International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 05 | May-2016 www.irjet.net p-ISSN: 2395-0072

"Study of Enhancement of Security and Performance during Information Sharing by Data Compression, Encryption and Steganography"

Nikhil R. Mahajan[1], Aniket P. Bonde[2], Utkarsh S. Patil[3], Prasad U. Kale[4]

UG Student, Department of Computer Engineering, SSBT's College of Engineering and Technology, Jalgaon, India

---

Abstract:*Today, information is the major thing. Sharing of information is the major activity that is being carried out in every business operation. We carry out such tasks securely by using steganography, cryptography, compression or combination of these approaches. During such tasks, it is necessary to look after the security and confidentiality of the information without affecting the performance factor. Cryptography and Steganography are the commonly used approach for information sharing. These approaches provide a better way to achieve information sharing. This paper provides a modified solution that combines Compression, Cryptography and Steganography approach together forming a "triple layer approach" in order to provide better way for sharing of highly vital and too large information using audio and text file without compromising the performance of the application.*

Keywords:**Compression, Cryptography, Performance factor, Steganography, Triple Layer, Vital.**

1. INTRODUCTION

Today is the era of innovation, development in the field of science and advancement in the field of technology has created a boom change in the performance of the business operations. Now days, every sector is in need of sharing of data or information. We may need to send extremely important or confidential data to some clients to fulfil our business requirements. There might be possibility that the data that we wish to send is too large or it is highly secret. Such data might get open to have threat during transferring, such as information may be compromised by unauthorized users. Hence it is necessary to find significant solution for situations like this.

Till now, we handle such situations by applying data hiding and data encryption separately. Hiding of data during sharing provides security and privacy whereas encryption of data provides a security mechanism. [1]

Now, it is possible to extract hidden data by Multicarrier Spread-Spectrum Embedding. [2] Also encrypted data is being accessed by Brute Force Attack. [3] Hence it is necessary to have a modified solution for data transfer. To provide a better solution for such problems, here we suggest combination of Compression, Encryption and Steganography approach i.e. a triple layer approach so that we don't need to worry for data size or its security either. The data hiding and data encryption comes under the concept of steganography and cryptography respectively. [4]

1.1 Compression

It is the concept that describes a way to minimize the file size in terms of memory. This approach implies that a text file size can be reduced up to a level without affecting its content. [8]

1.2 Steganography

It is the concept that describes an art of hiding data or information behind some carrier medium such as audio file. [1]

1.3 Cryptography

It is the concept that describes that a file's content can be converted into a cipher form so that it is almost impossible to decode without prior techniques. It implies that a plain text file can be converted into a cipher text form. [4]

2. RELATED WORK

Data compression is a novel approach; it describes the concept of reducing memory aspect but it does not cause any damage to the data. Compression is being practiced with evolvement of science. We use Lossy and Lossless compression techniques to minimize data file size. A series of approach has been put forward time to time to compress text files. These approaches implies several Lossy and Lossless compression algorithms such as Huffman Algorithm, Model based compression, Gzip Stream algorithm, Deflate Stream Algorithm, Burrow's wheeler and Vector quantization etc. All these compression approach specify a particular procedure for text file compression and the result varies accordingly. [8]

Steganography firstly discovered during the Greece Empire. During this time, people practice melting wax off wax tablets and then they hide the message in the underlying wood. Since the message was hidden under the wax, hence no one can guess about the hidden message.

After that microdot technique has been introduced. Microdots were used to permit the transfer of huge amount of data and drawings invisibly. Afterwards the concept of invisible ink came into existence and became much popular. Certain drawbacks have been recognized in such techniques and new hiding techniques has put forward with floating time. [5]

Since ancient ages, data encryption is the popular approach for transferring important data securely. An encryption technique came into existence since the Babylonian Era, and was evolving continuously as they were used in the military and political aspects. Hieroglyphics is the ancient encryption technique. Later, Scytale Cipher technique was used which includes use of cylinder and a parchment strip so that the text can be written on that strip. Caesar Cipher was another encryption technique which involves shifting of characters to encrypt the data. Substitution Cipher and Enigma are the most famous encryption techniques in the history of encryption. Newer techniques have been introduced day by day considering the drawbacks in the existing systems. [6]

EXISTING APPROACH

While studying about all these approaches, we come across a situation that currently it is possible to get a text file as an input from user, this text file then can be encrypted and made hidden behind some carrier medium let's say .wav file at sender side and it can be extracted and decrypted to get original file at receiver side. [9]

After reviewing this procedure, a query can be raised regarding performance and security of the application i.e. what if the text file that user wish to send is too large in terms of memory and content? Will the application still be functional?

3. MODIFIED APPROACH

The answer to above question is probably no. By considering performance factor, security and privacy, here we suggest a modified approach as a solution in such cases. We suggest a Triple layer approach that combines three different approaches together. Here we define a Triple layer approach that combines the features of compression, encryption and steganography together to provide an optimum solution for existing system's drawbacks.

We are assuming the situation where the user is having a text file which is too large in terms of memory size and contents, and this file is need to be sent securely over some wired or wireless network.

3.1 Proposed System

The proposed system or application will employ concept of compression, encryption and steganography to build a Triple layer approach. The proposed system will first accept text file from user (this text file can be of any size now). This text file is then can be compressed to produce a low memory size compressed text file. This compressed text file then can be encrypted by RSA algorithm to provide additional security. After encryption, the resulting encrypted file is now can be made hidden behind some carrier medium so that no one can guess the availability of text file for compromising the data.

This way it will be a safer and efficient option to send too large text file data over wired or wireless network by using this approach because in the end, we will be sending a carrier medium file (.wav file) to receiver over network and probability of getting noticed about vital data is negligible.

At the receiver side, de-steganography, decryption and decompression can be done to get the original text file message or data.

The proposed system approach can be visualized as follows:

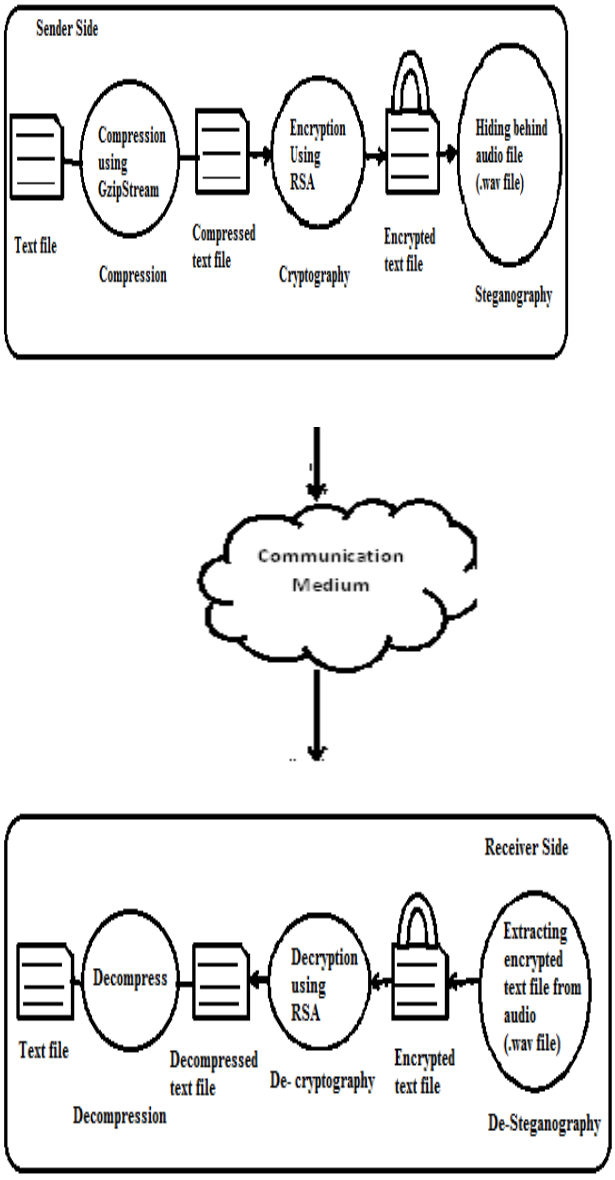

FIG. 1. PROPOSED SYSTEM

FLOWCHARTS:

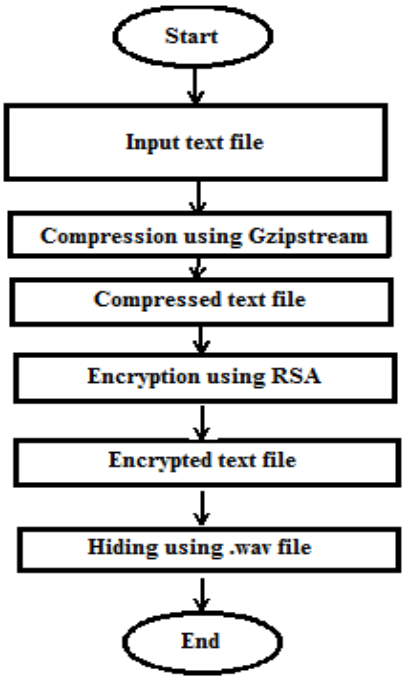

FIG. 2.SENDER SITE

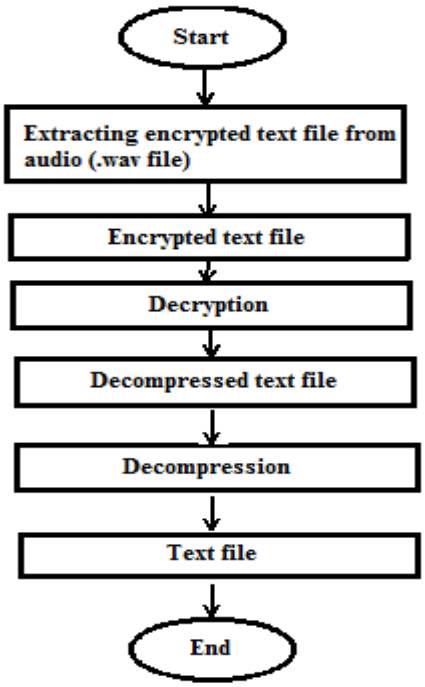

Fig. 3. Receiver site

3.2 Gzip Stream Algorithm

It is a compression algorithm which is considered as an industry standard practice. This algorithm is widely used in text compression aspect. This algorithm implies that within a text file, it references repeating character values as a single entity. For example, let us suppose there is a text file having some sort of content in it. The content can be alphabets, numbers, special symbols etc. Now this algorithm states that the repeating characters present in the file should be counted or termed as a single character entity. If the content of a text file contains "a" alphabet 20 times, then it is referred as single "a" character after compression. This way memory is reduced up to an extent without affecting content of the text file.

Decompression is exactly reverse of this, during decompression it revert back the references of each character and shows the original character values within the text file. [10]

3.3 RSA

RSA (Rivest, Shamir & Adleman) is unsymmetrical key cryptography algorithm. This algorithm based on the basis of two keys: public 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 three stages. First stage is the key generation which is to be used as a key to encrypt and decrypt data, next stage is encryption operation, where conversion of plain text to cipher text is being implemented and next 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).

3.4 Data Hiding

The term hiding means making the information unseen. The Steganography algorithms can be used to hide data behind digital media such as audio. As we are using digital media increasingly, in a computer based system, secret messages are hidden in digital sound, using audio file as a carrier object. In audio steganography, the weakness of the human auditory system is used to mask information in the audio. [4]

4. CONCLUSION

The compression, steganography and cryptography approach has certain drawbacks if we apply these concepts separately but the combination of all these three approach can yield an optimum solution that can help us build an application that will surely show enhancement in terms of performance and provides high level of security to our information during data transfer.

ACKNOWLEDGMENT

We would like to obligate 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. Batalamaand Michael J. Medley, "Extracting Spread-Spectrum HiddenData 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. GirishVerma, "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.

[8]. T. SubhamastanRao, M. Soujanya, T. Hemalatha, T. Revathi, "Simultaneous Data Compression and Encryption", (IJCSIT) International Journal of Computser Science and Information Technologies, Vol. 2 (5) , 2011, 2369-2374

[9]. Raviraj B. Vyavahare, Amit J. Bajaj, Hitesh P. Fuse, Mr. Pravin K. Patil, "Study of Secure Data Transmission Using Audio File", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 2, February 2015

[10]. NAGASESHU.K, SRINIVASA RAO.V , HIMA DEEPTHI.V, "A Novel Approach for Embedding Text in Audio to Ensure Secrecy", Nagaseshu.K et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (4) , 2011 , 1592-1594.