Multilayer Security Using RSA Cryptography and Dual Audio Steganography

Kripa N Bangera
Student, Manipal Institute of technology,
Manipal University
kripanb94@gmail.com

Yashika Paddambail
Student, Manipal Institute of technology
Manipal University
yashikapaddambail@gmail.com

Dr.N.V. Subba Reddy
Professor, Manipal Institute of technology
Manipal University
nvs.reddy@manipal.edu

Shivaprasad G
Professor, Manipal Institute of technology
Manipal University
shiva.prasad@manipal.edu

Abstract—— In today's era, millions of users make use of internet in their day to day activities. In various commercial and non-commercial applications it is very essential to protect the confidentiality of data. Hence it is mandatory to have automated tools to protect the data. With the introduction of distributed computing systems, network communication security has become another major aspect. All academic institutions, business and government organisations make use of distribution networks to process their data. Therefore, protecting data during a transmission within a network of computers located at different geographical locations where end users working simultaneously are inevitable. Also for people making modern day e-transactions like money transfer, online shopping etc., a secure framework is adequate. Cryptography and Steganography are a few of the methods used for secure communication. In this paper, a technique has been proposed for providing multilayer security by combining cryptography and steganography. The proposed RSA cryptographic algorithm integrated with dual audio steganography algorithm provides a higher level of security.

Keywords— Cryptography, Steganography, RSA Algorithm, LSB Audio Steganography Algorithm, Information Security

I. Introduction

In the world today, there is a rapid increase in the number of internet users. A recent statistics shows that there are 3.5 billion people who use internet. Within a year, there has been a tremendous increase in the internet users to over a billion. Due to the increase in the internet for commercial and non-commercial purposes, there is an increased need for security of data that is transferred or exchanged. The communication between a sender and a receiver without the interference by any third party is called a secure communication. During communication, an insecure channel is highly vulnerable to attacks such as SQL injection, IP spoofing, eavesdropping etc.

Steganography, identity based networks, firewalls, anonymous proxies and cryptography are the very few major techniques that are employed to achieve secure communication currently. Cryptography is a method of storing and transmitting the data in an unintelligible manner so that only the intended recipient or receiver can read and process it [1]. In cryptography, the original message, which is called as the plaintext can be converted to an unintelligible form called cipher text. This is done by using an encryption algorithm. The cipher text is converted back to the plaintext using a decryption algorithm.

Steganography is a method where it takes information and hides it within another piece of information. It takes

advantage of files such as text files, audio files and images that contain few blocks of data which is either unused or not important and hides it in the encrypted message [8]. The components of a steganographic message are:

1.Secret Message: Secret message refers to that part of a steganographic message that is to be concealed. This message has to be enciphered. Since this message is meant to be hidden, it makes it difficult for a third person to know the hidden message.

2.Cover Data: The secret message is hidden in cover data component. It acts as a container that can hide the message. It may include audio files, digital images, text files and digital video.

3.Stego Message: Stego message refers to the final product and it is as important as the secret message.

II. OVERVIEW OF LITERATURE

A. Cryptography

Cryptography is a technique for transmitting and storing the data in a particular unintelligible form so that only the intended receiver can read and process it. The process of producing cipher text from plaintext is called encryption. The reverse process of producing the plaintext back from the cipher text is called decryption [2]. Cryptographic systems tend to involve both an algorithm as well as a secret value. The secret value is called the key. There are two types of cryptography:

1. Symmetric Key Cryptography:

In symmetric key cryptography, the sender and the receiver agree on a secret key which is used for encrypting and decrypting the messages. The main concern in this type of Crypto-system is a way to share the secret key safely between the two parties. The whole system collapses if the key is known by a third party by any means. Various algorithms that use this mechanism are DES, AES, TDES and Blowfish.

2. Asymmetric Key Cryptography:

In asymmetric key cryptography, two different keys are used, one for encryption and the other for decryption. This mechanism is also called as the Public Key Cryptography

978-1-5090-3704-9/17/$31.00 © 2017 IEEE

(PKC) since the users use two keys that is, public key, which is known to the public, and private key, which is known only to the user. RSA employs asymmetric key cryptography.

Ron Rivest, Shamir and Adleman proposed the RSA algorithm. It is a public key cryptosystem which s useful for security in emails and other electronic transactions. Its advantages are: increased security, provides digital signature that cannot be repudiated and large prime numbers can be selected for enhancing the security of keys.

However, the RSA algorithm has some disadvantages as well. The main disadvantage is its speed during encryption [7]. RSA may be vulnerable to impersonation, even if the user's private keys are not available.

B. *Steganography*

Steganography is a method that is used for hiding data like text, image, audio and video in some another piece of information. .doc, .wav, .mp3, .au, .bmp, .gif, .txt and .jpeg are the various formats that can be used for hiding the message. Embedding secret content into digital sound is known as audio steganography. .wav, .au and .mp3 are the formats that can be used to embed messages in audio steganography.

LSB coding is a method to imbed data in an audio file. Here, the LSB of each sampling point is interchanged with a binary content to encode vast data [3]. The data transmission rate of 1 kilo bits per second per one kilo hertz is allowed. At the other end, the receiver needs to obtain access to the sequence of sample indices to distil the secret content.

III. PROBLEM DEFINITION

With the increase in consumption of internet, security has become a major concern to everyone. To cope up with this security issue, the developers are unremittingly working to make the internet free from cyber-attacks and jamming. Many algorithms and techniques are developed but the hackers are smart enough to hack information [1]. Steganography is constrained with same limitations as cryptography. A sender and the reciever must first agree on a method of steganography for which they need to exchange messages consisting of secret parameters.

IV. EXISTING SOLUTIONS

Very few methods such as combining steganography with cryptography are presented. Furthermore, most of these methods are based on image steganography. The combined usage of audio steganography along with RSA cryptography is unattended by a lot of researchers until now. Both steganography and cryptography have their own vulnerabilities. So, the third option is to combine them instead of using them individually [10]. Using cryptography, the information can be hidden from the user but it cannot hide the existence of communication.

V. PROPOSED METHOD

The proposed technique is implemented using MATLAB. In this technique, first of all the message is converted to cipher text by RSA cryptographic algorithm. The cipher text is then hidden in the audio content using the LSB audio steganography algorithm. The obtained output audio is used as input audio in the second round of audio steganography. At the receiver end, the cipher text is extracted from the audio cover first [6] by using the decoding algorithm of audio steganography twice. It is then decrypted into the original message using RSA decryption. Hence this method combines the characteristics of both audio steganography and cryptography to provide a higher level of security

.

A. *RSA Algorithm*

i. Key Generation

1. Generate two prime numbers randomly that are large, say, p and q and are approximately of equal size.
2. Calculate

$$n = pq$$

$$phi\ (ö) = (p-1)(q-1)$$

where n is called the modulus.

3. Choose an integer e, where $1 < e < phi$ and e is called the public exponent or encryption exponent. The integer e is chosen such that gcd(e, phi) = 1.
4. Compute the secret exponent d, where $1 < d < phi$. The secret exponent is also called the decryption exponent. It is chosen such that

$$ed \bmod (ö) = 1.$$

5. The public key is (n, e) and the private key is (n, d).

ii. Encryption

Suppose A is sending a message to B, then the encryption process involves the following steps:

1. Obtain the recipient's public key (n,e).
2. Represent the plaintext as a positive integer m, where $1 < m < n$. If the plaintext is a string of characters then each character is converted into its ASCII equivalent to represent it as a positive integer.
3. Compute the cipher text c by using the formula: $c = me \bmod n$
4. Sender that is A, sends the cipher text c to the recipient B.

iii. Decryption

The recipient B, on receiving the message follows the following steps:

1. Recipient B uses his own private key (n, d) to compute the message representative using the formula:

$$m = cd \bmod n$$

2. B then extracts the plaintext from the message representative m. The representative is converted from ASCII to the original message.

B. *LSB Encoding*

i. Encoding

1. The audio file consists of data in bytes.
2. The length of input string is determined.
3. In the original file, the offset from where the encoding process begins is assigned to be 500 by default.
4. Encode that length into the first 8 bytes of the audio file.

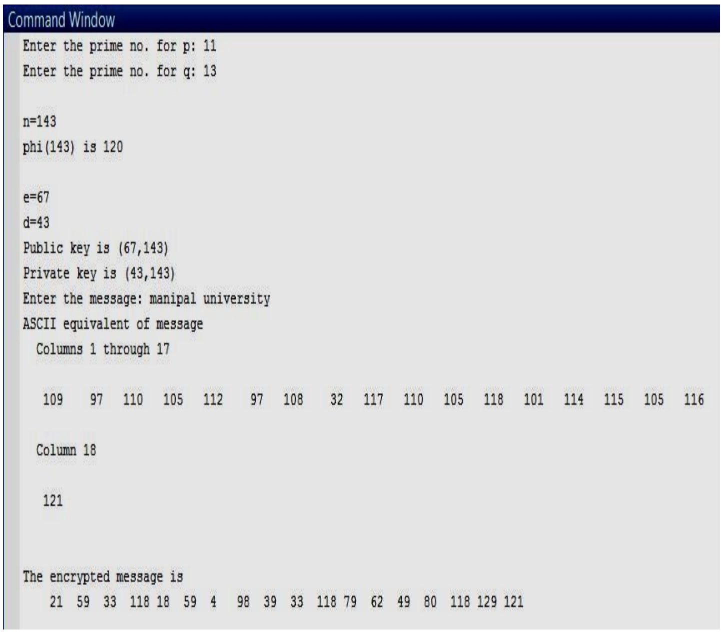
5. Each character from the message is taken to convert it into byte and modify the LSB of the consecutive 8 bytes of the audio file as per each of the bit of the character type.
6. Repeat the above steps for the entire message string.
7. On writing every byte to the new file, a new audio file is obtained where the message is hidden in it and can be directed to the receiver without the fear of eavesdropping.

ii. Decoding

1. The output audio file that has the message hidden is received by the receiver.
2. Start selecting from the offset which was mentioned at the sender's side. Fetch the LSB of next eight bytes to obtain the length of the original message.
3. Make a byte from the left significant byte of the next consecutive eight bytes and keep on storing each of the characters of the string in some variable or array.
4. Carry on with this procedure until the end of the string.

Hence, finally the concealed message from the received audio file is obtained in that array or variable.

VI. RESULTS AND DISCUSSIONS



```
Enter the prime no. for p: 11
Enter the prime no. for q: 13

n=143
phi(143) is 120

e=67
d=43
Public key is (67,143)
Private key is (43,143)
Enter the message: manipal university
ASCII equivalent of message
  Columns 1 through 17

   109    97   110   105   112    97   108    32   117   110   105   118   101   114   115   105   116

  Column 18

   121


The encrypted message is
    21   59   33   118 18   59   4    98   39   33   118 79   62   49   80   118 129 121
```

Fig.1. RSA Encryption Output

Fig 1 shows the the result of the RSA encryption. Here the message entered is **manipal university**. The value of p and q is initially taken as **11** and **13** respectively. Corresponding cipher text obtained from the RSA algorithm is - **109 97 110 105 112 97 108 32 117 110 105 118 114 115 105 116 121**

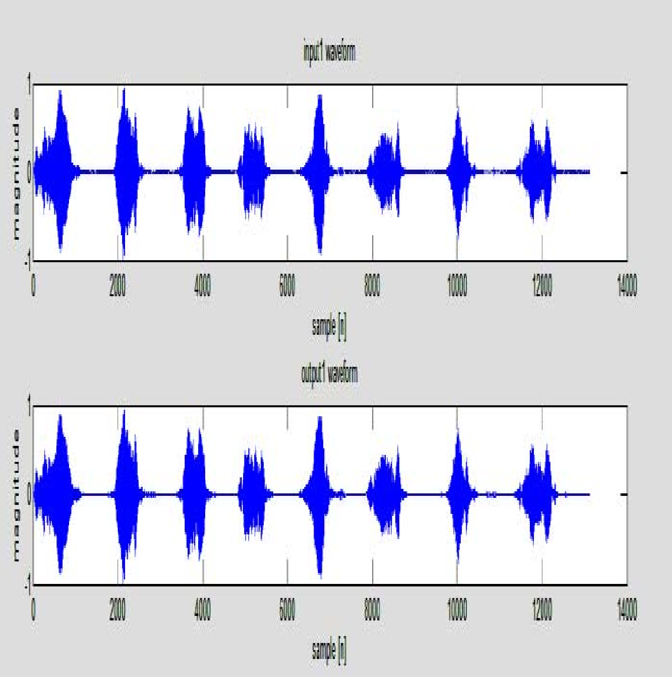


Fig.2. Representation of audio in first audio steganography

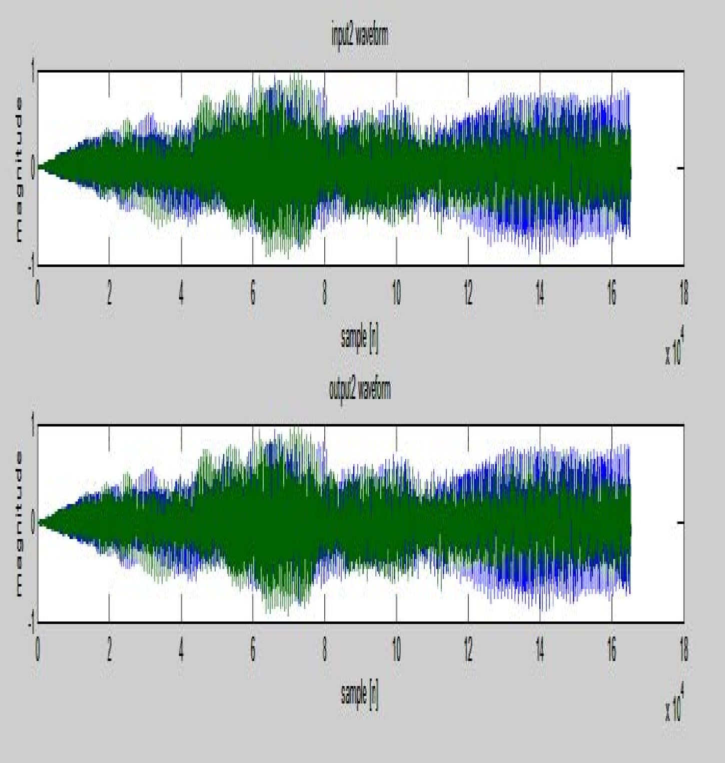
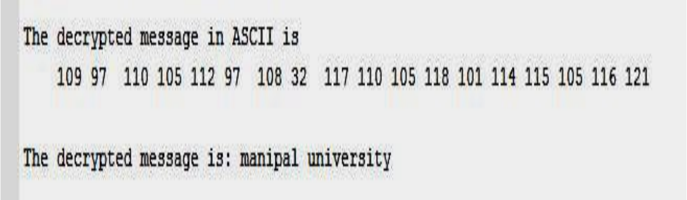


Fig.3. Representation of audio in second audio steganography

The output waveform of first round of steganography is taken as input text for second round of audio steganography. Whereas we have used two different audio files for two different rounds of steganography. From the figures Fig 2 and Fig 3 it can be observed that there is no modification in the corresponding output waveforms for a given input waveform in a single round of audio steganography. This says there will not be any modification in the features of the audio signal even after it is enclosed with data.

The result of RSA decryption is shown in Fig 4.



```
The decrypted message in ASCII is
    109 97  110 105 112 97  108 32  117 110 105 118 101 114 115 105 116 121


The decrypted message is: manipal university
```

Fig.4. RSA Decryption Output

The deciphered message is – **manipal university**

VII. CONCLUSION

Robust algorithms could be developed by integrating two different cryptographic techniques for serving the purpose of preventing cyber-attacks. This algorithm combines the features of both RSA cryptography and two rounds of audio steganography to provide a higher level of security. It can be observed from the result waveforms that input and the output waveforms are identical for a single round of audio steganography. This says there will not be any modification in features of the audio signal even after it is enclosed with data.

REFERENCES

[1] Ankit Gambhir and Sibaram Khara - Integrating RSA Cryptography & Audio Steganography, International Conference on Computing, Communication and Automation (ICCCA2016).

[2] R Joseph and V Sundaram - Cryptography and Steganography- A Survey, IJCTA, vol 2(3), 626-630.

[3] K Harish and Anuradha - Enhanced LSB Technique For Audio Steganography, IEEE 20180, ICCNT‘12.

[4] M. Piyush and M. Paresh - Visual Cryptographic Steganography in Images, IEEE, ICCNT‘10.

[6] S.Usha , K. Satish and K. Boopathybagan - A Secure Triple Level Encryption Method Using Cryptography and Steganography, IEEE, ICCNT‘11.

[7] M. Mishra, G.Tiwari and A. Yadav - Secret Communication using Public key Steganography, IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014),May 09-11,2014.

[8] Behrouz A. Forouzan- Textbook on Data communications & Networking ‘Published by McGraw-Hill Forouzan Networking Series.

[9] Md. Khalid Imam Rahmani, Kamiya Arora and Naina Pal - A Crypto-Steganography: A Survey, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 7, 2014

[10] S. Arfan, S. Kirankumar, U. Vishal and V. Neeraj - Audio Steganography and Security Using Cryptography, IJETAE vol.4, issue 2, Feb 2014.

[11] S. Prakash Chandra, S Ramneet and K. Abhishek, - Enhance Security in Steganography with Cryptography, IJARCCE vol. 3 issue 3, Mar 2014.