A Proposed Algorithm for Securing Signal-Encryption using Cryptography and Steganography

Sudipto Dhar
Department of Computer
Science and Engineering
Budge Budge
Institute of Technology

ABSTRACT
In this era of digital transmission, security of information is crucial. Steganography and cryptography helps in providing this much needed data confidentiality. Steganography hides secret information into a cover medium and cryptography converts data into an unrecognizable form. For more secure communication RSA algorithm is been introduced, which is based on asymmetric key cryptography.By using Steganography methods third parties cannot percept the existence of message embedded in the audio file. The properties of the audio file remain the same after hiding the secret message. In this Paper a new-fangled substitution method (Discussed in Proposed Method section) for Steganography has been used with RSA Cryptosystem.

General Terms
Security, Proposed Algorithm et al.

Keywords
Cryptography, RSA, Steganography, Audio.

1. INTRODUCTION
Research by the signal Security community has given birth to a rich variety of signal recording, storage, processing, analysis, retrieval, and display techniques. Signal processing applications are found in many field.

In Digital transmission there are two types of security technique exist, i) Cryptography ii) Steganography. Steganography is not the same as cryptography unlike, data hiding techniques have been widely used to transmit

of hiding secret message for long time. Cryptography is used to encrypt the data by Keys so that it is unreadable by a third party. In this very approach, both of these two for giving more security to the signal has been introduced.

In this paper an Audio file taken as cover media and another Audio file as the secret message. Here, message signal is encrypted by RSA algorithm and then using a cover media to hide that cipher message into it by new proposed algorithm. Firstly, this method is very hard to be cracked, as well it is much easier to implement than LSB Substitution Steganography method.

2. PREVIOUS WORK
Valarmathi et al. [1], this paper mentioned two level encryption method (cryptography and steganography). The main disadvantage is that, the symmetric key cryptography is used which is very much easy to be cracked than asymmetric key cryptography. Arfan Shaikh et al. [2] revealed again the two level encryption techniques. Here also RSA encryption technique is used to give more security than symmetric key cryptography, but here multiple LSB substitution method is used so that there is some complication to retrieve the secret message back.Nishith Sinha et. al. [3] used amalgamated approach of cryptography which is not much secure because here only transposition of data is made so that information is there already so it can easily be cracked and also they have used LSB Substitution method which is a well known method in steganography. Khalil Challita et al.[4] ,in this paper author tries to focus to give new insights and directions on how to improve existing methods of hiding secret messages, possibly by combining steganography and cryptography.

So it is been observed that to secure the secret message more we have to use two level encryption i.e. cryptography and steganography simultaneously than that to be implemented either in cryptography or steganography, So RSA cryptosystem is used in this paper which is an asymmetric cryptography which is more secure than symmetric key cryptography and also a new method of steganography is proposed in place of some well known methods (like LSB substitution etc.).

3. PROPOSED METHOD
3.1 Theoretical Background
The system contains Sender Side and Receiver Side. Sender will send an Information as Audio Signal to Receiver. Here the show up of the work focuses on securing that Signal by means of Cryptography and Steganography.

- **Encryption Part**

At First, an audio file (.WAV Format) is taken in Native

format (W). It is been stored in an array.

Let the value of 1st location of array is 127. Now Encrypt this value using RSA algorithm using public key, Now, say the new value is 67 after encryption. Convert 67 in 16 bit Binary value.

$\mathbf{W_{CB}= (0000000001000011)_2}$

Now, Take the Cover File as Audio then convert it to Native Format.It also been stored to another array. Let there, the value of 1st location of array is 123. Now convert it to 16 bit Binary Value

$\mathbf{C_B = (0000000001111011)_2}$

Subsequently calculate $Es = W_{CB} \oplus C_B$

0000000001000011

$\oplus$ **0000000001111011**

0000000000111000

So, Es = $(0000000000111000)_2$

Then Covert $(0000000000111000)_2$ **to** $(56)_{10}$.

Afterward keep 127 in 1st location intact and 28 in the 2nd (i.e. consecutive) location. In this way I traversed all the native values of Secret Message from the array. Finally remodification of the cover file need to be done. If cover message is in i^{th} location then encrypted message value will be kept in $(i+1)^{th}$ location. So if the size of secret message is n then the size of cover file must be of 2*n.

Finally that Cover message will be sent as audio.

The above procedure is been described in the following figure (fig.1)

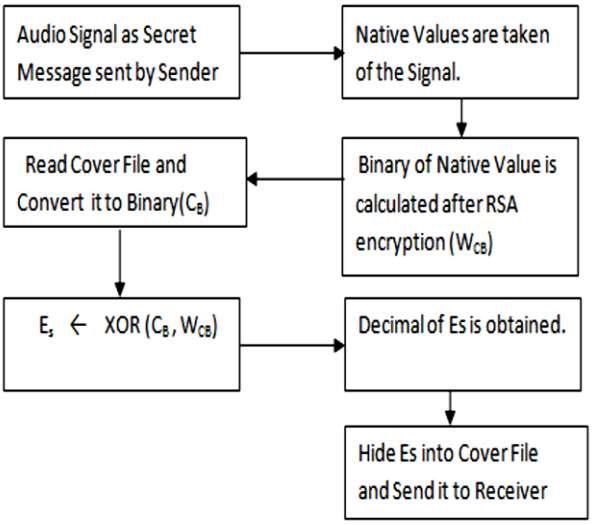

Fig.1 (Encryption)

- **Decryption Part**

At First ,the encrypted (.WAV) is taken from the Sender in Native format (W) in an array. First location array value is 123 in the cover message, and in very next bit encrypted value is fetched as 56.Using both of these two values we can easily get the secret message. i.e.

C_B = **(0000000001111011)**
Es = **(0000000000111000)**

0000000001111011
⊕ **0000000000111000**

0000000001000011

$W_{CB} = (0000000001000011)_2$

Convert it to the Decimal i.e. 67

W_C = 67(which is the encrypted value)

Now, Decryption by Private key using RSA algorithm we can get the original secret message i.e. 127.

The above procedure is been described in the following figure (fig.2)

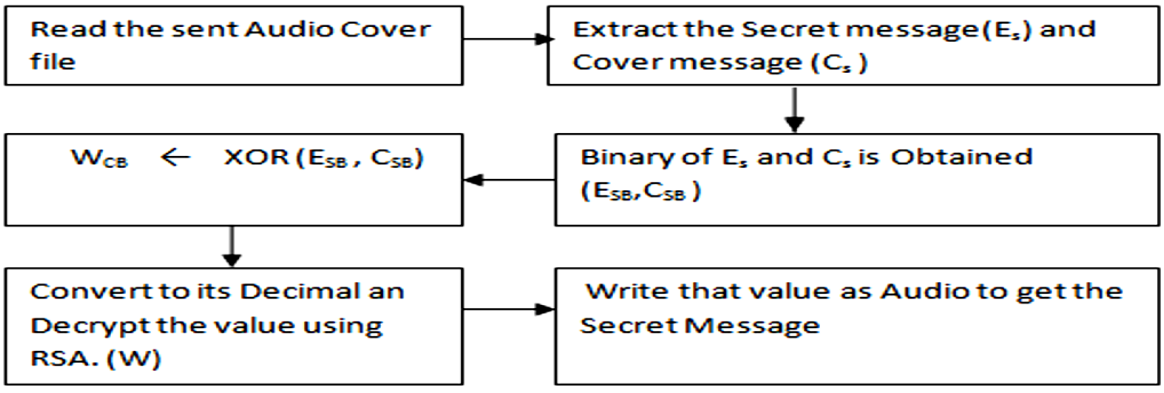

Fig.2 (Decryption)

3.2 Algorithm for Encryption

INPUT: Source (.WAV) Audio Signal.
OUTPUT: Cover File (CN) with source Audio File.

BEGIN
1. Read the Signal (.WAV) in Native Format (W).
2. Encrypt the Signal(W) using RSA Algorithm
Enc (W, PUK) $\xrightarrow{RSA}$ S_{WC}
//S_{WC} is the cipher signal of W & PUK is the Public key
3. Read S_{WC} in Native format.
4. For all (Native(S_{WC})) do
S_{WC} $\xrightarrow[16\ bit]{}$ Binary(S_{WC})
= S_{WCB} // S_{WC} is the Binary equivalent
Count=Count+1
End loop
5. Read the Cover File Signal (.WAV) in Native Format (C).
6. For i =1 to (2*Count) do
C[i] $\xrightarrow{16\ bit}$ C_B // C_B is the Binary equivalent
E_s $\xleftarrow{}$ XOR(S_{WCB}[i], C_B[i])
// E_s is the encrypted Binary XORed Value.
7. Convert $_{Es}$ into its Decimal of Es (DE_s).
8. C [i+1] $\xleftarrow{}$ DEs
i=i+2
go to step 8
9. Send the New Cover File C to Receiver.
END

3.3 Algorithm for Decryption

INPUT: Cover File (C) with source Audio File.

OUTPUT: Source (.WAV) Audio Signal.

BEGIN

1. For i =1 to (2*Count) do

S_{WCB} $\xleftarrow[16\ bit]{}$ XOR(C[i] , Decimal(C[i+1])

i=i+2

go to step 1

2. Convert S_{WCB} to Decimal // S_{WCB} is in Binary

S_{WCB} $\longrightarrow$ Decimal(S_{WCB})

= S_{WC}

3. Decrypt the Cipher Signal (S_{wc}) using RSA Algorithm

Enc ($W_{wc,}$ PRK) $\xrightarrow{RSA}$ W

//W is the message Signal & PRK is the Private Key of the Receiver.

END

4. CONCLUSION AND FUTURE WORK

As discussed earlier, security of information over the internet is becoming a major concern. In this paper two level of security is been introduced.RSA cryptosystem is very well known Asymmetric key cryptosystem, it is used here for giving a shield to the information and the proposed method of steganography is used to hide the information in a way that for any unauthorized person it is hardly accessible.

As a part of future work, it is recommended more secure encryption algorithms to be utilized for text encryption. Further, different steganographic techniques can also be used. This proposed algorithm can be modified also for giving more security to the secret message. Here the cover file size must be near twice of the secret file, so that thing should have some flexibility in the future work.

5. REFERENCES

[1] R.Valarmathi, G.M.Kadhar Nawaz, "Information Hiding Using Audio Steganography with Encrypted Data", in International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 1, January 2014, ISSN (Online) : 2278-1021.

[2] Arfan Shaikh, Kirankumar Solanki, Vishal Uttekar, Neeraj Vishwakarma, " Audio Steganography And Security Using Cryptography", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 2, February 2014.

[3] Nishith Sinha, Anirban Bhowmick, B.Kishore," Encrypted Information Hiding using Audio Steganography and Audio Cryptography", International Journal of Computer Applications (0975 – 8887) Volume 112 No. 5, February 2015

[4] Khalil Challita and Hikmat Farhat," Combining Steganography and Cryptography: New Directions", International Journal on New Computer Architectures and Their Applications (IJNCAA) 1(1): 199-208,The Society of Digital Information and Wireless Communications, 2011 (ISSN 2220-9085).

[5] S Usha G A Sathish Kumal, K Boopathybagan," 2011 International Conference on Computer Science and Network Technology".

[6] Ajit Singh, Swati Malik," International Journal of Advanced Research in Computer Science and Software Engineering", Volume 3, Issue 5, May 2013 ISSN: 2277 128X.

[7] Meenakshiv Shankar, Akshaya.P, "Hybrid Cyptographic Technique Using RSA Algorithm And Scheduling Concepts", in International Journal of Network Security & Its Applications (IJNSA) Vol.6, No.6, November 2014.

[8] Amrita Jain, Vivek Kapoor," Secure Communication using RSA Algorithm for Network Environment", International Journal of Computer Applications (0975 – 8887) Volume 118 – No. 7, May 2015.

[9] Saleh Saraireh," A Secure Data CommunicationSystem Using Cryptography And Steganography", International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.3, May 2013.

[10] Aarti Mehndiratta," Data Hiding System Using Cryptography & Steganography: A Comprehensive Modern Investigation", International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 Volume: 02 Issue: 01 Apr-2015.

[11] Lokesh Kumar," Novel Security Scheme for Image Steganography using Cryptography technique", International Journal of Advanced Research in Computer Science and Software Engineering , Volume 2, Issue 4, April 2012 ISSN: 2277 128X.

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

[13] Jayaram P, Ranganatha H R, Anupama H S," Information Hiding Using Audio Steganography – A Survey", The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011.

[14] Unik Lokhande,A.K.Gulve,"Steganography using Cryptography and Pseudo Random Numbers", International Journal of Computer Applications (0975 – 8887) Volume 96– No.19, June 2014.

[15] Hayfaa Abdulzahra,Robiah Ahmad, Norliza Mohd Noor ," Combining Cryptography and SteganographyFor Data Hiding in Images", ISBN: 978-960-474-368-1

[16] Prof. Samir Kumar Bandyopadhyay, Barnali Gupta Banik," LSB Modification and Phase Encoding Technique of Audio Steganography Revisited", International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 4, June 2012, ISSN : 2278 – 1021.