Research article Available online www.ijsrr.org ISSN: 2279–0543

International Journal of Scientific Research and Reviews

Securing Text Message Using Audio Steganography AndCryptography

Rasmi M

Dept. of Computer Science and Applications, St. Mary's College, Thrissur-20
Email: m.rasmi.m@gmail.com

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. So the attractive solution for this problem is Steganography and Cryptography. Steganography hides secret information into a cover medium and Cryptography convert data into an unrecognizable form. The proposed algorithm is an amalgamation of text encryption, audio steganography and audio encryption. The original text message is encrypted using RSA algorithm. This cipher text gets embedded into the cover audio using LSB encoding. This scrambled audio is transmitted to the receiver which carries the encrypted secret data. Audio steganography is scheme of hiding the existence of secret information by concealing it into another medium such as audio file. It will give more protection to the data.

***Corresponding author**

Rasmi M

Assistant Professor,

Dept. of Computer Science and Applications,

St. Mary's College, Thrissur-20

Email: m.rasmi.m@gmail.com

I. INTRODUCTION

The network security is becoming more important as the volume of data being exchanged over the internet increases day by day[1].Two important techniques for providing security are:

STEGANOGRAPHY

Asthe need of security increases only encryption is notenough. So stegnograpghy is the supplementary to encryption. It is not the replacement of encryption. But Steganography along with encryption gives more security to data. The word steganography is of Greek origin and means "concealed writing" from the Greek words stegnos meaning "covered or protected", and graphei meaning "writing". Steganography is the technique to hide the information in some media so that third party can't recognize that information is hidden into the cover media. That media may be text, image, audio or video. The information that to be hidden is called stego and the media in whichthe information is hidden is called host. The stego object can be text, image, audio or video. When the informationis hidden into the audio then it is called Audio steganography[2].

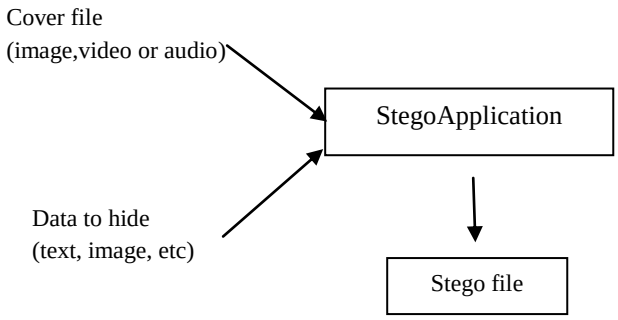

Fig 1: Steganography

USES OF STEGANOGRAPHY

1. Steganography can be a solution which makes it possible to send news and information without being censored and without the fear of the messages being intercepted and traced back to us.
2. It is also possible to simply use steganography to store information on a location. For example, several information sources like our private banking information, some military secrets, can be stored in a cover source. When we are required to unhide the secret information in our cover source, we can easily reveal our banking data and it will be impossible to prove the existence of the military secrets inside[3].
3. The transportation of sensitive data is another key use ofsteganography. A potential problem with cryptography is that eavesdroppers know they have an encrypted message when they see one. Steganography allows to transport of sensitive data past eavesdroppers without them

knowing any sensitive data has passed them. The idea of using steganography in data transportation can be applied to just about any data transportation method, from e-mail to images on internet websites.

4. E-commerce allows for an interesting use of steganography. Incurrent e-commerce transactions, most users are protected by ausername and password, with no real method of verifying that theuser is the actual card holder. Biometric finger print scanning,combined with unique session IDs embedded into the fingerprint images via steganography, allow for a very secure option to open ecommerce transaction verification[4].

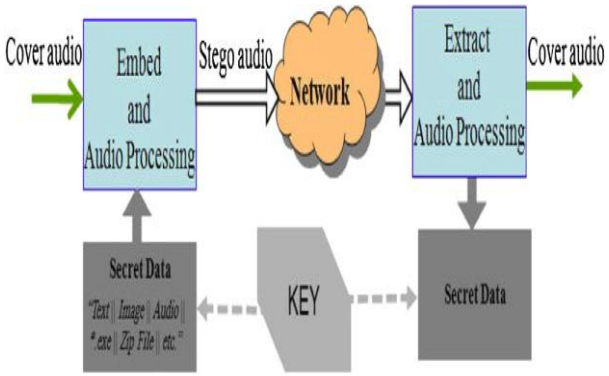

Fig 2: Audio Steganography

II. IMPLEMENTATION

RSA ALGORITHM

RSA is an Internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is the most commonly used encryption and authentication algorithm and is included as part of the Web browsers from Microsoft and Netscape. It's also part of Lotus Notes, Intuit's Quicken, and many other products. The encryption system is owned by RSA security[5]. The mathematical details of the algorithm used in obtaining the public and private keys are available at the RSA Website. Briefly, the algorithm involves multiplying two large prime numbers (a prime number is a number divisible only by that number and 1) and through additional operations deriving a set of two numbers that constitutes the public key and another set that is the private key.

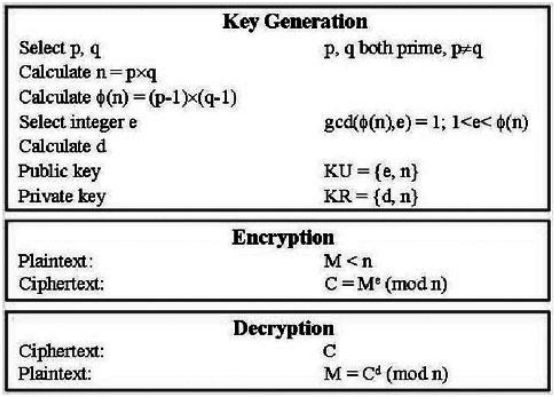

Fig 3: RSA Algorithm

LSB CODING

A very popular methodology for audio steganography is the LSB (Least Significant Bit) algorithm, which replaces the least significant bit in some bytes of the cover file to hide a sequence of bytes containing the hidden data. That's usually an effective technique in cases where the LSB substitution doesn't cause significant quality degradation, such as in 24-bit bitmaps[6]. In computing, the least significant bit (LSB) is the bit position in a binary integer giving the units value, that is, determining whether the number is even or odd. The LSB is sometimes referred to as the right-most bit, due to the convention in positional notation of writing less significant digit further to the right. It is analogous to the least significant digit of a decimal integer, which is the digit in the ones (right-most) position[7].

III. PROPOSED SYSTEM

The larger part of today's steganographic frameworks utilizes mixed media items like picture, sound, feature and so on as spread media in light of the fact that individuals frequently transmit advanced pictures over email and other internet correspondence. In a machine based sound steganography framework, mystery messages are installed in advanced sound. The mystery message is implanted by marginally modifying the twofold grouping of a sound document.

To overcome the drawbacks of existing system, an efficient encryption algorithm should be used. In proposed technique the algorithm will be implemented for Audio Signal to hide text. Number, uppercase alphabet or lowercase alphabet, special symbols like !, “ , # , $, %, & , (, ,) , *, + , ‘, - , . , / is also observed and these special symbols can also be embedded in WAV file. Objective of the project is to develop a tool that can be used to securely transmit secret messages as well as data.

RSA is an asymmetric key algorithm, the algorithm that uses different keys for encryption and decryption purposes. A user can upload the information RSA encoding schemes are used to encrypt data. The Block Diagram of proposed work is shown in following figure:

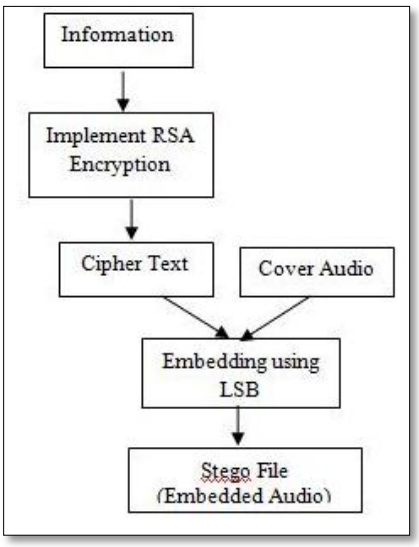

Fig 4: LSB Encoding

As Shown in figure 4, the steps of audio steganography will be as follows;

- Upload the information
- Implement RSA Algorithm to generate first level encryption
- Select the cover audio for embedding.
- Embed the cipher text in the selected audio using LSB coding to generate the stego file
- Send this stego file to the required destination through the communication channel

And when downloading the audio file, apply LSB decoding algorithm for decoding the data. Then apply the RSA Decryption algorithm to get the original information. The Block Diagram of proposed work is shown in following figure:

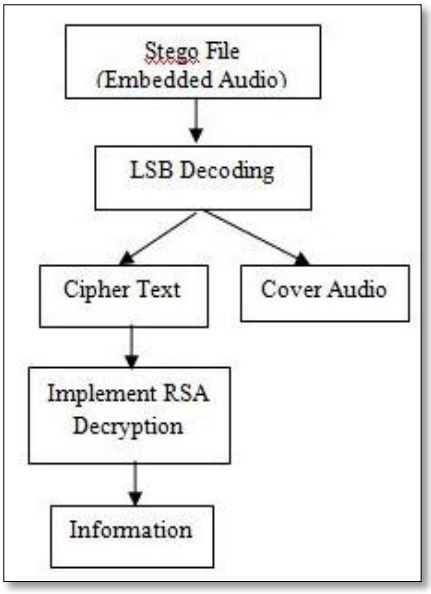

Fig 5: Extraction of text and audio

As Shown in figure 5, the steps of decryption will be as follows:

- Take the stego file (embedded audio)
- Apply LSB decoding algorithm to extract text and cover audio
- Use RSA decryption algorithm on the extracted text to generate Plain Text.
- Plain Text will be displayed to the User.

Proposed Audio Steganography framework is a strategy for information stowing away is the methodology of concealing data behind the wave record that is transporter document. The message is initially scrambled and after that installed in the transporter. It can also be used in forensic application to conceal data as well as in the music industry to monitor data sharing. For Protection of copyrighted digital media and government information system security and covert communications, data can hide in audio and video files[8].

ADVANTAGES:

1. Audio based Steganography has the potential to conceal more information:
    - Audio files are generally larger thanimages
    - Our hearing can be easily fooled
    - Slight changes in amplitude can store vast amounts of information
2. The flexibility of audio Steganography is makes it very potentially powerful :
3. Another aspect of audio Steganography that makes it so attractive is its ability to combine with existing cryptographic technologies.
4. Greater amounts of information can be embedded without audible degradation
5. Security :

- Many attacks that are malicious against image Steganography algorithms cannot be implemented against audio Steganography schemes. Consequently, embedding information into audio seems more secure due to less steganalysistechniques for attacking to audio.
- As emphasis placed on the areas of copyright protection, privacy protection, and surveillance increases, Steganography will continue to grow in importance as a protection mechanism.

IV. CONCLUSION

The steganography is one of the safest forms of data transmissions in this digital world. In our proposed method, audio steganography is enhanced more by means of cryptographic key algorithms. The message signal is transmitted with utmost security and can be retrieved without any loss in transmission in this method. Apart from lossless transmission this method easily blinds the hackers securing from data piracy. The key can be both public and private depending upon the user and serves better in both aspects. The output waveforms show that the recovered message resembles exactly as that of the transmitted message. Similarly, the carrier and transmitted signal resembles the same.These results shows that this method is lesser prone to error while transmission. Hence, this method is well suited for digital data transmission through internet and other communication systems.

REFERENCES

1. Nishith Sinha, Anirban Bhowmick, B. Kishore, "*Encrypted Information Hiding using Audio Steganography and Audio Cryptography"*, International Journal of Computer Applications, February 2015; 112 :5.
2. K.P. Adhiya Swati A. Patil CSE Dept. SSBT's COET Bambhori,Jalgaon,Bambhori,India,*"Hiding Text in Audio Using LSB Based Steganography"*, *Information and Knowledge Management* 2012; 2(3).
3. A.P.Petitcolas, R.J.Anderson, M.G.Kuhn,*"Information Hiding- A Survey"*, Process of IEEE, July, 1999; 87(7): 1062-1078.
4. Arvind Kumar, Km. Pooja, "*Steganography- A Data Hiding Technique"*, International Journal of Computer Applications, *November 2010;9:7.*
5. Gurpreet Singh, Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security", International Journal of ComputerApplications (0975 – 8887),April 2013; 67:19.

6. Nedeljko Cvejic, Tapio Seppben, "Increasing the capacity of LSB-based audio steganography", FIN90014 University of Oulu, Finland ,2002.
7. Mohammad Pooyan, Ahmad Delforouzi, "*LSB based Audio Steganography Method Based on Lifting Wavelet Transform"*, IEEE International Symposium on Signal Processing and Information Technology,2007.
8. Gunjan Nehru, Puja Dhar, "*A Detailed look of Audio Steganography Techniques using LSB and Genetic Algorithm Approach"*, IJCSI International Journal of Computer Science, IssuesJanuary 2012; 9(1): 2.