology (ICCSNT), 2011
[16] Djebbar, F.; Ayad, B.; Hamam, H.; Abed-Meraim, K "A view on latest audio steganography techniques", Innovations in Information Technology (IIT), 2011
[17] Nugraha, R.M. "Implementation of Direct Sequence Spread Spectrum steganography on audio data", Electrical Engineering and Informatics (ICEEI), 2011
[18] Asad, M., Gilan, J., "Khalid, A, "An enhanced least significant bit modification technique for audio steganography", Computer Networks and Information Technology (ICCNIT), 2011
[19] Shahadi, H.I., Jidin, R., "High capacity and inaudibility audio steganography scheme Information Assurance and Security (IAS)", 2011
[20] Chang-Chou Lin, Wen-Hsiang Tsai" Secret image sharing with steganography and authentication", 2004