ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

"Study of Secure Data Transmission Using Audio File"

Raviraj B. Vyavahare[1], Amit J. Bajaj[2], Hitesh P. Fuse[3], Mr. Pravin K. Patil[4]

UG Student, Dept., of Information Technology, SSBT's College of Engineering and Technology, Jalgaon, India[1,2,3]

Assistant Professor, Dept. of Information Technology, SSBT's College of Engineering and Technology, Jalgaon, India[4]

Abstract: In today's digitized environment, information has become a vital part of our day to day activities. Sharing of information becomes a drastic need in order to carry out business specific operations. Several mean of convenience has been brought forward to accomplish this task. Both security and privacy are the major concern while sharing information. Hiding of data i.e. steganography and encryption of data i.e. cryptography are the two familiar approaches in case of sharing of highly confidential data. Both approaches have efficient features and the collaboration of these two can yield optimum result. This paper suggests a modified approach that brings up both cryptography and steganography together in order to enhance the sharing of highly vital information using audio file.

Keywords: Confidential, Cryptography, Encryption, Steganography, RSA.

I. INTRODUCTION

In the 21st century, due to the advancement in the field of science and technology, our business operation goes to a peak level. Day to day operations, business specific functions and several processes involves transfer of information. Sometimes it is necessary to transfer highly secure information between communicating parties to accomplish desired functions. There might be possibility that the highly confidential information that we are transferring may be compromised by the hackers or by unauthorized users. Hence it is necessary to find an appropriate solution for such situations.

Till so far, such kind of situations has been negotiated by applying the concept of data hiding and data encryption separately. Hiding of highly secure data during transfer provides security and privacy up to an extent whereas encryption of highly confidential data provides a better option. [1]

Nowadays it is possible to extract hidden data by applying certain techniques like Multicarrier Spread-Spectrum Embedding. [2] Also encrypted data can be compromised by applying certain techniques like Brute Force Attack. [3] Hence it is necessary to bring up a significant solution for data transfer. We suggest the combining approach of data encryption and data hiding can be a better solution for such cases. The data hiding and data encryption comes under the concept of steganography and cryptography respectively. [4]

A. Steganography

It is a technique of hiding information. It is possible to hide necessary information by applying the steganography approach without causing any affect to the information. Once the information is hidden, it cannot be identified easily. [1]

B. Cryptography

It is a technique of converting plain text into cipher text. It is possible to encrypt highly secure data by applying cryptography approach. This approach helps to convert data in such a way that it can't be understood. Only the authorised user can decrypt the encrypted data. [4]

II. RELATED WORK

It is said that the steganography approach was first practiced during the Greece Empire. History of ancient Greece specifies that they practices melting wax off wax tablets and then they hides the message in the underlying wood. As the message was hidden under the wax, hence no one can have any suspect about the hidden message. Later on a microdot technique has been introduced for hiding secret messages. Microdots were used to permit the transfer of large amount of data and drawings invisibly. After that the concept of invisible ink came into existence and was much popular till world war-II. Certain drawbacks have been identified in such techniques and new hiding techniques has put forward time to time. [5]

Since ancient ages, encryption is the popular approach for transferring important data securely. An encryption technique has been evolved since the Babylonian Era, and was evolving continuously as they were used in the military and political aspects. Hieroglyphics is the oldest encryption technique. Later, Scytale Cipher technique was used which involves use of cylinder and a parchment strip so that the text can be written on that strip. Caesar Cipher was another encryption technique which involved shifting of characters to encrypt the data. Substitution Cipher and Enigma are the most popular encryption techniques in the history of encryption. Every time an encryption technique introduced, someone finds out a decryption method for that. Hence considering drawbacks in existing techniques, newer techniques have been introduced day by day. [6]

III. EXISTING APPROACH

In an equal interval of time, several concepts has been brought forward in order to provide an optimum solution to ensure security, privacy and authentication of the information while carrying out data transfer over network. These concepts involved certain data hiding and data encryption techniques. Considering security and privacy as a major concern, initially the vital data is to be sent after hiding it behind some digital media such as audio, video, images etc. [1] This technique was quite popular, later on

DOI 10.17148/IJARCCE.2015.4232

hackers found a way out, now it is possible to extract the hidden data from the digital media. [2]

With the advent in the field of cryptography, encryption becomes a gossiping fact among all. Later on encryption was used during the data transfer. This technique was better option among other but, only encryption or data hiding cannot provide full assurance towards the data.

Recently, the concept of double layer protection technique has put forward to fill this gap. The double layer protection technique is simply cryptography cum steganography approach which can definitely provide efficient security mechanism for transferring data among communicating parties. [4]

IV. MODIFIED APPROACH

Considering security and privacy as a major aspect, we suggest that the implementation of a double layer protection approach will help user to send vital data without having any worry. We suggest an approach that constitutes both cryptography and steganography.

We are considering a situation where user wants to share some sort of vital information with another party located over some distance. The medium of communication may be wired or wireless.

Now the information that is to be sent should be delivered securely. So in order to achieve this concern, we are suggesting a system that will implement the double layer protection approach.

C. *Proposed System*

We are suggesting a system that can be built by considering steganography and cryptography approach. The proposed system will accept the information as an input (txt file).

This information (txt file) will be then encrypted by an approach of cryptography i.e. RSA algorithm. Once the encryption is done, then the data can be made ready to hide behind an audio file format (.wav file) by applying steganography approach.

This way it will be a safe option to send this audio file (.wav) over network without worrying for the hidden information. This way sender may feel quality trust on his data sharing aspect.

Also it is less suspicious to send the highly confidential data over network, in an encrypted format, hidden behind audio file. This way it can be made possible to maintain security and privacy of the highly vital data.

Following diagram suggests a typical aspect of our proposed system; the overall working of the system can be visualised as follows:

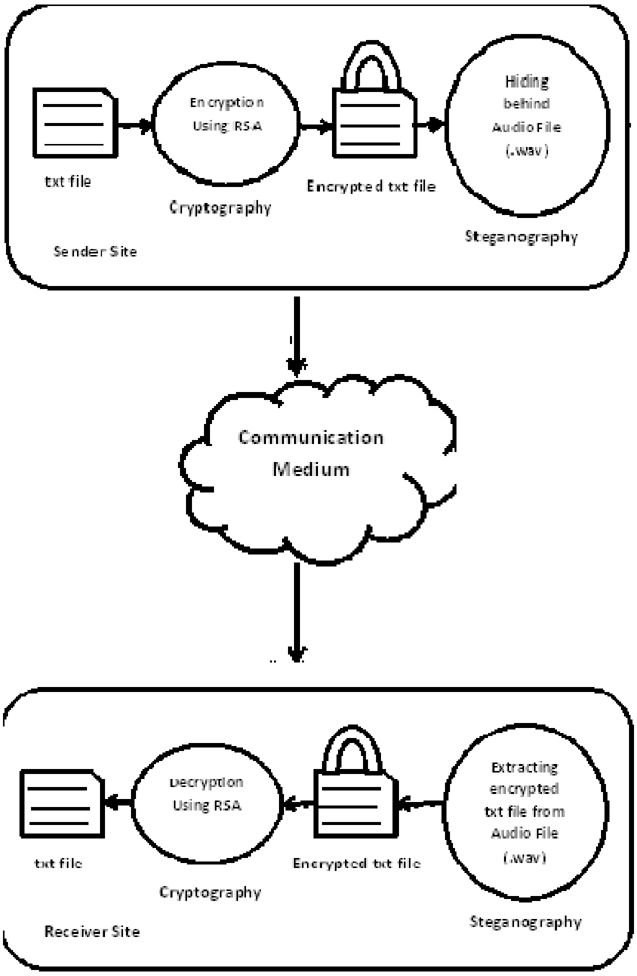

FIG. 1.PROPOSED SYSTEM

FLOWCHARTS:

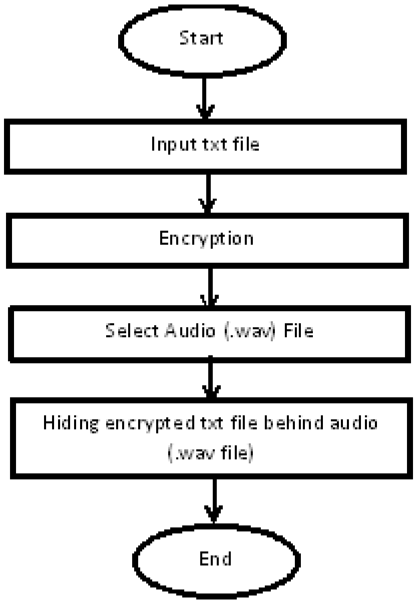

FIG. 2.SENDER SITE

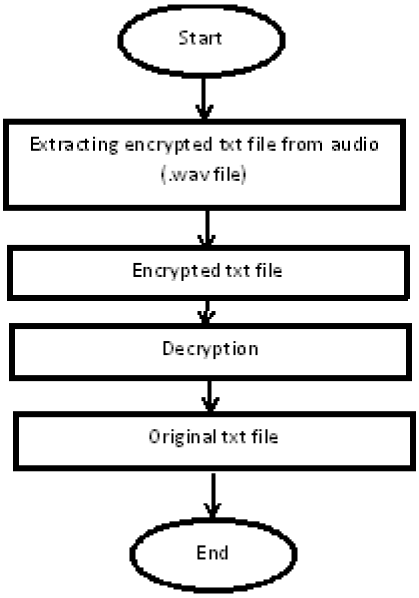

FIG. 3.RECEIVER SITE

D. *RSA*

Cryptography provides data protection facility to the applications that involves sharing of information over network. This makes sure that the sender can send vital data without having any doubt. It's the need of today to make sure the security and privacy of the data as we make use of electronic devices more and more.

RSA (Rivest, Shamir & Adleman) is asymmetric key cryptography algorithm. This algorithm was developed considering the need of security of important data. This algorithm was developed in 1977 by the above mentioned persons. This algorithm works on the basis of two keys: public key and private key. In RSA, public key is used to encrypt the data whereas private is used to decrypt the encrypted data. Working of RSA algorithm involves 3 stages. First stage is the key generation which is to be used as key to encrypt and decrypt data, second stage is encryption operation, where conversion of plaintext to cipher text is being carried out and third stage is decryption, where encrypted text is converted back to plain text at receiver side.

Algorithm Steps-

1. Select two prime numbers p, q, such that $p \neq q$.
2. Calculate n = p*q.
3. Calculate f (n) = (p-1)*(q-1).
4. Select integer e, where 1<e<f (n), e and n are co-primes.
5. Calculate d, such that (d*e) %f (n) =1.
6. Public Key = (e, n).
7. Private Key = (d, n).

e.g.

Let us consider, two prime numbers p = 3, q = 11 then according to the algorithm, the solution flow will be as follows-

1. p = 3, q = 11.
2. n = 3*11 = 33.
3. f (n) = (3-1)*(11-1) = 20.
4. let e = 7.
5. d = (3*7)%20 = 1.
6. Public Key = (7, 33).
7. Private Key = (3, 33).

It is very easy to encrypt or decrypt the needed data. [7]

E. *Data Hiding*

Steganography is an approach to provide invisible message transmission facility. It focuses on hiding the existence of messages. The term hiding means making the information invisible during data transfer. The Steganography algorithms can be used to hide data behind digital media such as audio, video or images. As we are using digital media increasingly, drastic research in audio steganography has already started. In a computer based system, secret messages are hidden in digital sound, using audio file as a cover object. In audio steganography, the weakness of the human auditory system is used to hide information in the audio. [4]

V. CONCLUSION

Both steganography and cryptography has certain limitations, yet these are the most familiar aspects of security and privacy. Either steganography or cryptography cannot provide maximum trust towards security separately. The combination of steganography and cryptography forming a double layer protection approach can yield better secure solution for information sharing. This way a comprehensive approach can be suggested that works on a combined approach that first encrypts the highly secure data and then hides it behind audio. This suggested approach can provide an advanced level of security and privacy to the confidential information over network.

ACKNOWLEDGMENT

We would like to thank our Head of Department, Principal and North Maharashtra University for their constant support and encouragement.

REFERENCES

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

[2]. Ming Li, Michel Kulhandjian, Dimitris A. Pados, Stella N. Batalama and Michael J. Medley, "Extracting Spread-Spectrum Hidden Data from Digital Media", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. X, NO. X.

[3]. Akansha Tuteja and Amit Shrivastava, " Faster Decryption and More Secure RSA Cryptosystem", Ijarcsse, Volume 4, Issue 11, November 2014 ISSN: 2277 128X.

[4]. Tanmaiy G. Verma, Zohaib Hasan and Dr. Girish Verma, "A Unique Approach for Data Hiding Using Audio Steganography", ijmer, Vol. 3, Issue. 4, Jul - Aug. 2013 pp-2098-2101 ISSN: 2249-6645.

[5]. Arvind Kumar and Km. Pooja, "Steganography- A Data Hiding Technique", International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010.

[6]. Simon Singh, "The Code Book" (2001, Shinchosha).

[7]. Nentawe Y. Goshwe, "Data Encryption and Decryption Using RSA Algorithm in a Network Environment", IJCSNS International Journal of Computer Science and Network Security, VOL.13 No.7, July 2013.

DOI 10.17148/IJARCCE.2015.4232

BIOGRAPHIES

Mr. Raviraj B. Vyavahare, UG student, Department of Information Technology, Shram Sadhna Bombay Trust's College of Engineering and Technology, Bambhori, Jalgaon. Area of Interests: Network Security, Cyber Security, IT Infrastructure Management and Software Development.

Mr. Amit J. Bajaj, UG student, Department of Information Technology, Shram Sadhna Bombay Trust's College of Engineering and Technology, Bambhori, Jalgaon. Area of Interests: Network Analysis, Data Mining, Information Hiding and Database Management System.

Mr. Hitesh P. Fuse, UG student, Department of Information Technology, Shram Sadhna Bombay Trust's College of Engineering and Technology, Bambhori, Jalgaon. Area of Interests: Data Ware Housing, Data Mining and Network Management.

Mr. Pravin K. Patil, M.E. (Computer Science and Engineering), currently working as Assistant Professor, Department of Information Technology, Shram Sadhna Bombay Trust's College of Engineering and Technology, Bambhori, Jalgaon since 2014. Area of Interests: Data Warehousing, Artificial Intelligence, Network Security, and Information Retrieval. Has published two papers namely-

1. "Machine Learning Approaches for Automatic Sentiment Analysis of Twitter Messages" in Cyber Times International Journal of Technology and Management.
2. "Study on Altered Fingerprint Detection using Artificial Neural Network" in International Journal of Science and Research.

Also presented a paper on "Machine Learning Approaches for Automatic Sentiment Analysis of Twitter Messages" at International Conference on Global Trends in Engineering, Technology and Management. M.E. Project – "Automatic Sentiment analysis of Twitter Messages using Naive Bayes and Lexicon based approach with sentiment variation".

DOI 10.17148/IJARCCE.2015.4232