ENHANCING SECURE COMMUNICATION USING COMBINED CRYPTOGRAPHY AND STEGANOGRAPHY

Linu Tony[1], Rosminna Paulson[2], Lini P M[3], Roshni R Menon[4]
[1,2,3] Computer Science and Engineering, Sahrdaya College of Engineering, Thrissur, India
[4]Asst. Professor, Computer Science department, Sahrdaya College Of Engineering & Technology, Thrissur, India

Abstract
Security protocols are essential for communication over digital media and Internet. From ancient days to present,different techniques have been adopted to communicate secret messages. To provide secure communication, sender and receiver should exercise an efficient technique to convert original message to an unintelligible format to everyone except the intended receiver. Cryptography and Steganography are two popular techniques to provide secure communication, where Cryptography distorts the message and Steganography hide the existence of the message. By combining the strength of Cryptography and Steganography into a single system, security of secret communication can be enhanced. In this project, the strength of cryptosystems and audio steganography are utilized as a single system for enhancing security of secret information

Index Terms: Steganography, Cryptography, RSA, Echo hiding .

I. INTRODUCTION

Security protocols are a must for the secret communication between two parties. Now a days we need secrecy in all the electronic communication areas like personal communication, military purposes, financial transactions, electronic banking, medical diagnosis etc. To attain security in these communications, the commonly used techniques are Cryptography and Steganography.

Cryptography ensure the security by encrypting the plain text into 'Cipher text' form by using cryptographic algorithms and secret keys. The cipher text is send from sender to receiver side. Unauthorized user cannot understand the actual plain text message from cipher text without knowing the secret keys. At the receiver's side, by using decryption algorithm and secret keys the receiver decrypts the cipher text and obtains the plain text/secret message. Steganography ensure the security of secrets by hiding them within the cover files. So messages cannot be seen by the unauthorized user. Steganographic algorithm embeds the plain text into the cover files and obtains the 'Stego files'. These stego files are sending from the sender to the receiver. The authorized receiver knows that the secret is present in the stego file and he can extract the actual message from stego file using proper steganographic algorithms and secret keys.

In this project, the features of Cryptography and Steganography are utilized as a single system. The main areas involved in this system are Cryptographic algorithms and Manipulation of cipher text. These two areas should be managed properly by an efficient cryptosystem. One of the most popular and classical cryptosystem is RSA cryptosystem. There are number of variants of RSA cryptosystem, we find out some of them and list out their properties and limitations. Finally most of these limitations can be resolved using an algorithm which uses Jordan's Totient function for the computations.

II. EXISTING TECHNIQUE

Increase in the number of attack recorded during electronic exchange of information between the source and intended destination has indeed called for a more robust method for

securing data transfer. Cryptography and steganography are well known and widely used techniques that manipulate information in order to cipher or hide their existence. Several techniques have been proposed by researchers for securing electronic communication. Initially, the cryptography and steganography methods were used separately. Widely used steganography technique was image steganography. Here the data will be hidden within the image. Similarly, the commonly used cryptographic method is LSB. This algorithm replaces the least significant bit in some bytes of the cover file to hide a sequence of bytes containing the hidden data.

Then combined cryptography – steganography methods came into existence. These two techniques share the common goals and services of protecting the confidentiality, integrity and availability of information from unauthorized access. A data hiding system that is based on audio steganography and cryptography is in existence that secure data transfer between the source and destination. Audio medium is used for the steganography and a LSB algorithm is employed to encode the message inside the audio file.

The limitation of this system is that in addition to low robustness, it is not immune to manipulation. Messages can be extracted easily. Also LSB is the most commonly used steganography method .

III. THE PROPOSED WORK

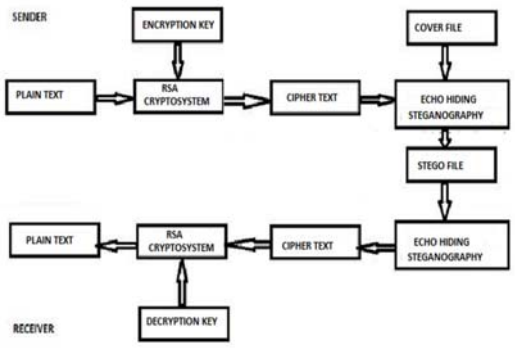
Security protocols are a must for the secret communication between two parties. Now a days we need secrecy in all the electronic communication areas like personal communication, military purposes, financial transactions, electronic banking, medical diagnosis etc. To attain security in these communications, the commonly used techniques are Cryptography and Steganography.

Cryptography ensure the security by encrypting the plain text into 'Cipher text' form by using cryptographic algorithms and secret keys. The cipher text is send from sender to receiver side. Unauthorized user cannot understand the actual plain text message from cipher text without knowing the secret keys. At the receiver's side, by using decryption algorithm and secret keys the receiver decrypts the cipher text and obtains the plain text/secret message. Steganography ensure the security of secrets by hiding them within the cover files. So messages cannot be seen by the unauthorized user. Steganographic algorithm embeds the plain text into the cover files and obtains the 'Stego files'. These stego files are sending from the sender to the receiver. The authorized receiver knows that the secret is present in the stego file and he can extract the actual message from stego file using proper steganographic algorithms and secret keys.

In this project, the features of Cryptography and Steganography are utilized as a single system. The main areas involved in this system are Cryptographic algorithms and Manipulation of cipher text. These two areas should be managed properly by an efficient cryptosystem. One of the most popular and classical cryptosystem is RSA cryptosystem. There are number of variants of RSA cryptosystem,we find out some of them and list out their properties and limitations. Finally most of these limitations can be resolved using an algorithm which uses Jordan's Totient function for the computations.

IV. METHODOLOGY

The overall design of the proposed system can be depicted as shown in Figure. Here plain text is encrypted using RSA cryptosystem and the obtained cipher text is processed with the steganographic module. Steganographic module takes cipher text and audio file as its inputs and embeds the cipher text into cover file using echo hiding steganography. Then, the obtained stego file is send to the receiver. Receiver extracts the stego file into cipher text and cover audio file. The cipher text is decrypted using the decryption algorithm of RSA cryptosystem and private key of the receiver. The entire system consists of Cryptographic module and Steganographic module.



a. Cryptographic Module

Cryptographic module shows the overall design of the RSA cryptosystem using Jordan totient function and it consists of following components.

1 Jordan's Totient Function computing: This module computes the value of Jordan's Totient function based on the user input. In this stage user input are set of prime numbers and the generalizing index of Generalized RSA cryptosystem. The generated value is required for all the sub modules such as Key generator, Encryptor, and Decryptor.

o JK (N) = NK ∏P/n (1 – P − K) Where K, N are positive integers

2 Key Generator: Key Generator is the module which generates the public key and private key for decryption and encryption. Select a random integer E such that, o gcd (E, JK(N)) = 1, where 1 < $E < JK\ (N)$, E = M mod JK(N)

Select integer D such that, ED = 1 (mod JK (N)) i.e.,

o D = E − 1 mod JK (N) where 1 < D < JK (N)

3 Encryption: Encryption module performs the encoding of plain text with public key. Output of encryption process is the cipher text. This cipher text is in unreadable form and Decryption process is required to make it readable. Given a public-key (JK (N);E) and a message M compute the cipher text

o C = M ∗ E mod JK(N)

4 Decryption: Decryption module performs the decoding of cipher text with private key. Only the intended receiver can decrypt the cipher into readable plain text. Given a private-key (JK (N), D) and cipher text C, compute the message o M = C ∗ D mod JK (N)

5 Numerical assignment: This module assigns the numerical values to the characters. Since the public key cryptography is based on the mathematical functions, it is necessary to assign numerical values to characters before encryption.

6 Inverse Numerical assignment: This module performs the inverse mapping of numerical to character assignment. It is necessary after the decryption.

b. Steganographic Module

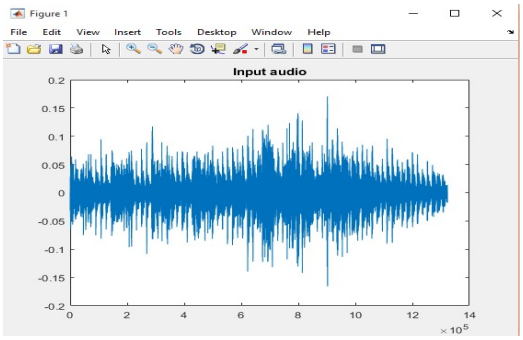
After the encryption process the generated cipher text is in text format. Even though its syntax and semantics are different from the natural languages, the intruder can assume the presence of something secret in cipher text and he can try for the actual message. Here we use the assumption that hiding data is better than sending it as shown as encrypted. So we use echo hiding steganography for data hiding. This algorithm is an enhanced version of LSB technique. Since the original LSB which is quite vulnerable, most common and well known method, hackers can easily try this method to retrieve the message.

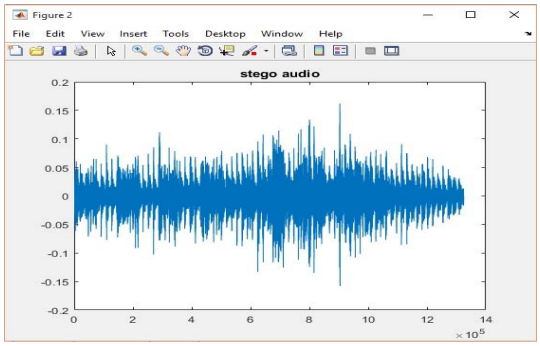
Echo hiding method embeds data into audio signals by introducing a short echo to the host signal. The nature of the echo is a resonance added to the host audio. Therefore, the problem of the HAS sensitivity to the additive noise is avoided. After the echo has been added, the stego signal retains the same statistical and perceptual characteristics. The primary objective of steganography is to avoid drawing attention to the transmission of hidden information. If any attacker or hacker noted any changes in the stego file, then he can try for the inner contents. So the quality degradation of stego file should be prevented.

V. RESULT AND CONCLUSION

The entire system consists of Cryptographic module and Steganographic module. Cryptography distorts the message and Steganography hide the existence of the message. Here we expect to provide secure communication. Sender and receiver should exercise an efficient technique to convert original plain text message to an unintelligible format to everyone except the intended receiver. Here plain text is encrypted using RSA cryptosystem and the obtained cipher text is processed with the steganographic module.

Steganographic module takes cipher text and a audio co file as inputs and embeds the cipher text into cover file using echo hiding steganography. Then, the obtained stego file is send to the receiver. Receiver extracts the stego file into cipher text and cover audio file. The cipher text is decrypted using the decryption algorithm of RSA cryptosystem and private key of the receiver.





Combining Cryptography and Steganography in communication can enhance the security. RSA along with Jordan Totient Function reduces the requirements of RSA cryptosystem such as the requirement exponential computations for encryption and decryption. For the same set of prime numbers, it provides better key size and message space size than the conventional RSA. It is faster than RSA in the case of encryption and decryption. By combining Cryptography and Steganography and utilizing their features in the combined manner we can enhance the security of secret data communication. The work done in this project provides basis for future research in steganography and can be extended in several ways. One possible extension is to use cover video files for echo hiding steganography without degrading the quality of video. The possibility and the impact of such work needs to be investigated.

REFERENCES

[1] Amandeep kaur Singh , Satveer Singh Computer Engineering Punjabi University Patiala, Punjab, India , A Hybrid Technique of Cryptography and Watermarking for Data Encryption and Decryption 2016 fourth international conference on PDGC.

[2] Jayaram, P., Ranganatha, H. R. and Anupama, H. S. 2011. Information Hiding Using Audio Steganography – ASurvey. International Journal of Multimedia and Its Application, 3(3), pp. 86-96.

[3] 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)

[4] R.L. Rivest, A. Shamir, and L. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

[5] M.Saritha , India Vishwanath.M.Khadabadi., Sushravya.M Dept of Electronics & Communication Engineering Jain College of Engineering,Belagavi, Karnataka , India Image and Text Steganography withCryptography using MATLAB , International conference on Signal Processing, Communication, Power and Embedded System (SCOPES)-2016

[6] S. Thajoddin and S. Vangipuram, A Note On Jordans Totient function, Indian j. pure appl. Math December 1988

[7] Suresh K and Venkataramana.K, Study of Analysis on RSA and its Variants, International Journal of Computer Science Research & Technology (IJCSR),Vol. 1 Issue 4, September2013.

[8] E.Madhusudhana Reddy, B. Muneendra Nayak and M.Padmavathamma, Communication between two Parties using MJ2 -RSA Cryptosystem and Signature Scheme, IEEE CONECCT 2013

[9] Audio Steganography Rohit Tanwar IT Department, ManavRachna College ofEngg, Faridabad, India Audio Steganography 2014 International Conference on Reliability, Optimization and Information Technology -ICROIT 2014, India, Feb 6-8 2014

[10] Chi-Kwong Chan and L M Cheng, Hiding data in images by simple LSB Substitution, The Journal of the Pattern Recognition Society

[11] H. Wu, H. Wang, C. Tsai and C. Wang, Reversible image steganographic scheme via predictive coding, Reversible image steganographic scheme via predictive coding 1 (2010), ISSN: 01419382, 35-43

[12] Vipul Sharma and Sunny Kumar, A New Approach to Hide Text in Images Using Steganography, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 2013

[13] Comparative study of digital audio steganography techniques Fatiha Djebbar1*, Beghdad Ayad2, Karim Abed Meraim3 and Habib Hamam4 SPRINGER.