ISSN 2347-4289

Implementation Of Audio Steganography Using RSA Algorithm

Neha Deshpande, Rashmi Fusate, Pooja Malviya, Shweta Dhyavartiwar

Computer Technology Department, Yeshwantrao Chavan College of Engineering, Nagpur, India
neha.deshpande05@gmail.com, rashufusate27@gmail.com, pmpoojamalviya2@gmail.com, dhyavartiwar@yahoo.com

Abstract: Steganography is the method of hiding the message in a cover file. Modern methods of steganography are: Image Steganography, Audio Steganography, and Video Steganography. In this paper we are focusing on "Audio Steganography".In Audio Steganography system, secret messages are embedded in digital sound. In this paper, the secret message is embedded by altering the least significant bit of a sound file. Audio Steganography software can embed messages in WAV, AU, and even MP3 formats. Our approach is to hide message in audio file by Least Significant Bit (LSB) insertion along with asymmetric key based RSA algorithm. The idea behind this paper is to enhance the security of information that has to be sending to receiver.

Keywords: Steganography,Audio Steganography, Least Significant Bit(LSB), Cryptography, RSA Algorithm.

I. INTRODUCTION

Steganography is the art of hiding text into some form of cover file. Steganography comes from the Greek words Steganós (Covered) and Graptos (Writing). Steganography and cryptography are two different concepts. Cryptography is encrypting the plaintext whereas; steganography is embedding the text into cover file. There are many approaches to hide the information, suchas, Least Significant Bit (LSB), Phase Coding, ParityCoding, Spread Spectrum, and Echo Hiding. The most common approach is Least Significant Bit (LSB) insertion. Among all these methods Least Significant Bit (LSB) is the simplest method to embed the information in audio file. In LSB method, the information is embedded into bit stream of audio file.

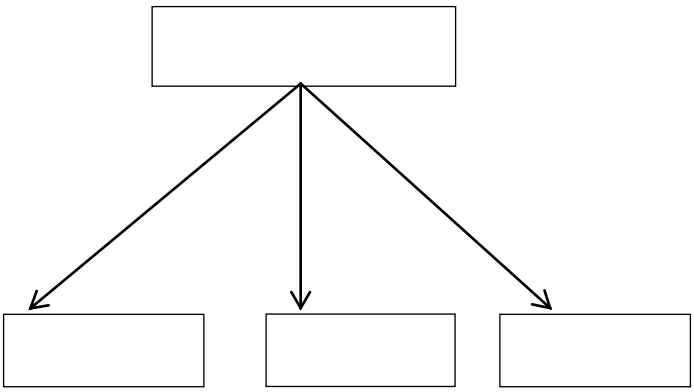

Fig1. *Different types of Steganography technique*

To make information more secure and to prevent it from accessible by unauthorised user the concept of cryptography can be introduced. Cryptography is of two types: symmetric key and asymmetric key. The symmetric key is one which uses only one secret key. The RSA Algorithm is asymmetric key cryptography and it uses two keys, i.e. one is private key and the other is public key. The RSA Algorithm makes use of private key and public key to encrypt and decrypt the message.

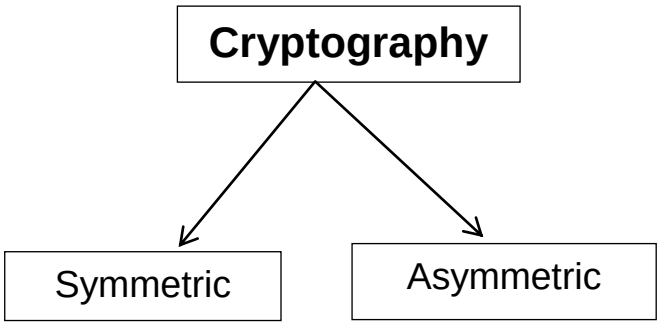

Fig2. *Cryptography Techniques*

The steganography and cryptography concepts are combined to implement audio steganography. The audio is converted into bit stream. The text which is to be send to receiver is first encrypted using public key and then this encrypted text is encoded in audio file. At the receiver site, the receiver will first decode the text and then decrypt it using private key to obtain original text.

II. LITERATURE SURVEY

Steganographic technique is implemented in many ways these days. The literature survey of steganography shows that it can be implemented in modern ways: Image, Audio, Video, Protocol etc. The steganography technique was first implemented for digital images and video sequences. The disadvantages in image steganography are covered in audio steganography. Some old methods of steganography are explained in the table.

SrNo	INVENTION	DESCRIPTION
1.	Earliest recordings of Steganography were by the Greek historian Herodotus in his chronicles known as "Histories" and date back to around 440 BC	King Darius of Susa shaved the head of one of his prisoners and wrote a secret message on his scalp. When the prisoner's hair grew back, he was sent to the Kings son in law Aristogoras in Miletus undetected.
2.	Roman's found invisible ink technique for steganography.	It is based on natural substances such as fruit juices and milk. This was accomplished by heating the hidden text, thus revealing its contents.
3.	Inventions in 15th and 16th Century	Many writers including Johannes Trithemius (author of steganographia) and Gaspari Schotti (author of steganographia) wrote on steganographia techniques such as coding techniques for text, invisible ink, incorporating hidden messages in music.

III. PROPOSED WORK

Our work focuses more on information security. This paper tells the way in which how information can be made more secure. In our, project we used least significant bit (lsb) technique for embedding the information in last bit of audio cover. Also, we have converted the audio into wave (.wav) format, so that the audio does not become noisy. This will only embed the information in audio cover and there is no security to information. For the purpose of making information more secure we used cryptography. The best known algorithm to provide security is RSA Algorithm. This will first encrypt the message and then embed it into audio cover. This on receiver side will first have to decode it and then decrypt the message to obtain original information.

A. Least Significant Bit (LSB)

LSB works by replacing directly the last bit of the media with secret bits to get the stego image hence this method is supposed as an easy and fast in the algorithm.[2]These bits are divided into 4- MSB's and 4-LSB's. Changing LSB's does not give drastic change and hence used commonly for steganography purpose.[3]

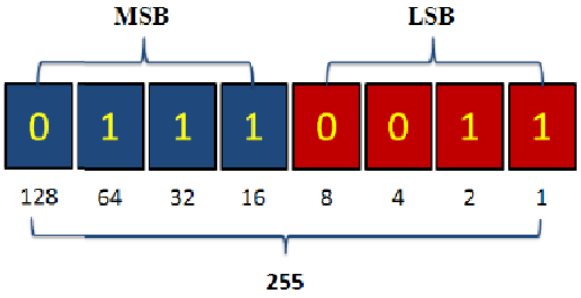

Fig3. *Binary Representation*

B. RSA Algorithm

RSA was invented byfor Ron Rives, Adi Shamirand Leonard Adleman. It is the algorithm used for encrypting and decrypting messages. RSA is asymmetric key algorithm, hence using two different keys. One is private key: it is kept secret and other is public key: can be shared. Using these two keys the message is encrypted and decrypted.[3]

C. Wave Format(.wav)

WAV is a variant of the RIFF bit stream format method for storing data in "chunks". WAV files are usually stored uncompressed, which means that they can get quite large, but they cannot exceed 4 gigabytes due to the fact that the file size header field is a 32-bit unsigned integer (32 bit file length means a maximum of 4 gigs)

D. Flow Diagram

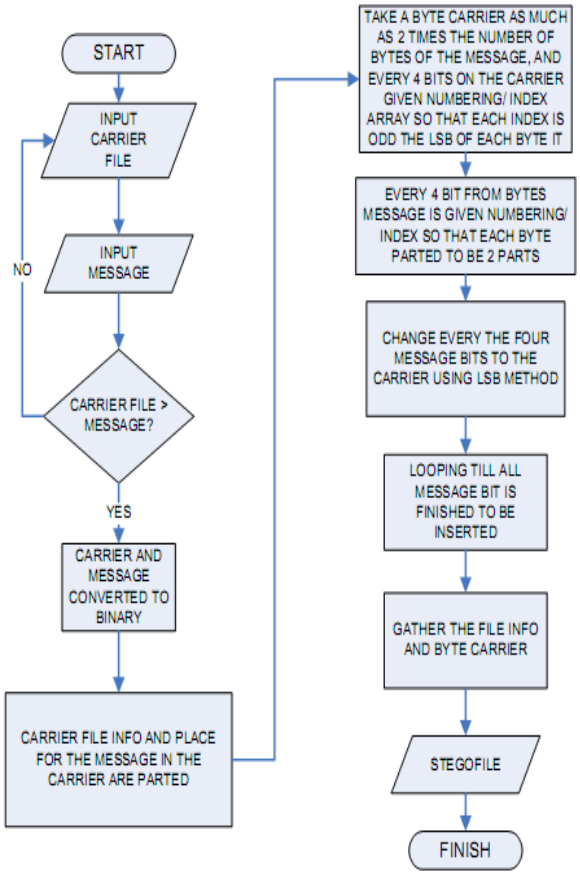

Fig4. *Embedding the text*

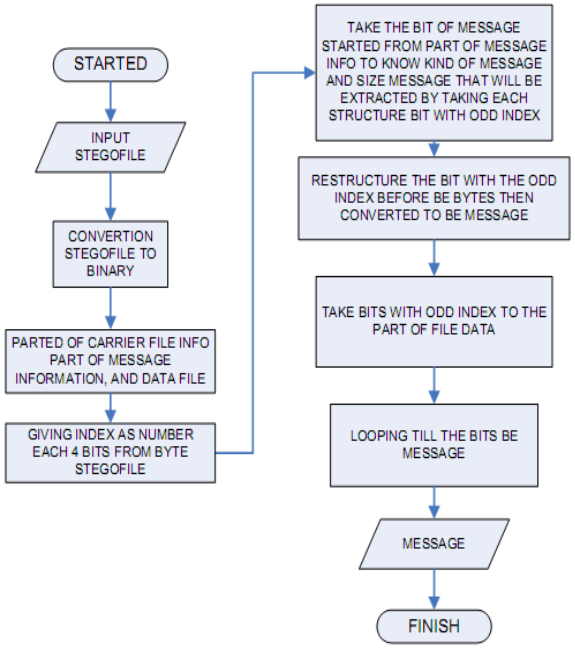

Fig5. *Decoding the text*

IV. EXPERIMENTAL RESULTS

The audio file is in wave format (.wav). We can either record a audio file or use the existing one. The secret key must be provide so that further process can be done. The new encoded audio file must be saved with new name. The text can be either written in text box or existing file can be considered. As we click hide button, the message gets encrypted and we get a pop-up-menu showing "hiding done". This is the hiding process. In extraction process, we need to provide the secret key, the new audio file. When we click on extract button the message is decoded and we a decrypted message which is an original message.[5]

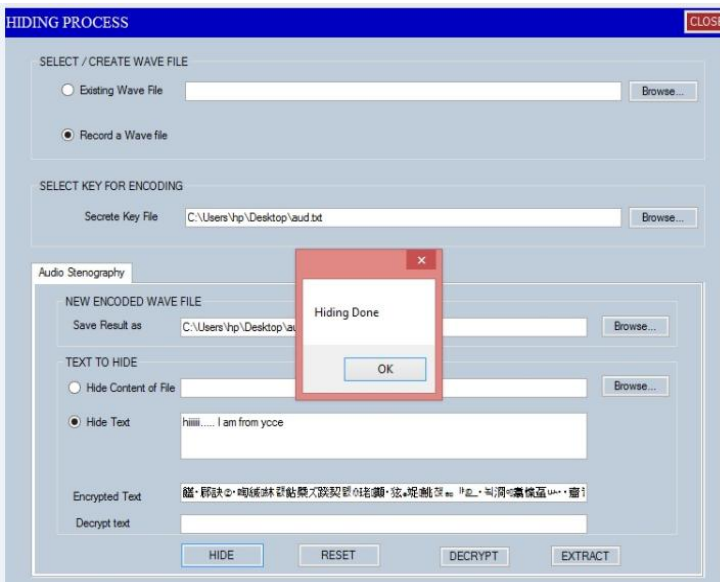

Fig6. *This figure shows the encryption and embedding of text into audio file.*

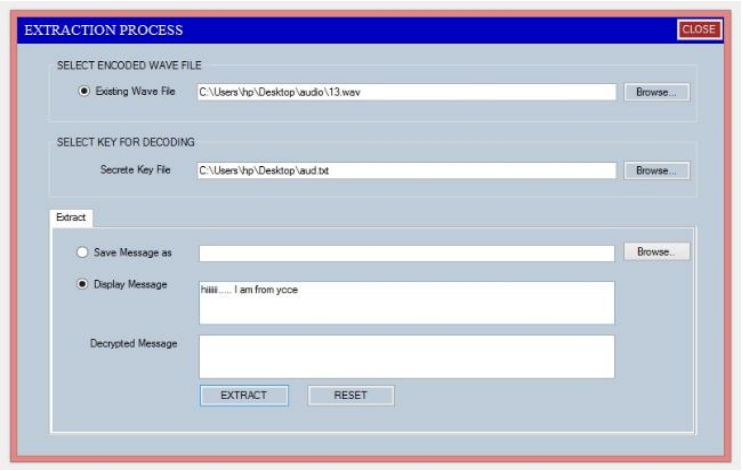

Fig7. *This figure shows the decryption and decoding of text from audio file*

V. CONCLUSIONS

Since text is hidden in a cover file, steganography can be said as the safe way of transmission of text. To make this data more secure cryptographic techniques are applied on data. The data is first encrypted and then embedded in audio file. This technique makes it difficult to third party to access the data. Hence it can be said as the most secure form to send message over a network. Even after hiding the text in audio file, the size of audio file does not change and hence it is difficult to identify whether the data is present in it or not.

REFERENCES

[1] Vijaya Lakshmi Chittimalli B.Tech, Jawaharlal Nehru Technological University, 2006 **"KEEPING SECRETS SECRET – IMPLEMENTATION OF STEGANOGRAPHY WITH AUDIO FILE AND ENCRYPTED DOCUMENT",**at CALIFORNIA STATE UNIVERSITY, SACRAMENTO FALL 2009.

[2] Jasril, Ismail Marzuki, Faisal Rahmat INTERNATIONAL JOURNAL ON SMART SENSING AND INTELLIGENT SYSTEM **"CAPACITY ENHANCEMENT OF MESSAGES CONCEALM IN IMAGE AND AUDIO STEGANOGRAPHY"**, Informatics Department, Faculty of Sciences and Technology, State Islamic University of Sultan Syarif Kasim Riau, Indonesia, VOL. 6, NO. 5, DECEMBER 2013.

[3] Jatinder Kaur, Ira Gabba, **"Steganography Using RSA Algorithm",** International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-3, Issue-3, August 2013

[4] Masoud Nosrati, Ronak Karimi, Mehdi Hariri, **"Audio Steganography: A Survey on Recent Approaches"**, World Applied Programming, Vol (2), No (3), March 2012. 202-205 ISSN: 2222-2510 ©2011 WAP journal.

[5] K.Sakthisudhan, P.Prabhu, P.Thangaraj, **"Secure Audio Steganography for Hiding Secret information",** International Conference on Recent

Trends in Computational Methods, Communication and Controls (ICON3C 2012)

[6] Shikha Sharda1, Sumit Budhiraja2, **"Image Steganography: A Review"**, International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459,ISO 9001:2008 Certified Journal, Volume 3,Issue 1, January 2013)

[7] Gaurav Singh, Kuldeep Tiwari,Shubhangi Singh, **"Audio Steganography using RSA Algorithm and Genetic based Substitution method to Enhance Security"**, International Journal of Scientific & Engineering Research, Volume 5, Issue 5, May-2014, ISSN 2229-5518