IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

Hop-to-Hop Secure Data Transmission using Cryptography and Audio Steganography Algorithm

V. Vetri Selvi[1], S. Gayathri[2]

Assistant Professor, Department of MCA, Shrimati Indra Gandhi College, Trichy, India[1]

Research Scholar, Department of Computer Science, Shrimati Indra Gandhi College, Trichy, India[2]

Abstract: Today's large demand of internet applications requires data to be transmitted in a secure manner. Data transmission in public communication system is not secure because of interception and improper manipulation by eavesdropper. In this thesis we implement two security algorithms they are cryptography and steganography. For secure communication we are providing security by using the RSA which is based on Cryptography. Steganography is an art of sending hidden data or secret messages over a public channel so that a third party cannot detect the presence of the secret messages. Audio signals have a characteristic redundancy and unpredictable nature that make them ideal to be used as a cover to hide secret information. A Steganographic technique for embedding text information in audio using LSB based algorithm is presented in this paper. In the proposed method each audio sample is converted into bits and then the text data is embedded. In embedding process, first the message character is converted into its equivalent binary. By using proposed LSB based algorithm, the capacity of stego system to hide the text increases. The performance of the proposed algorithm is computed using SNR values for various audio input. By using these methods third parties cannot percept the existence of message embedded in the audio file. The properties of the audio file remain the same after hiding the secret message.

Keywords: Cryptography, steganography, LSB, RSA.

I. INTRODUCTION

Nowadays it is possible to extract hidden data by applying certain techniques like Multicarrier Spread-Spectrum Embedding. Also encrypted data can be compromised by applying certain techniques like Brute Force Attack. Hence it is necessary to bring up a significant solution for data transfer. We suggest the combining approach of data encryption and data hiding can be a better solution for such cases. The data hiding and data encryption comes under the concept of steganography and cryptography respectively. It is a technique of hiding information. It is possible to hide necessary information by applying the steganography approach without causing any affect to the information. Once the information is hidden, it cannot be identified easily. It is a technique of converting plain text into cipher text. It is possible to encrypt highly secure data by applying cryptography approach. This approach helps to convert data in such a way that it can't be understood. Only the authorised user can decrypt the encrypted data. There might be possibility that the highly confidential information that we are transferring may be compromised by the hackers or by unauthorized users. Hence it is necessary to find an appropriate solution for such situations. Till so far, such kind of situations has been negotiated by applying the concept of data hiding and data encryption separately.

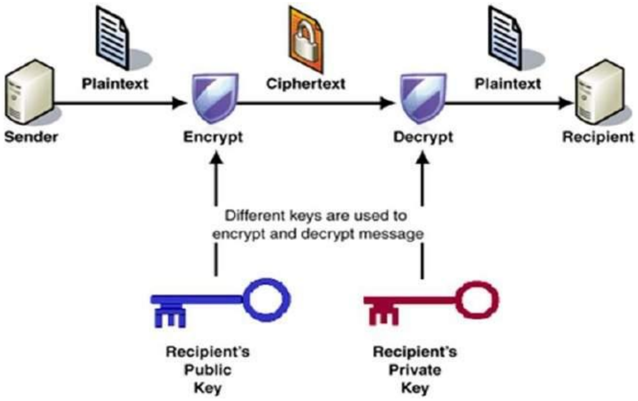
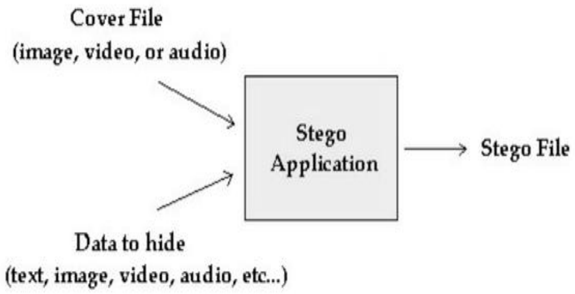
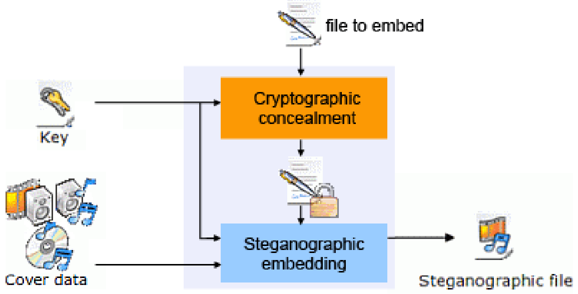


Fig. 1 Cryptography Working Process

DOI10.17148/IJARCCE.2017.6693



Hiding of highly secure data during transfer provides security and privacy up to an extent whereas encryption of highly confidential data provides a better option.
Cryptography's main aspect is that the information is somehow distorted, scrambled by the sender using normally an encryption key also known only by the intended receiver who decrypts the message. The problem with cryptography is that a user intercepting the message, although he cannot decrypt it, he might detect that there is encrypted, secret information. Audio steganography is one of the popular data hiding techniques that embeds secret data in audio signals .On the other hand in steganography. The secret data is hidden in a way that unauthorized persons are not aware of the existence of the embedded data and without altering the quality of the cover audio. In addition, the security of classical steganography system relies on secrecy of the data encoding system. Once the encoding system is known, the steganography system is defeated.



II. PROPOSED METHOD

A system that can be built by considering steganography and cryptography approach . The proposed system will accept the information as an input (txt file). This information (txt file) will be then encrypted by an approach of cryptography i.e. RSA algorithm. Once the encryption is done, then the data can be made ready to hide behind an audio file format by applying steganography approach. This way it will be a safe option to send this audio file over network without worrying for the hidden information. This way sender may feel quality trust on his data sharing aspect.

III. LITERATURE REVIEW

[1]. Debnath Bhattacharyya, Poulami Das, Samir Kumar Bandyopadhyay, and Tai-hoop Kim, "Text Steganography: A Novel Approach", This paper presents an approach for text steganography through a technique that uses reflection symmetry of the English alphabets. To hide secret data bits, the proposed method checks the vertical and horizontal reflection symmetry properties of the characters present in each sentence of the text and, if followed, it selects the sentence to generate a summary of the text, known as cover text or stego- text. [2]. Ming Li, Michel Kulhandjian, Dimitris A. Pados, Stella N. Batalama and Michael J. Medley, "Extracting Spread-Spectrum Hidden Data from Digital Media", We develop a novel multi-carrier/signature iterative generalized least-squares (M-IGLS) core procedure to seek unknown data hidden in hosts via multi-carrier spread spectrum embedding. Neither the original host nor the embedding carriers are assumed available. [3] Akansha Tuteja and AmitShrivastava, " Faster Decryption and More Secure RSA Cryptosystem", This paper proposed four time faster RSA-CRT algorithm for decryption of data and effective representation of encryption using Chinese Remainder Theorem (CRT) for the data security. The algorithm is implemented in Java source code. [4] Tanmaiy G. Verma, ZohaibHasan and Dr.GirishVerma, "A Unique Approach for Data Hiding Using Audio Steganography", Steganography and Cryptography are considered as one of the techniques which are used to protect the important information, but both techniques have their pro's and con's. This paper aims to conquer their respective drawbacks and to achieve this we are using a double layer protection technique which is cryptography cum steganography approach. [5] Arvind Kumar and Km. Pooja, "Steganography- A Data Hiding

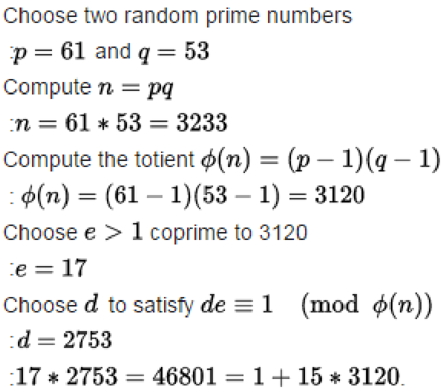
DOI10.17148/IJARCCE.2017.6693

Technique", Steganography is a form of data hiding technique that provides mechanism for securing data over insecure channel by concealing information within information. It is based on invisible communication and this technique strives to hide the very existence of the secret message from the observer. As a result it is very commonly used by Intelligence Agencies for securely broadcasting and communicating information over the internet by hiding secret information inside images and text. Imperceptibility, robustness and capacity of the hidden data are the main characteristics of steganography.

IV. ALGORITHM

A. RSA Algorithm

RSA algorithm was designed by Ron Rivest, Adi Shamir and Leonard Adleman. This algorithm was specially designed for encryption of data. RSA algorithm is one of the technique use to implement cryptography. RSA algorithm is based on public key cryptography. It generates public and private key. Public key is used for encryption purpose and private key is used for decryption purpose. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of them can be given to everyone. The other key must be kept private. RSA involves a public key and private key. The public key can be known to everyone; it is used to encrypt messages. Messages encrypted using the public key can only be decrypted with the private key. The keys for the RSA algorithm are generated the following way:



Choose two random prime numbers

:$p = 61$ and $q = 53$

Compute $n = pq$

:$n = 61 * 53 = 3233$

Compute the totient $\phi(n) = (p-1)(q-1)$

: $\phi(n) = (61-1)(53-1) = 3120$

Choose $e > 1$ coprime to 3120

:$e = 17$

Choose d to satisfy $de \equiv 1 \pmod{\phi(n)}$

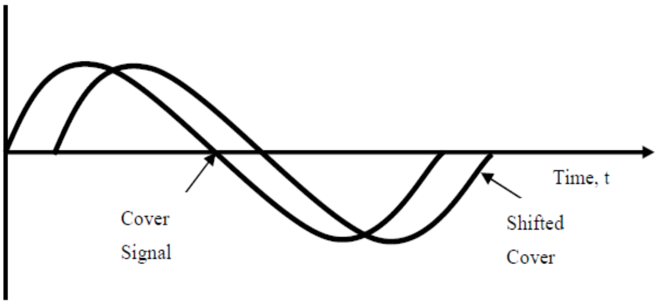
:$d = 2753$

:$17 * 2753 = 46801 = 1 + 15 * 3120$.

B. Audio Stenography Technique

To provide more security the original data file is encrypted first before embedding. And second purpose of this system is to increase robustness in case of security. In this system we initially encrypt the message using asymmetric public key algorithm (RSA) and then encrypted message bits are inserted at random higher LSB layer position of the host audio. We have original audio sample and inserting message bit in different LSB layer positions we get some new samples. Sometimes it can happen that for more than one LSB layer we get the same difference between original audio sample and new audio samples. In this case we will choose the higher LSB layer.

Least significant bit (LSB) coding is the simple, fast and popular methodology to embed information in a digital audio file. In this technique, LSB of binary sequences of each sample of digitized audio file is replaced with binary equivalent of secret message. LSB coding permits for a huge amount of data to be encoded by replacing the least significant bit (LSB) of each sampling point with a binary information. Data transmission rate In LSB coding is 1 kbps per kHz. In some of LSB coding implementations, two LSB of a sample are substituted with two information bits. It increases the quantity of data which can be encoded but it also increases the quantity of resulting noise in the audio file.



DOI10.17148/IJARCCE.2017.6693

To extract a secret information from an LSB encoded audio file (stego object), the receiver requires access to the sequence of sample which used in the embedding process. Usually, the length of the secret information to be encoded is slighter than the total number of samples in an audio file.

V. CONCLUSION

Both steganography and cryptography has certain limitations, yet these are the most familiar aspects of security and privacy. Either steganography or cryptography cannot provide maximum trust towards security separately. The combination of steganography and cryptography forming a double layer protection approach can yield better secure solution for information sharing. This way a comprehensive approach can be suggested that works on a combined approach that first encrypts the highly secure data and then hides it behind audio. This suggested approach can provide an advanced level of security and privacy to the confidential information over network.

VI. FUTURE ENHANCEMENTS

It focuses on hiding the existence of messages. The term hiding means making the information invisible during data transfer. The Steganography algorithms can be used to hide data behind digital media such as audio, video or images. As we are using digital media increasingly, drastic research in audio steganography has already started. In a computer based system, secret messages are hidden in digital sound, using audio file as a cover object. In audio steganography, the weakness of the human auditory system is used to hide information in the audio.

REFERENCES

[1]. Debnath Bhattacharyya, Poulami Das, Samir Kumar Bandyopadhyay, and Tai-hoon Kim, “Text Steganography: A Novel Approach”, International Journal of Advanced Science and Technology Vol. 3, February, 2009.
[2]. Ming Li, Michel Kulhandjian, Dimitris A. Pados, Stella N. Batalama and Michael J. Medley, “Extracting Spread-Spectrum Hidden Data from Digital Media”.
[3]. AkanshaTuteja and Amit Shrivastava, “Faster Decryption and More Secure RSA Cryptosystem”.
[4]. Tanmaiy G. Verma, ZohaibHasan and Dr.Girish Verma, “A Unique Approach for Data Hiding Using Audio Steganography”.
[5]. Arvind Kumar and Km. Pooja, “Steganography- A Data Hiding Technique”.
[6]. Simon Singh, “The Code Book” (2001, Shinchosha).
[7]. Nentawe Y. Goshwe, “Data Encryption and Decryption Using RSA Algorithm in a Network Environment”.

DOI10.17148/IJARCCE.2017.6693