

A New Secure Encryption Algorithm Using Combination of Cryptography and Steganography

Payal Gupta, Ravimohan, Sumit Sharma

Department of Electronics and Communication

Shri Ram Institute of Technology, Jabalpur

Madhya Pradesh, India

Abstract: The rapid development of multimedia and internet allows for wide distribution of digital media data. It becomes much easier to edit, modify and duplicate digital information. Besides that, digital documents are also easy to copy and distribute, therefore it will be faced by many threats. It is a big security and privacy issue, it become necessary to find appropriate rotation because of the significance, accuracy and sensitivity of the information. Steganography and Cryptography are considered as one of the techniques which are used to protect the important information, but both techniques have their pro's and con's. This paper aims to conquer their respective drawbacks and to achieve this we are using a double layer protection technique which is cryptography cum steganography approach.

Con's:- limited for mobile devices only, complex hardware, easy to detect cipher patterns.

1.2 Steganography:

It is an ancient art of hiding information. It hides information in digital images.

Pros: Steganography methods reduce the chance of a message being detected.

Cons: Transmitting same images again and again may arouse suspicious-ness to the intruder, easy to decipher ones detected.

Proposed method:

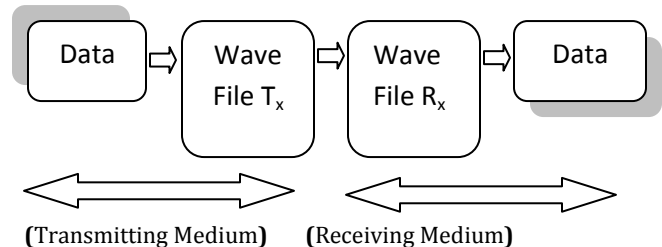


Fig 1.1

As shown above, the data is converted in stegano-object (in this case audio file) and is being transmitted and on the receiving terminal the stegano-object is processed and is converted back into the original data.

1. INTRODUCTION

Information security is essential for confidential data transfer. Steganography is one of the ways used for secure transmission of confidential information. Hiding information in a photograph is less suspicious than communicating an encrypted file.

The main purpose of steganography is to convey the information secretly by concealing the very existence of information in some other medium such as image, audio or video.

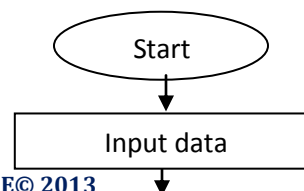
1.1. -Cryptography:

Cryptography scrambles messages so it can't be understood.

Modulo encryption is a popular data hiding technique in mobile devices.

Pro's: - secure data, variable bit key for data hiding, fast and flexible easy to implement.

1.3 Process flow of transmitter



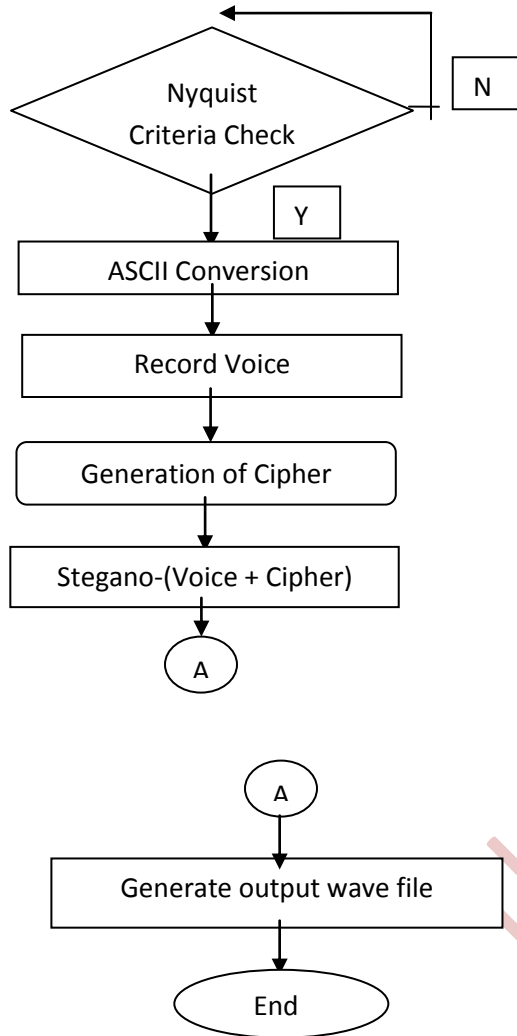


Fig. 1.2

In the above fig. it can be depicted that the data is entered by the user. Then the sampling rate is being entered by the user. Now the sampling rate entered by the user is being compared with the Nyquist rate. If the sampling rate entered by the user is greater than Nyquist rate then next step is followed else previous step is repeated. Then this step is followed by ASCII conversion in which the data is converted in ASCII format. Now the input is given by the user which is in the form of voice. This step is followed by generation of cipher. In the following step stegano-object (i.e. voice generated by the user) and the cipher so generated are combined and the output wave is being generated.

1.4 Process flow of receiver

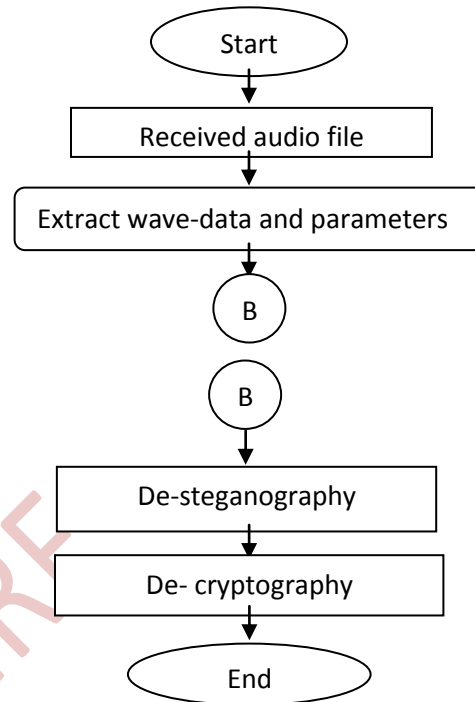


Fig. 1.3

Fig. 1.3 represents data flow of the receiver. At the receiving terminal audio file is received. Then wave-data and parameters are extracted. These parameters include length of data, frequency and step size. As shown in the next step De-steganography is performed in which voice and data cipher are being extracted. Now to convert cipher into data, de-cryptography is performed in which data is obtained in its original form.

Algorithm used for cryptography:

1. Get the data from the user(Data)
2. Transpose the given data to obtain a transposed matrix(Tdata)
 $Tdata = \text{transpose}(\text{data})$
3. Divide the Tdata by any numerical value say '200'
 $M = Tdata / 200$
4. The 'Cipher' so generated can be obtained by calculating the modulo
 $Cipher = M \% 256$

Algorithm used for steganography:

1. 'X' represents ciphered data
2. 'W' represents wave signal
3. 'Y' represents wave sound stegano-object
4. Then

$$Y = [W_0(\text{---}),x(0), W_1(\text{---}),x(1), W_2(\text{---}),x(2), W_3(\text{---}),x(3),\text{-----}]$$
5. The range of block of 'W' is decided at run time as per size of 'X'

Simulation Results:

The fig. 1.4 illustrated below represents the pictorial view on the data being transmitted (Transmitter section).

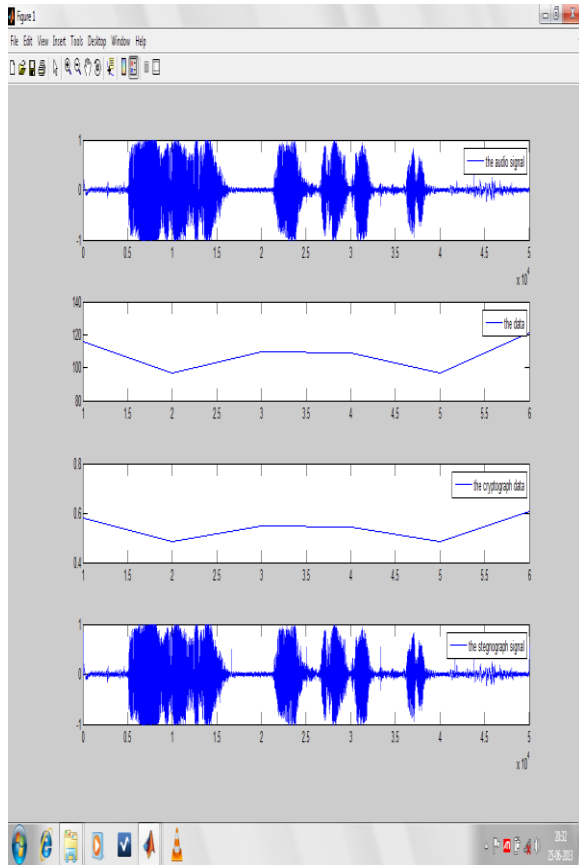


Fig. 1.4

The first part of the fig.1.4 represents the audio signal which has been taken into consideration for the transmission.

The second part of the fig.1.4 represents the data which has to be transmitted over the given channel.

The third part of the fig.1.4 represents the encrypted data or the so called 'cipher' which has been generated by the algorithm used for cryptography.

The fourth part of the fig.1.4 represents the combination of the audio signal and the cipher and the combination of the above is called stegano-object.

The fig. 1.5 illustrated below represents the pictorial view on the data being received (Receiver section).

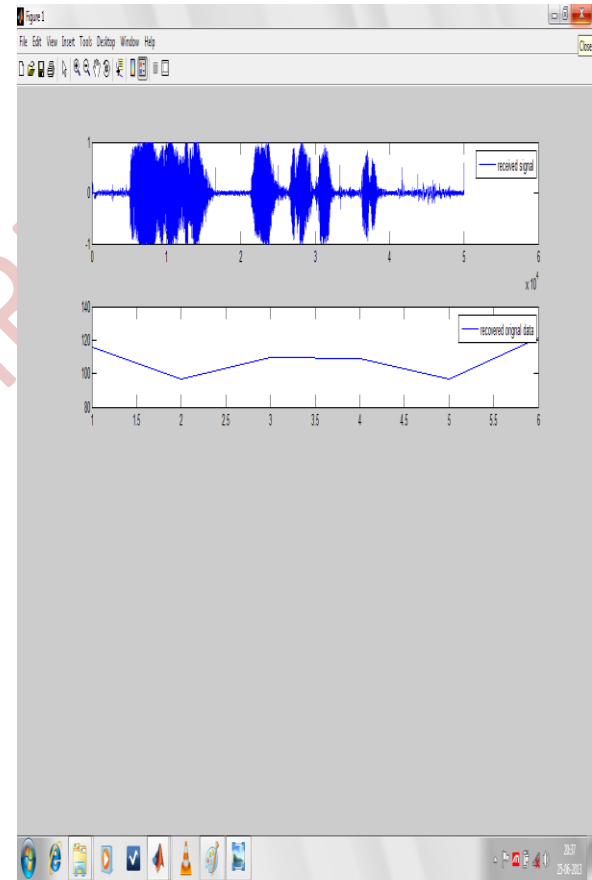


Fig. 1.5

First part of the fig 1.5 displays the received signal which has been received from the transmitter.

The second part of the fig.1.5 represents the original recovered data received by the receiver.

From fig 1.4 and fig. 1.5 it can be seen that both in transmitter and receiver recovered data is same.

Conclusions

Both the cryptography and steganography have their own respective pros and cons, but the combination of both the model provides better protection of the data from the intruders.

References:

[1] Debnath Bhattacharyya, Poulami Das, Samir Kumar Bandyopadhyay and Tai-hoon Kim, Text Steganography: A Novel Approach, *Research paper*, International Journal of Advanced Science and Technology, Vol. 3, February, 2009

[2] Arvind Kumar, Km. Pooja, Steganography- A Data Hiding Technique, *Research paper*, International Journal of Computer Applications (0975 - 8887) Volume 9- No.7, November 2010

[3] Zaidoon Kh. AL-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan.O.Alanazi, Overview: Main Fundamentals for Steganography, JOURNAL OF COMPUTING, VOLUME 2, ISSUE 3, MARCH 2010

[4] Ross J. Anderson, Fabien A.P. Petitcolas, On The Limits of Steganography, *IEEE Journal*, May 1998

[5] Miroslav Dobs'cek, Modern Steganography, Czech Technical University in Prague