IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

Hiding Data into Audio using Steganographic Methods

[1] Susheel Kanaujiya, [2]Bharat Chaudhari, [3]Virat Kannaujiya, [4]Prof. Madhura Vyawahare

[1]B.E,Student, [2]B.E,Student, [3]B.E,Student, [4]Assistant Professor
[1]Information Technology, [2]Information Technology, [3]Information Technology, [4]Computer Engineering
[1]Pillai College of Engineering, Mumbai, India, [2]Pillai College of Engineering, Navi Mumbai, India
[3]Pillai College of Engineering, Mumbai, India,[4]Pillai College of Engineering, Navi Mumbai, India

Abstract: Security is the major challenge of digital communication. Cryptography and steganography are two common methods available to ensure security.Steganography is the term used to hide secret messages in a text, audio or image file.Modern methods are necessary to keep information secret and to protect it from the growing danger of external hackers.Steganography makes it possible to transmit information through communication channels. In this work we have focused on digital audio as the carrier and cover file. Audio steganography is a method to safely conceal a secret message into an audio cover file in various ways.The audio files are in the standard WAV format, in which the secret message is embedded by using the LSB algorithm. The secret message gets encrypted using the RSA algorithm before the embedding process. This combination is providing two level security to the secret message to be transmitted.

***Index Terms** - Steganography,CryptographyData hiding,LSB;*

I.INTRODUCTION

In the 21st century, many private messages are transmitted by the Internet world. Most people in this world think that sending messages through the Internet are safe and secure, but that is not always the case. We may protect our information by covering data within certain other files (audio, picture) and it can be done with the help of steganographic techniques. Steganography is the method of concealing data within the other data file. Steganography is the process of hiding a message into an appropriate carrier file, that can be an image or an audio file. The transporter can then be sent to a receptor without anyone knowing that it contains a hidden message.

Audio steganography conceals information in such a way that unwanted persons cannot access the information. They utilize different types of audio files like WAV, MP3 or AU. In data hiding, the secret message can be transferred on the receiver side by using an audio file. We are using the steganography technique for the data hiding purpose. We are first encrypting the message using the RSA algorithm and then using audio file as a cover for hiding data. For data hiding in audio files LSB method is used. This Audio Steganography consists of modules i.e. sender and receiver modules.

II. LITERATURE SURVEY

Many people are exploring the data hiding using steganography and over that advantages of audio steganography. Author Palwinder Singh et.al. has highlighted some emerging concepts and recent techniques like Echo Data Hiding ,Parity Coding, Phase Coding, Spread Spectrum, Least Significant Bit Coding (LSB), about audio steganography [1]**.** In this paper we understood the performance of recent audio steganography techniques in relation to strengths, weaknesses and the degree of concealment. They have discussed certain developments such as audio steganography based on the genetic algorithm. Among all the methods that have been mentioned above they have concentrated and implemented the project in the Enhanced Least Significant Bit algorithm by using LSB it minimizes the distortion level of the image file and security can also be increased.

From another paper we understood the different steganography software such as DeepSound and Mp3Stego which is by Chua Teck Jian et.al [2]. The authors focused on the security related to the encryption process. According to the authors, This is good security practice; but, the secret information may become too long after encryption to fit into the audio and distort the audio file. Therefore, the authors claim that it is necessary for encryption of a secret message with an encryption stream prior to embedding the message in the audio file . That's because stream encryption provides bit-by-bit encryption whereas block encryption provides a fixed amount of bit encryption. They have proposed a method to improve the security of secret communication and quality of file.

Mazhar Taye et.al. in their work have used the least significant method for Embedding secret messages in the digital sound [3]. This audio steganography program processes audio files such as WAV, AU and even MP3. The integration of secret messages into digital audio is usually more difficult than the integration of messages in other formats, such as digital images. Audio steganography uses a variety of algorithms, but the least significant bit (LSB) is applied here.The sound quality depends on the size of the user's choice of audio and the length of the message.

A robust substitution technique is used to implement proposed work of audio steganography by Pooja Kengale et.al. [4]. The technique solves the different problems inherent in the use of traditional alternative techniques. It enhances the ability to mask data while being robust to diverse intentional (viruses, denial of service attacks, theft of data etc) as well as unintentional attacks (human error, environmental hazards, and computer failures etc). In the way it provides privacy to data successfully.

From the literature survey we have summarized the steps for this Audio Steganography:

- First the sender prompts the receiver via message.text or Mail that he/she would like to share a secret message.
- The recipient module generates 2 keys (One private and One public) , shares the public key for encryption to the sender (by message.txt) and maintains the private key for decryption of secret messages.
- With the help of a public key the sender encrypts the secret messages and embed it into the audio wav file.
- At the encoder module frame bytes of the audio file is calculated and the last bit of each byte modified with encrypted data.
- In the receiver module, the decoder decodes the encoded audio data.
- The encrypted data is then decrypted using the receive module using his private key.

III. TECHNIQUES USED

There were a lot of techniques to hide information or messages in the audio. Among all of them we used LSB encoding and for data encryption we used the RSA algorithm.

LSB coding:

Least Significant Bit Coding is a way to integrate data into an audio file. By replacing the last bit of each frame bytes with a binary message, the LSB encoding makes it possible to encode a large quantity of data.

RSA Algorithm:

RSA (Rivest–Shamir–Adleman) is an algorithm for modern computers to encrypt and decrypt messages. RSA is an asymmetric algorithm which has two different keys: a public key and a private key. The public key can be known by anyone and is used for message encryption. Messages encrypted using the public key can only be decoded with the private key. The private key must remain confidential. It is very hard to calculate the private key from the public key.

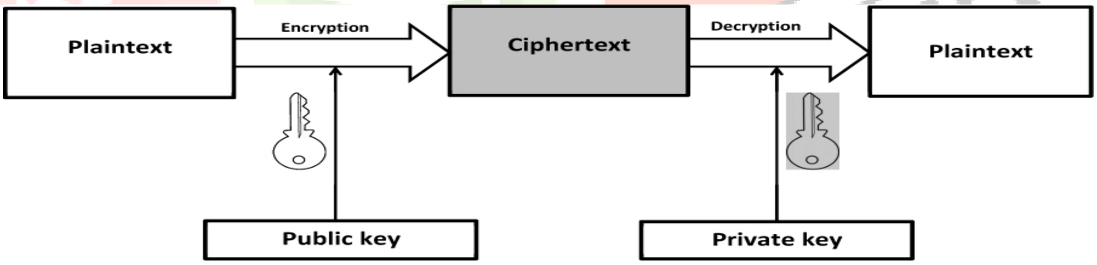

Figure 1: RSA Algorithm

Generating keys:

RSA algorithm generates the keys in following way:

1.Select two different large random prime numbers p and q .This should be kept secret.
2.Calculate n = p.q, n is the public and private key modulus.
3.Compute the totient $\lambda(n)$=(p-1)(q-1).
4.Select an integer e such as $1 < e < \lambda(n)$ .Here e is known as the public key exponent.
5.Compute d to satisfy the congruence relation $d \equiv e^{-1}$ (mod $\lambda(n)$). d is kept as the private key exponent.

Encrypting Message:

Sender uses public key (n,e) to encrypt the message using formula c=m^e mod n . This will be carried out quickly using the technique of exponentiation by way of squaring.

Decrypting Message:

Receiver can recover the original message from c by using his/her private key d by the formula of m = c^d mod n.

.

IV. PROPOSED WORK

The method we used was to encrypt text and hide it under a cover audio file.The embedding process at the sender's side and the extraction process at the receiver's side are the two aspects of this approach. The encoded text is concealed inside the audio cover file during the embedding phase, and there may be no distortion in the audio signal due to the LSB being changed while all other parameters remain the same. The secret text is extracted from the stego-object, which is the audio cover file carrying the secret data, in the extraction stage. The secret information in this case is text, which should be encoded before being embedded in the audio.

System Architecture:

The system architecture is given in Figure 2. Each block is described in this Section.

A. Secret Message: Here Secret message is nothing but the text data which should be less than the size of the cover file.

B. Audio cover file: Audio file used for Embedding data into it by way of using LSB of audio steganography methods. It is very important that Audio files need to be in WAV audio type.

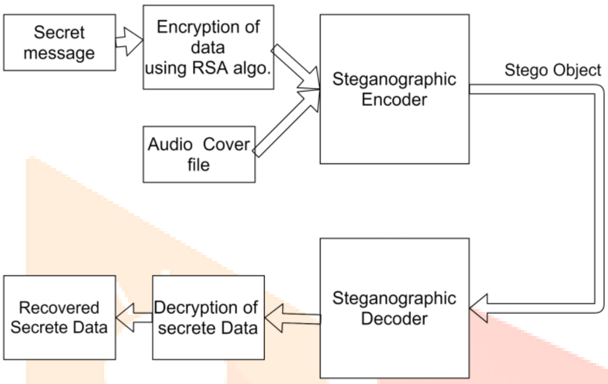

Figure 2: Proposed system architecture

C. Steganographic Encoder: The audio file and the encrypted secret message are submitted to the steganographic encoder. The secret message is then encoded using the RSA cryptographic method and placed in the audio file. The encoder's output is an audio file with all of its LSBs updated using the message bits. The output is the Stego-object, and is shared to the recipient by email or text.

D. Steganographic Decoder: The stego object is only processed on the receiver end if the precise key used at the encoder is provided. The decoder retrieves the message from the stego-object and returns the secret message file once the user has provided the key. The audio cover file and data are separated as a result of this decoder.

E. Received secret message: After the steganographic decoder secret message separated from the audio file that's the same as a secret message on the time it got embedded within the audio.

V. REQUIREMENT ANALYSIS

1. Software

For this project, we've used Pycharm, which is an integrated development environment utilized in pc programming, in particular for the Python language. As Pycharm supports python, we use python programming language.

2. Hardware

To work on the Project minimum of 300 Mhz processor and minimum of 4 GB RAM needed and no strict specification about the hard disk.

VI. RESULT AND ANALYSIS

After performing various experiments the following observations are taken:

The carrier file should be an Audio (.wav) file and the secret message should be a text message.

Here for the experimental scenario the carrier audio file is song.wav of 34.3 MB size. Thus the carrier file must be greater than secret message.

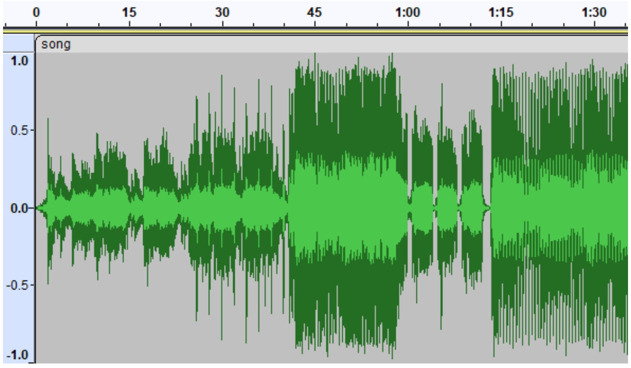

Figure 3: Waveform of original audio file

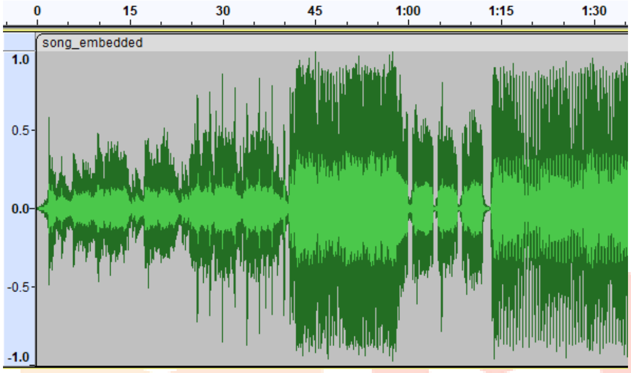

Figure 4: Waveform of text embedded audio file

Above figure shows the comparison between the original file before the secret data is embedded in it and the file after the secret data is embedded in it. This comparison shows that both audio files have the same waveform.

	Cover File	Secret data	Stego file
File name	song.wav	Peter Parker is Spiderman!	song_embedded.wav
Size	34.3 MB		34.3 MB

Table No.1: While Embedding Data

	Stego File	Retrieved Secret data	Cover file
File name	song_embedded.wav	Peter Parker is Spiderman!	song.wav
Size	34.3 MB		34.3 MB

Table No.2: After Retrieving Data

By observing the above tables we analyze that there is no disturbance in the audio cover file after embedding data and the size of the original file is the same as the stego file.

VII. CONCLUSION AND FUTURE SCOPE

Steganography is one of the secure ways of secret data transmissions in today’s digital world. In this work, the secret message is encrypted using RSA Algorithm and then this encrypted message gets embedded into an audio file using LSB method .Future scope consists of improved protection and robustness by using advanced cryptography algorithms and size of message should be increased.

VIII. ACKNOWLEDGEMENTS

We authored this paper on security transfer messages, with the support of my external guide, prof. Prof. Madhura Vyawahare Assistant Professor and Phd Candidate, Pillai College of Engineering. We are thankful to our HOD Dr. Satish Kumar Verma. We are thankful to my principal sir, Dr. Sandeep Joshi for their support and inputs.

REFERENCES

[1] Ass. prof. Palwinder Singh, "A Comparative study of Audio Steganography Technique". IRJET. Volume 03 Issue:04.pp. 580-585 .Apr-2016.

[2] Pooja kengale, Rakhi kadam,Rajkumar chaudhari,Prof.Sagare,“Data Hiding In Audio by Using Audio Steganography”, vol. 5, Issue 1. pp. 88-91, IJLTEMAS .January, 2015.

[3] Mazhar Tayel, Ahmed Gamal, Hamed Shawky, “A Proposed Implementation Method of an Audio Steganography Technique,” J.Jan. 31 ~ Feb. 3, 2016 ICAST 2016 .

[4] Chua Teck Jian,Chuah Chai Wen, Nurul Hidyah Binti ,Ab. Rahman and Isredza Rahmi Binti A. Hamid . "Audio Steganography With Embedded Text".ECS, IRIS2017, IOP Conference Series: Materials Science and Engineering 226(2017)012084 doi:10.1088/1757-899X/226/1/012084 .

[5] Anupriya Arya, Sarita Soni ``A literature Review on Various Recent Steganography Techniques". international Journal on future revolution in Computer science and Communication engineering (IJFRCSCE). www.iifrcsce.org (ICATET 2018) Volume: 04, Issue: 01, January 2018.

[6] Mohit Kulkarni1, Maitreyee Phatak2, Uma Rathod3, Sudhir Prajapati4, “Efficient Data Hiding Scheme Using Audio Steganography,” IRJET, Maharashtra, India, March 2016, Volume:03 Issue:03 pp. 1701-1706.

[7]https://ukdiss.com/examples/implementation-design-for-audio-steganography.php#cite this.

[8]https://www.slideshare.net/rajanyadav18/datasecurityusingaudiosteganographyfinal-report.