Audio Cryptography

[1]M Sai Chandrahasa, [2]T S Srinivas, [3] Prasad B

[1]II/IV, [2][3]Associate Professor

[1][2][3] Department of CSE, Marri Laxman Reddy Institute of Technology and Management (MLRITM) Hyderabad

[1]chandu.hasa12@gmail.com [2]tumulurisri2909@gmail.com [3]bprasad@gmail.com

Abstract: **Cryptography secures information by protecting its confidentiality. It can also be used to protect information about the integrity and authenticity of data. Stronger cryptographic techniques are needed to ensure the integrity of data stored on a machine that may be infected or under attack. So far Cryptography is used in many forms but using it with Audio files is another Stronger Techniques. The process of Cryptography happens with Audio File for transferring more secure sensitive data. The Sensitive Data is Encoded with an Audio File and Passed over Insecure Channels to other end of Systems. Here we are using .wav file Format for Encryption and Decryption of Message. The given message will be encrypted with a given audio file using a secret key. The System will then embed the secret message into the audio file. The result will be a new audio file, which has the secret message in it. While decrypting the same key should be given for encrypted audio file to get the secret message from it.**

Keywords: **Cryptography, Secures information, Confidentiality, Encryption process, Decryption process, Least Significant Byte.**

I.   INTRODUCTION

Cryptography with Audio is a desktop application. The purpose of this application is to provide the security for the confidential information. This application does not allow the hackers to view the data, can view only audio file when it is being passed over the internet. Then at the recipient side the original information i.e., plain text will be extracted from the audio by performing decryption operations

In the encryption process each LSB (least significant byte) will be replaced by the encrypted data. During decryption process each data will be extracted from each LSB and then performs decryption operation which results into a plain text which was sent by the source side.

The data is embedded into the audio file. Before embedding it into the file, encryption operation will be performed by using the encryption key which is provided by the source. Then this audio file will be passed over the net, even if hacker hacks it, can be able to see only an audio file. At the destination side this data will be encrypted from audio file and performs decryption to get original message.

II.   BACKGROUND

Security often requires that data be kept safe from unauthorized access. And the best line of defense is physical security (placing the machine to be protected behind physical walls). However, physical security is not always an option (due to cost and/or   efficiency considerations).

Instead, most computers are interconnected with each other openly, thereby exposing them and the communication channels that they use.

Cryptography secures information by protecting its confidentiality. It can also be used to protect information about the integrity and authenticity of data. Stronger cryptographic techniques are needed to ensure the integrity of data stored on a machine that may be infected or under attack.

So far cryptography is used in many forms but using it with audio files is another stronger techniques. The process of cryptography happens with audio file for transferring more secure sensitive data. The sensitive data is encoded with an audio file and passed over insecure channels to other end of systems. Here we are using .wav file format for encryption and decryption of message.

The given message will be encrypted with a given audio file using a secret key. The system will then embed the secret message into the audio file. The result will be a new audio file, which has the secret message in it. While decrypting the same key should be given for encrypted audio file to get the secret message from it.

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 steganography is an art of secret communication. The term hiding refers to the process of making the information

imperceptible or keeping the existence of the information secret.

The steganography algorithm were primarily developed for digital images and video sequences. Interest in research in audio steganography started. Any steganography technique has to satisfy two basic requirements. The first requirement is perceptual transparency that is cover object (object containing any additional data) and stego object (object containing secret messages) must be perceptually indiscernible. The second constraint is high data rate of the embedded data. In this project we will hide data or secret message in an audio file using two algorithms.

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.

Multiple LSB algorithm is a specialized form of the standard LSB algorithm. We use 2 novel approaches of LSBs of audio samples for data hiding. These methods check the msbs of the samples, and then number of LSBs for data hiding is decided. In this way, multiple and variable LSBs are used for embedding secret data. These proposed methods remarkably increase the capacity for data hiding as compared to standard LSB without causing any noticeable distortion to the data. This method considers the value of the msb of the digitized samples of cover audio for data hiding.

III.   MODULES DESCRIPTION:
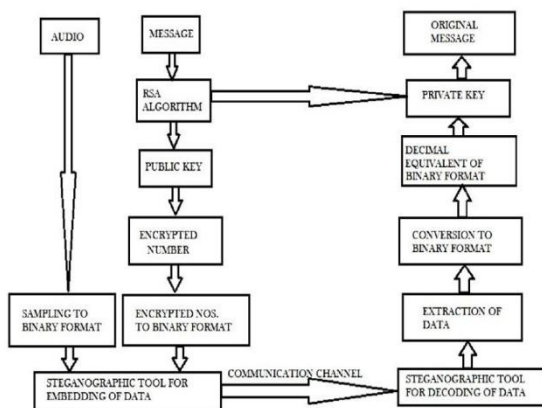
Fig 1: architecture

A.   *Sampling the message:*

1. First we will take an audio file and perform sampling on it. We will sample the file in 8 bits per frame.
2. Read the cover audio signal.
3. Read the stego object

B.   *Multiple LSB algorithms:*

Multiple LSB algorithm is a specialized form of the standard LSB algorithm. We use 2 novel approaches of LSBs of audio samples for data hiding. These methods check the msbs of the samples, and then number of LSBs for data hiding is decided. In this way, multiple and variable LSBs are used for embedding secret data. These proposed methods remarkably increase the capacity for data hiding as compared to standard LSB without causing any noticeable distortion to the data. This method considers the value of the msb of the digitized samples of cover audio for data hiding.

C. *Embedding the message:*
1.   Input the message file which we want to transmit.
2.   Then encrypt it using the rsa algorithm by the use of public key.
3.   Write the text in a file to be embedded.
4.   For embedding purpose, the msb of the cover sample is checked.
5.   If msb is "0" then use 6 LSBs for data embedding.
6.   If msb is "1" then use 7 LSBs for data embedding

D. *Encrypting the message*:
1.   After encryption we will embed the encrypted data in the audio file. Here for embedding we will use multiple LSB algorithms. The above operations will be performed at the transmitter end.
2.   Generate public and private key by using rsa algorithm.
3.   Apply encryption function on plaintext to produce cipher text.
4.   The intended receiver will extract the encrypted data using steps of extraction from the multiple LSB algorithms.

E. *Retrieving the message:*
1.   After that the stego audio is transmitted to the intended receiver.
2.   The intended receiver will extract the encrypted data using steps of extraction from the multiple LSB algorithms.
3.   Then receiver will use the private key for decryption to get the original message.
4.   After every such 16 messages bits retrieved, they are converted into their decimal equivalents to get ASCII values of the secret message.
5.   Finally apply rsa decryption to recover plaintext

F. *Basic RSA algorithm:*

1.   Choose 2 prime numbers p and q

2.   Compute n=p q
3.   Compute m(euler's totient function)=(p-1)(q-1)
4.   Select e such that gcd(e,m)=1
5.   Where (e,n) is the public key
6.   Find d such that 1=d e mod m
7.   1 = km + de
8.   Using the extended euclid algorithm we see that 1= - km + de
9.   Where (d,n) is the private key
10.   Encryption function $y = x^e \bmod n$
11.   Decryption function $x = y^d \bmod n$
12.   Here x is the number to be encrypted and y is its encrypted form

IV. EXPERIMENTAL RESULT

Fig 2: home screen

Fig 3: input screen

Fig 4: key encrypting screen

Advantages:

❖ Secrecy in terms of message hiding.
❖ High capacity of the audio file.
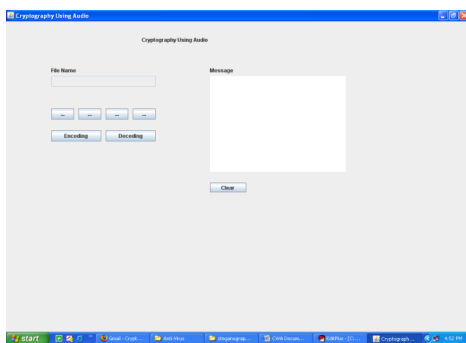❖ Accurate extraction.
❖ Resistance from external attacks.

Disadvantages:
❖ Small alteration in the audio file.
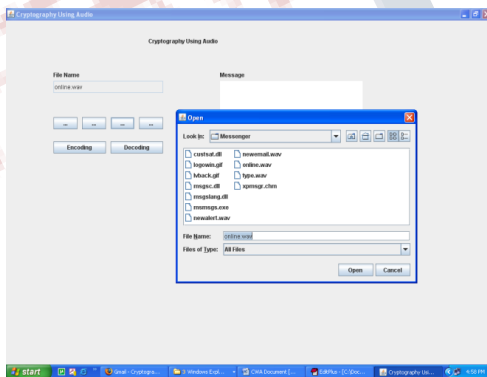❖ Complications in recovering original audio file.

V.   CONCLUSION

The target of this paper is to implement two techniques like steganography and cryptography for confidential communication between the two entities. In our paper we are using multiple LSB algorithm which is much more secure than the standard LSB technique. In addition to it we are using rsa algorithm for extra security which is based on cryptography. As we are using audio as a cover file, high amount of data can be embedded and also provides resistance from external attacks.
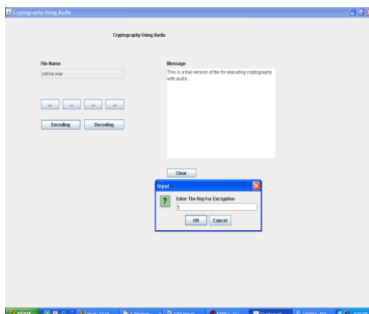
REFERENCES

[1] m.ram mohan reddy s.s divya. Hiding text in audio using multiple LSB steganography and provide security using cryptography. International journal of scientic technology research, 1(6):68-70, 2012 shobha lokhande. 2012.

[2] tanmay bhowmik pramatha nath basu. On embedding of text in audio a case of steganography.ieee publication. Pages 203-206, 2010.

[3] k. Gopalan. Audio steganography using bit modication. Proc. Ieee int.conf. Acoustics, speech, and signal processing, 2(2):421-424, 2009.

[4] teoh suk kuan rosziati ibrahim.steganography algorithm to hide secret message inside an image.computer technology and application, 2:102-108, 2011.