ISSN 2348 – 8034
Impact Factor- 3.155

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

DATA SECURITY USING RJDA & STEGANOGRPHIC ALGORITHM

Harsh Deepak Shrivastav*[1], Sushil Tiwari[2] and Sriram Yadav[3]

*[1]M.Tech. Scholar, Department of Computer Science & Engineering, MIT, Bhopal (MP) INDIA
[2]Associate Professor, Department of Computer Science & Engineering, MIT, Bhopal (MP)
[3]Associate Professor & Head, Department of Computer Science & Engineering, MIT, Bhopal (MP) INDIA

ABSTRACT

Now a day's internet is used to communicate and all the information is transferred through this insecure medium. There are number of hackers try to hack the information. To keep the information secure cryptographic algorithms are used. There are two type of cryptographic algorithm used: encryption/ decryption algorithm and steganography algorithm. Steganography is the process of exchanging secret information in such a way that nobody else can detect the presence of that secret message. To gain high security steganography algorithm is used to combine with encryption/decryption algorithm. In this paper, authors have studied many such steganography algorithms, analyze it and presented their experimental result and conclusion.

Keywords- Computer Security, Steganography, MSA Algorithm, Encryption Decryption Algorithm.

I. INTRODUCTION

Information security keeps most importance in today's fast developing era. Various networks are used to exchange the information, which may be secure or not. With the rapid growth of computer networks and advancement in technology, a large amount of information is being exchanged. Much of this information is confidential or private which increases the demand for stronger encryption techniques. Security has become a critical feature for endowed networks. Communication is not safe due to the presence of hackers who wait for a chance to gain access to confidential data. Cryptography is derived from the Greek words "kryptos" (meaning "hidden") and "graphein" (meaning "to write"). Cryptography is the study of shuffling information from in such a way that no one can understand the original meaning of message without knowing the secret key which make it again original text. The process of converting information (plain text) by transforming it into unreadable format (cipher text) is known as encryption. Encryption techniques can be sometimes broken by cryptanalysis, also called as code breaking, although modern cryptographic techniques are virtually unbreakable. Cryptography encrypts the original message that is being sent. This mechanism employs mathematical schemes and algorithms to scramble data into unreadable text. It can only be decoded or decrypted by the party that possesses the associated key [5].

Steganography is derived from the Greek word "stegnos" (meaning "covered/secret") and "graphein" (meaning "to write/draw") [2]. Steganography is the study of means of hiding the information in order to prevent hackers from detecting the presence of the secret information. The process of hiding the message in a cover without leaving a remarkable trace is known as Steganography. Steganography is the form of convert communication in which a secret message is hided with a carrier data. Steganography facade the presence of communication, making the true message not observable to the observer. Cryptography and Steganography achieve the same goal using different means. Encryption encodes the data so that an unintended recipient cannot determine its intended meaning. Steganography in contrast attempts to prevent an unintended recipient from suspecting that the data is there [3]. The authors studied both the algorithms and studied the techniques that use both the algorithm to provide high degree of security and also compare the result on the basis of timing and avalanche effect.

II. LITERATURE SURVEY

Nearly every steganography algorithm uses image as a cover image. Many algorithms have been proposed that uses different techniques to hide the secret message or a secret image behind the cover image. Among all of them LSB method is the best technique used to hide the secret message or image behind cover image because of low noise in the cover image. But here, author have studied the techniques where text file or MS Word file is used as a cover file.

Rishav Ray, Jeeyan Sanyal, Debanjan Das, Asoke Nath[1] used a text file/MS word file as a cover file to hide the secret data. To increase the degree of security authors have first encrypted the secret data by using Modified Generalized Vernam Cipher Method (MGVCM) and then hide the encrypted text behind the text file. Authors have proposed two new algorithms one is encryption/decryption algorithm and second algorithm is the hiding algorithm which explained the method to hide the secret message behind the text file. Authors have named his proposed algorithm "RJDA" which is architecture of joining these proposed two algorithms. To hide secret message inside the text file authors have proposed a new method in which the bits of each character of secret message file is inserted in place of eight randomly selected blank space characters of the cover files. In this method authors have first converted the secret file into binary format where every character is represented by 8 bits. To hide each bit, authors use blank spaces, to hide bit–0 authors left the blank space as it is, and for bit-1 authors replace the blank space to a character having ASCII value 160 and this character also appear like a blank space on the screen or while printing.

III. ANALYSIS OF RJDA ALGORITHM

This section is providing analysis of RJDA algorithm on the basis of different parameters like execution time and for security avalanche effect. Dot Net implementation has used to test this algorithm. For experiment, Intel Pentium Dual Core E2200 2.20 Ghz, 1 GB of RAM and Window-XP SP2, have used in which performance data is collected.

Analysis of RJDA encryption and decryption algorithm:

There are many encryption/decryption algorithms, but still there is always a competition to develop an algorithm which will provide high security in minimum time. Time and robustness of internal structure both are the important parameters for any cryptographic algorithm. If an algorithm has robust internal structure but not a time efficient then there is no significance to use it. Such algorithms cannot be used for real time transmission or in ad-hoc networks because of the time taken by an algorithm and also if algorithm is time efficient but not secure than again it is useless.

Time Efficiency and Throughput

Time efficiency is a important parameter used to measure the performance of cryptographic algorithm. It is a time taken by an algorithm to convert the plaintext into cipher text. Throughput is one another parameter depended on time. It can be defined as the amount of text encrypted per unit time. The algorithm having higher throughput is considered better than the other.

Table1 Execution Time and Throughput of RJDA Encryption algorithm

File Size (in KB)	**RJDA Encryption Algorithm**	
	Execution Time (in Seconds)	Throughput (Bytes/ Second)
1 KB	8.658	118
5 KB	16.582	308
10 KB	24.663	415

Table 1 shows the execution time of encryption algorithm and throughput (Bytes/ Second) of RJDA algorithm and Table 2 shows the execution time of decryption algorithm.

Table2 Execution Time and Throughput of RJDA Decryption algorithm

File Size (in KB)	**RJDA Decryption Algorithm**	
	Execution Time (in Seconds)	Throughput (Bytes/ Second)
1 KB	8.672	118
5 KB	16.358	312

10 KB	24.363	420

From Table 1, it can be concluded that RJDA encryption/decryption is not a time efficient algorithm. It takes more time to encrypt or decrypt a secret message. Timing for encryption/decryption algorithm is almost same. It is also observe that throughput of RJDA algorithm increases as the size of file increases. Graphical representation of time and throughput of encryption/decryption algorithm is shown in figure 2, 3, 4 and 5 respectively.

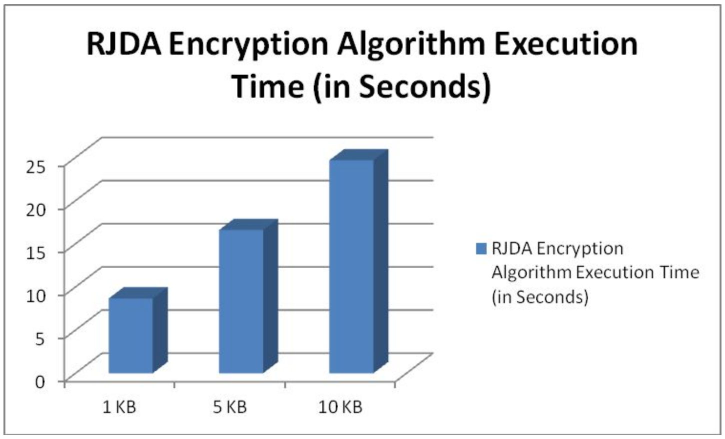

Figure 2 Encryption Time of RJDA Encryption algorithm

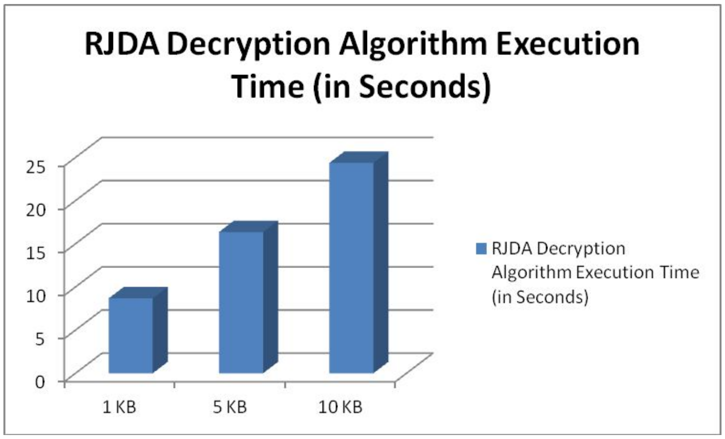

Figure 3 Decryption Time of RJDA Encryption algorithm

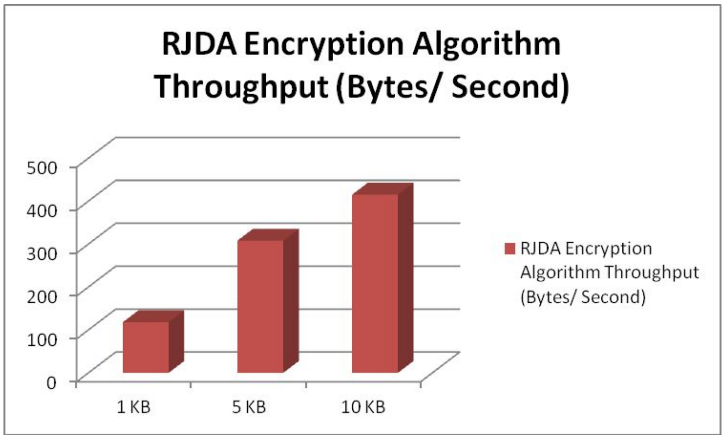

Figure 4 Throughput of RJDA Encryption algorithm

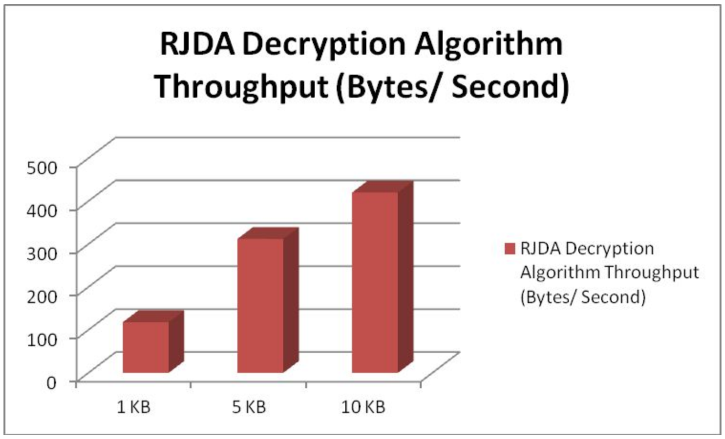

Figure 5 Throughput of RJDA Encryption algorithm

Analysis of RJDA Avalanche Effect:
Another parameter used to evaluate the performance of cryptographic algorithm is avalanche effect. It is used to show the internal strength of algorithm. According to avalanche effect change in a single bit of plaintext will change 50% of bits of cipher text. The algorithm closed to avalanche effect condition is considered more secure than others. To check the internal strength of RJDA algorithm authors have computed the value of avalanche effect and show the result at Table 3 and its graphical representation at figure 6.

From Table 3, it can be concluded that avalanche effect of RJDA algorithm is not upto the mark. Hence, internal structure of RJDA algorithm is not that much strong which is demanded in todys scenario with the rapid increase in technologies.

Table 3 Avalanche Effect of RJDA algorithm

File Size in KB	**RJDA Algorithm**
	Avalanche Effect
Single bit change in key	42.1875%

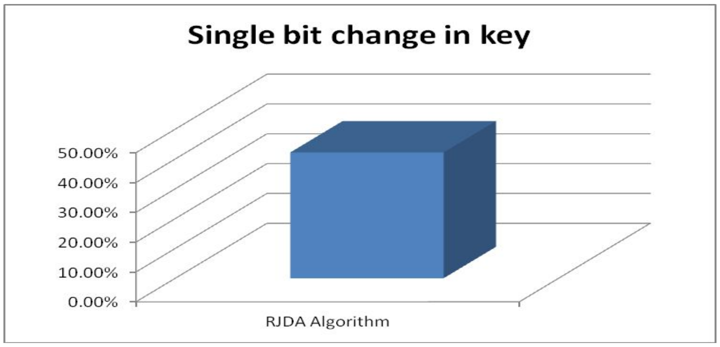

Figure 6 Avalanche Effect of RJDA algorithm

Analysis of RJDA Data Hiding and Unhiding Algorithm.

RJDA introduces an algorithm to hide the text data behind text file. Authors analyzed the performance of this algorithm on the basis of timing. Authors have implemented this algorithm and calculated the time taken by this algorithm. Experiment results is shown in Table 4 and in Figure 7. Also during study of this algorithm, authors have marked some issues that is the size of cover file is very large. To hide a single character, this algorithm needed a cover file having 8 spaces. therefor to hide normal size file it requires very large cover file in size.

Table1 Execution Time and Throughput of RJDA Encryption algorithm

RJDA Hiding Algorithm	
File Size (in KB)	Execution Time (in Seconds)
1 KB	0.11
2 KB	1.323
3 KB	8.319

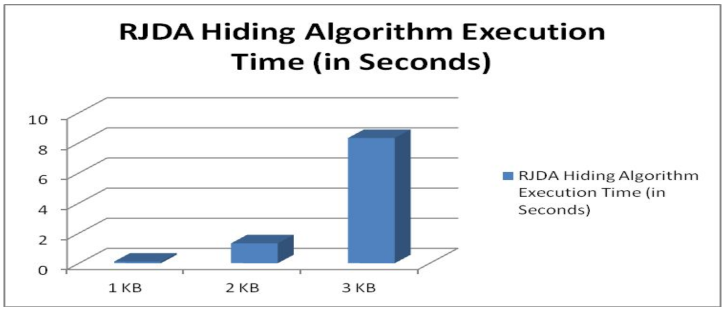

Figure 7 Execution Time of RJDA Hiding Algorithm

IV. CONCLUSION

As the technology changes very rapidly, demand for the security of secret information also changes very rapidly. In this paper author have done the detail analysis of RJDA algorithm which is used to provide security on the transmitted data. In this secret data is firs shuffled with the help of encryption/decryption algorithm and then hide the shuffled data behind the text file. After deep study of both the algorithms used in RJDA algorithm, authors have concluded that the encryption/decryption algorithm used in RJDA is not time efficient as well as the internal structure of encryption/decryption is not very robust. Hence it cannot be used for secure transmission and also not used for fast transmission. And also the second hiding algorithm used in RJDA uses eight spaces in cover file to hide a single ascii character, therefore it required large over file to hide a secret message. In transmission cover file is the file that is transmitted, if the size of cover file is large than it has to transmit large size file means more time in transmission which make the performance of this algorithm more poor. RJDA algorithm is a new step to hide text data behind text file but it needed some correction to improve the performance and security over transmitted data.

REFERENCES

[1] *Rishav Ray, Jeeyan Sanyal, Debanjan Das, Asoke Nath. "A new Challenge of hiding any encrypted secret message inside any Text/ASCII file or in MS word file: RJDA Algorithm". 2012 IEEE International Conference on Communication Systems and Network Technologies*

[2] *Clair, Bryan. "Steganography: How to Send a Secret Message." 8 Nov. 2001.*

[3] Westfeld, A., and G. Wolf, Steganography in a Video conferencing system, in proceedings of the second international workshop on information hiding, vol. 1525 of lecture notes in computer science, Springer, 1998.pp. 32-47.

[4] Johnson, N. F. and Jajodia, S, "Exploring steganography: Seeing the unseen", IEEE Computer Magazine, pp. 26-34, February 1998.

[5] William Stallings, Cryptography and Network Security, Principles and Practice, Third edition, Pearson Education, Singapore, 2003.

[6] Symmetric Key Cryptography using Random Key generator: Asoke Nath, Saima Ghosh, Meheboob Alam Mallik: "Proceedings of International conference on security and management(SAM'10" held at Las Vegas, USA Jul 12-15, 2010), P-Vol-2, 239-244(2010).

[7] An Integrated Symmetric key Cryptography Algorithm using Generalised modified Vernam Cipher method and DJSA method: DJMNA symmetric key algorithm : Debanjan Das, Joyshree Nath, Megholova Mukherjee, Neha Choudhary, Asoke Nath: Communicated for publication in IEEE International conference WICT 2011 to be held at Mumbai Dec 11-14, 2011.

[8] Data Hiding and Retrieval: Asoke Nath, Sankar Das, Amlan Chakraborty, published in IEEE "Proceedings of International Conference on Computational Intelligence and Communication Networks (CICN 2010)" held from 26-28 NOV' 2010 at Bhopal.

[9] Advanced Steganographic approach for hiding encrypted secret message in LSB, LSB+1, LSB+2, LSB+3 bits in non standard cover files : Joyshree Nath, Sankar Das, Shalabh Agarwal and Asoke Nath, International Journal of Computer Applications, Vol- 14, No. 7, Page-31-35, Feb (2011).

[10]Advanced Steganography Algorithm using encrypted secret message: Joyshree Nath and Asoke Nath, International Journal of Computer Science and Applications, Vol-2, No. 3, Page- 19-24, Mar (2010).

[11]A Challenge in hiding encrypted message in LSB and LSB+1 bit positions in any cover files: executable files, Microsoft Office files and database files, image files, audio and video files : Joyshree Nath, Sankar Das, Shalabh Agarwal and Asoke Nath : JGRCS, Vol-2, No. 4, Page- 180-185, Apr (2011).

[12]New Data Hiding Algorithm in MATLAB using Encrypted secret message: Agniswar Dutta, Abhirup Kumar Sen, Sankar Das, Shalabh Agarwal and Asoke Nath : Proceedings of IEEE CSNT- 2011 held at SMVDU (Jammu), 03-06 Jun, 2011, Page 262-267.

[13]New Steganography algorithm using encrypted secret message: Joyshree Nath, Meheboob Alam Mallik, Saima Ghosh and Asoke Nath : Proceedings of Worldcomp 2011 held at Las Vegas (USA), 18-21 Jul, 2011.

[14]Steganography In Digital Media: Principles, Algorithms and Applications by Jessica Fridrich : Cambridge University Press.

[15]Cryptography and Network Security, William Stallings, Prentice Hall of India.

[16]Cryptography & Network Security, Behrouz A. Forouzan, Tata McGraw Hill Book Company.

[17]Cryptography and Information Security, V. K. Pachghare, Prentice Hall of India.

[18]SANS Security Essentials, (volume 1.4, chapter 4) Encryption and Exploits, 2001.

[19]Petitcolas, Fabien A.P., "Information Hiding: Techniques for Steganography and Digital Watermarking.", 2000.

[20]StegoArchive, "Steganography Information, Software and News to enhance your Privacy", 2001

[21]Petitcolas, Fabien A.P., "The Information Hiding Homepage: Digital Watermarking and Steganography"

[22]Johnson, Neil F., "Steganography", 2000.

[23]The WEPIN Store, "Steganography (Hidden Writing)", 1995

[24]Sellars, D., "An Introduction to Steganography"

[25]Bender, W., "Techniques for Data Hiding", IBM Systems Journal, Vol. 35, Nos 3+4, Pgs 313-336, 1996.

[26]Krinn, J., "Introduction to Steganography", 2000

[27]Noto, M., "MP3Stego: Hiding Text in MP3 files", 2001

[28]"Chameleon", Image Steganography by Mark David Gan

[29]Translation-Based Steganography: Christian Grothoff, Krista Grothoff, Ludmila Alkhutova, Ryan Stutsman, Mikhail Atallah

[30]Hide and Seek: An introduction to Steganography: Niels Provos, Peter Honeyman.

[31]Modren Steganography: Miroslav Dobší_ek