International Journal of Innovations & Advancement in Computer Science
IJIACS
ISSN 2347 – 8616
Volume 4, Special Issue
May 2015

Crypticsteganography
A New Data Hiding Technique with Multilayer Security System.

Ankit Gambhir
M.tech Scholar
Galgotias University

Anant Raj Mishra
M.tech Scholar
Galgotias University

ABSTRACT

Information security plays an essential role during internet communication in today's era of technology. It is enormously important for people committing e-transactions like online shopping, money transfer etc. There are various methods that provide a means for secure commerce and payment to private communications and protecting passwords. Cryptography and Steganography are such methods. The principle of cryptography is to manipulate the information so that unintended receiver will not be able to understand however the principle of steganography is to mask the very presence of communication; it hides the existence of message. Both the techniques are widely used to prevent unintended receiver's attacks from unauthorized access. This paper proposes a new technique that provides multilayer security by integrating cryptography with steganography.

Keywords: Cryptography, Steganography, Information Security, Unintended Receiver

INTRODUCTION

In today's era the enormous use of internet for communication has increased the attacks to users hence security of data is a significant issue related to privacy as well as safety during communication. Cryptography and Steganography are two techniques that help in sending vital information in a secret way. Cryptography manipulates the information so that unintended receiver will not be able to understand. It scrambles the information by converting message in cipher text where as steganography mask the very presence of communication; it hides message under some media like image, audio and video. Cryptography [1] defines as the art and science of transforming data into a sequence of bits that appears as random and meaningless to a side observer or attacker. It comes from Greek words; crypto (secret) and graphy (writing or drawing) [2]. Cryptanalysis [3] is the reverse engineering of cryptography—attempts to identify weaknesses of various cryptographic algorithms and their implementations to exploit them. The process of converting message (plain text) into unreadable form (cipher text) is called encryption and the reverse process is called decryption. Steganography [2] also comes from the Greek steganos (covered) and graphy (writing or drawing). Steganography [1] can be defined as the hiding of information by embedding messages within other, seemingly harmless messages, graphics or sounds. The first steganographic technique was developed in ancient Greece around 440 B.C. The Greek ruler Histaeus employed an early version of steganography which involved: shaving the head of a slave, tattooing the message on the slaves scalp, waiting for the growth of hair to disclose the secret message, and sending the slave on his way to deliver the message. The recipient would have the slave's head to uncover the message. The recipient would reply in the same form of steganography [1].

PREVIOUS WORK

Different methods are used to hide message in media such as image steganography, audio steganography and video steganography, depending on the type of cover file used. However there are very less papers available that present multilayer security using both cryptography and steganography.

In this research paper, combination of both the techniques is presented. Audio steganography is used but prior to that, message is encrypted by RSA algorithm to make communication more secure and immune to unauthorized access.

PROPOSED TECHNIQUE

Although cryptography and steganography techniques are separately used to secure data but still there is a requirement of technique that provide more level of security. Crypticsteganography is such a technique that provides multilayer security by merging cryptography with steganography. In this proposed system first message is converted into cipher text by RSA algorithm and then cipher text is hidden in audio using LSB audio steganography technique similarly at reception first cipher text is reveal from audio thereafter it decrypted into message by using RSA decryption. So this technique combines the features of both cryptography and steganography and provides a higher level of security. It is better than either of the technique used separately.

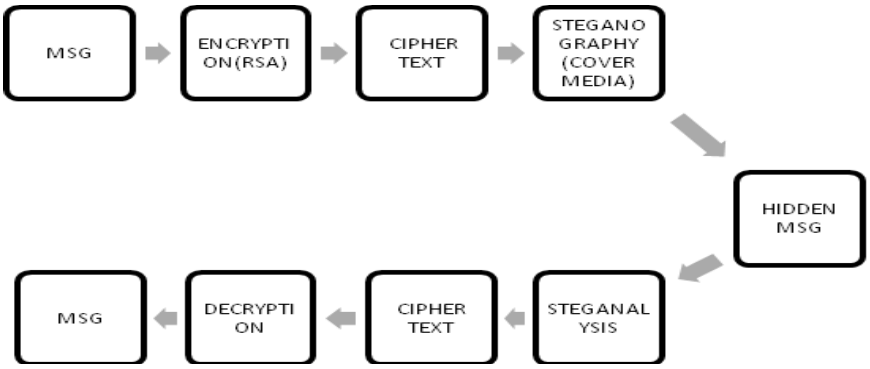

Fig: Block diagram

ALGORITHM

Sender’s end

Step 1: Select the message that has to be sent.

Step 2: Encrypt the message by using RSA algorithm.

Step 3: For RSA algorithm;

a) Choose two large prime numbers P and Q (say) such that P is not equal to Q.

b) Calculate N, by multiplying P and Q; N=P*Q.

c) Now calculate T by formula; T= (P-1)*(Q-1).

d) Select a public key E such that E is not the factor of T.

e) Next is to select the private key D such that (D*E) modT=1.

f) To calculate cipher text (C): $C=M^{E}\text{mod}N$.

Step 4: Convert cipher text into binary form.

Step 5: Read the audio file in binary.

Step 6: Sampled the binary audio file into 8 bit equal size samples.

Step 7: Embed the cipher text in audio file by least significant bit coding.

Step 8: Send this audio to receiver.

Receiver’s end

Step 9: Read the audio file in binary form.

Step 10: Store the values of least significant bits.

Step 11: Convert the binary values into decimal form to get cipher text.
Step 12: To calculate message (plain text) (M): $M=C^{D}\text{mod}N$ (RSA Decryption).

CONCLUSION AND FUTURE SCOPE

Security has always been an important issue in communication. Crypticsteganography combines the features of both steganography and cryptography, and provides a high level of security. It satisfies the requirement of high security and robustness between sender and receiver. The steganalysis of this technique by unintended receiver is more challenging so this method can be used in areas where highly sensitive data is to transfer through network such as Banks, RAW agencies etc. There is a wide scope of future work in this proposed method such as a new algorithm can de design by modifying RSA, DES or AES cryptographic algorithm, modification can also be done in least significant bit embedding technique.

ACKNOLEDGEMENT

We would like to express our deepest thanks to Dr Sibaram Khara, Dean Academics Galgotias University, for his esteemed guidance and expert contribution to this paper.

References

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

[2] Liddell and Scott's Greek- English Oxford University Press.

[4] Robert krenn, 'Steganography and Steganalysis', an article Jan 2004.

[5] Aung Pye Pye and Naing Min Tun, 'A Novel Secure Combination Technique of Steganography and Cryptography' IJITMC vol.2, no.1, Feb 2014.

[6] Kumar Harish and Anuradha, 'Enhanced LSB Technique For Audio Steganography', IEEE 20180, ICCNT'12.

[7] Marwaha Piyush and Marwaha Paresh, 'Visual Cryptographic Steganography in Images' IEEE, ICCNT'10.

[8] Usha S, Kumar Satish and Boopathybagan K, 'A Secure Triple Level Encryption Method Using Cryptography and Steganography' IEEE, ICCNT'11.

[9] Kumar Manoj, Upadhyaya Amit and Agarwal Shalini, 'Adaptive Steganographic Algorithm Using Cryptographic Encryption RSA Algorithms' JEC&AS vol 2, no.1 Jan 2013.

[10] Sheikh Arfan, Solanki Kirankumar, Uttekar Vishal and Vishwakarma Neeraj, 'Audio Steganography and Security Using Cryptography' IJETAE vol.4, issue 2, Feb 2014.

[11] Shukla Prakash Chandra, Chadha S Ramneet and Kumar Abhishek, 'Enhance Security in Steganography with Cryptography' IJARCCE vol. 3 issue 3, Mar 2014.