Volume 4, Issue 4, April 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Information Security System using RYPTO_Steganography System

R.Venkateswaran

Lecturer, Salalah College of Technology, Salalah, Sultanate of Oman and

Research Scholar – Ph.D, Karpagam University ,INDIA.

Abstract: The importance of information and communications systems for society is intensifying with the increasing value and quantity of data that is transmitted and stored in the system. At the same time those data and information are highly vulnerable to a variety of threats, such as unauthorized access and use, misappropriation, alteration, and destruction. Proliferation of computers increased computing power, interconnectivity, decentralization, growth of networks and huge number of users as well as the convergence of information and communications technologies. So Cryptography and Steganography have become an important component of information security and communications systems. In the proposed model, new cryptography systems is developed with combining the features of Steganography for higher security.

Keywords: Security, Steganography, Keys, Cryptosystem, Algorithm.

I. INTRODUCTION

There are legitimate governmental, confidential information are exchanged between nations, and officials in the departments. Commercial and business people want their innovation documents, product details to be secured on the system. Individual required secured communication to send and receive files; they used cryptography methods to protect their information from illegal activities, which can affect public safety, national security, the enforcement of laws, business interests, Consumer interests and privacy. Governments, together with industry and the general public, gained a lot but are challenged by hackers and attackers of today's digital communication. Hence to have secure communication of government, private and general public, secret communications have taken a very important role within the cyberspace. So Cryptography and Steganography have become an important part of information security and communications systems.

II MOTIVATION OF RESEARCH WORK

Encryption of data plays a vital role in the real time environment to keep the data out of reach of unauthorized people, such that it is not altered and tampered. After encryption, the files can be transferred securely to the end user by using different cryptography tools. The applications should have a fool proof reversal process as of which should be in a position to decrypt the data to its original format upon the proper request by the genuine user. This is analyzed at the outset.

Single tier security is not sufficient as it is vulnerable to different attacks. Hence a second level of security is introduced using steganography. In this research work, Embed and De-Embed processes of information hiding methods is done in various format .It is efficiently carried out and analyzed on different ways of hiding information inside the image and audio file and other methods. The motivation of this research work is to analyze Information security system in using Cryto_Steganography for providing secured data transmission.

III LITERATURE SURVEY

Ranjan Bose [11], William Stallings [12] studied the concepts of cryptography, cryptology, cryptosystem and fundamental concepts of ceaser cipher, features and break analysis and various related cipher substitutions like mono, homo and PolyGram and transposition substitution ciphers.

Michal E [13] analyzed in detailed about transposition, substitution, transformation and other encryption and decryption methods of symmetric and asymmetric algorithms with simulation result.

Verma A K , Mauyank Dave and Joshi R C [3] presented cryptanalysis method based on Genetic Algorithm and Tabu Search to break a Mono-Alphabetic Substitution Cipher in Adhoc networks.

Diaa Salama Abd Elminaam [7] conducted a comparison of general encryption algorithms at different settings for each algorithm such as different sizes of data blocks, different data types, battery power consumption, different key size and encryption/decryption speed.

Aleksey Gorodilov, Vladimir Morozenko [4] discussed about the possibility to use genetic algorithms in cryptanalysis. They described the algorithm for finding the secret key of a block permutation cipher with controlled accuracy.

Mukhopadhyay D, Mukerjee A[1] concentrated on the method in which the substitution technique of steganography can been used to hide data in a 24-bit bitmap file. And Popular audio hiding techniques based on methods of steganography is also discussed in this paper.

Based on all the above study we have developed our base work. We carried out different analysis of various substitution ciphers, related issues of attacking cipher text and analyzed various information hiding methods.

IV FINDINGS

In this work, we have investigated Information security models with proposed concepts,

Stage1 Poly substitution based cryptography System

Stage 2 Development of secured Crypto_steganography system,

4.1 Stage 1 : POLY SUBSTITUTION BASED CRYPTOGRAPHY

4.1.1 Problem Statement

In this work poly substitution methods are used to generate ASCII values of the given text in a linear way and substituted in different layers by applying some permutation methods for encryption and decryption of information.

4.1.2 Methodology

- In this methodology, we take 3 different keys e1, e2 and e3 for encryption. We add ASCII value of e1 to ASCII value of first character, and e2 to second character and e3 to third character, alternatively successively till the end of the given text.
- In a similar way two more different sets of keys are taken and encryption is done to the resultant text.
- Then the resultant text is an encrypted message, and it generate a combination of 3* (256 * 256 * 256) letters encrypted text.
- Finally, it takes the symbols of each updated character from the windows operating system. They are forwarded and stored in the file for secured communication to the receiver and decryption also done for this process with similar algorithms.

4.1.3 Implementation

This method is implemented using C and C++ languages and the results are compared with other symmetric cipher system with online crypto tool.

4.1.5 Results

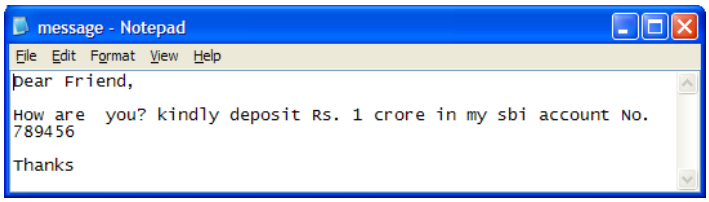

Fig 1. Original Message.

After Stage1.

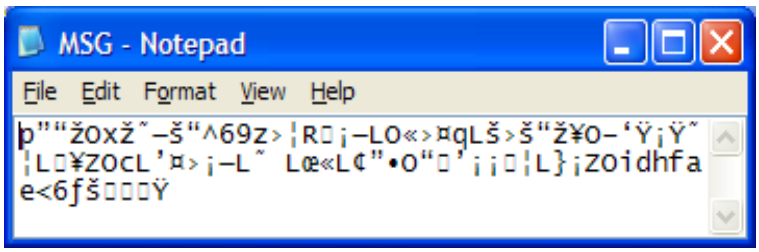

Fig 2. Encrypted Message.

4.2 Stage 2 : Development of Secured Cryto_Steganography System

4.2.1 Problem Statement

In this work, we embed a poly substitution based encrypted text of the original message in an image file using LSB Methods.

4.2.2 Methodology

In Normal steganography software system, the work is implemented within available encryption algorithms for data security. But we have developed the new poly substitution cipher systems for data security and hiding. In this method, the

user can set a different password for every message he sends, which will enable the user of to transmit the same image to two groups with security

4.2.3 Steps for hiding the data in image steganography

- Reading the encrypted file and converting each character to ASCII values and then converted into binary 8 bits
- Reading the 24 bit bitmap file, replacing the last bit in each byte in 24 bits pixel with some permutation for watermarking.
- Final bitmap is stored and forwarded to the end user for secured transmission
- Reverse process is also developed to reveal the information in a secured manner.

4.2.4 Implementation

This method is Implemented Using Microsoft VC++ language and the results are compared with other symmetric cipher system with online crypto tool.

4.2.5 Results

Fig 3. Encrypted File hidden in image

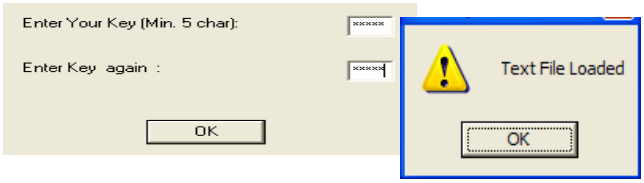

Fig 4. Secret Key.

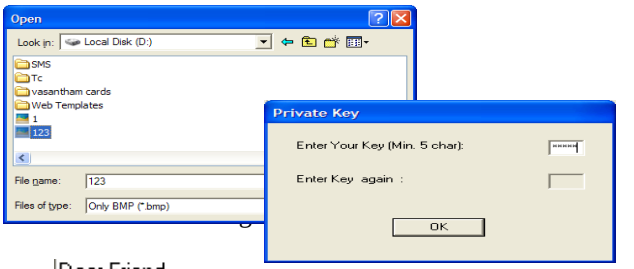

Fig 6. Original Message.

V CONCLUSION

The Research work carried out will give the new area of research on cryptography with combined features of Steganography with reference to poly substitution ciphers Methods. The presented work showed that proposed poly substitution method has a better performance than other common encryption algorithms used. Since poly substitution method has not known any security weak points so far, Other Substitution ciphers like mono, homo, transposition ciphers and poly alphabetic ciphers showed poor performance results compared to present algorithms. This model is easy to embed with multimedia files like image, and text for higher security.

REFERENCES

[1] Mukhopadhyay D, A Mukherjee, S Ghosh, S Biswas, P Chakarborty: An Approach for Message Hiding using Substitution Techniques and Audio Hiding in Steganography, IEEE 2005

[2] Nalani N, Raghavendra Rao G,' Cryptanalysis of Simplified Data Encryption Standard via Optimisation

,Heuristics;IJCSNS, Vol.6 No.1B, January 2006

[3] Verma A K , Mauyank Dave and Joshi R C,'Genetic Algorithm and Tabu Search Attack on the Mono Alphabetic Substitution Cipher in Adhoc Networks; Journal of Computer Science 3(3): 134-137, 2007

[4] Aleksey Gorodilov, Vladimir Morozenko," genetic algorithm for finding the key's length and cryptanalysis of the permutation cipher", International Journal "Information Theories & applications" Vol.15 / 2008.

[5] Sujith Ravi, Kevin Knight,' Attacking Letter Substitution Ciphers with Integer Programming', Oct 2009, 33, 4; Proquest Science Journals Pg.321

[6] Pradeep Kumar Singh, Agarwal R S, "Enhancement of LSP based steganography for hiding data., IJCSE , 02, No. 05, 2010, Page No.1652-1658

[7] Diaa Salama Abd Elminaam " Evaluating The Performance of Symmetric Encryption Algorithms", International Journal of Network Security, Vol.10, No.3, PP.216–222, May 2010, Pg. 216

[8] Geetha K , Vanthia muthu P V," International journal of Computer Science and Engineering" vol 2 No.4 PG No: 1308-1312, Year 2010

[9] Maram Balajee, Unicode and color integration tool for encryption and decryption , IJCSE, Vol. 3 No. 3 Mar 2011

[10] Lokeswara reddy V, Subramaniyam A, Cheena reddy P, implementation of LSP Steganograpy and its evaluation of various file formats , Int. J. Advanced Networking and Applications, Volume: 02, Issue: 05, Pages: 868-872 (2011)

[11] Ranjan Bose, Introduction to Cryptography — Tata Mc-Grew – hill Publisher ltd, 2001.

[12] William Stallings," Cryptography and Network Security: Principles and Practice", 2/3e Prentice hall, 2010.

[13] Michael E. Whitman and Herbert J. Mattord (2008). *Principles of Information Security*, 2/e; Thomson Course Technology

[14] Darrell Whitley,' A Genetic Algorithm Tutorial', Computer Science Department, Colorado State University, Fort Collins, CO 80523.

VII . BIOGRAPHY

R. Venkateswaran received his professional degree MCA and MBA (IS) from Bharathiar University, Tamilnadu, India, He received his M.Phil in computer science from Bharathidasan University, Tamilnadu, India, and He is currently a Ph.D Scholar in the Karpagam Academy of Higher Education, Karapagam University, Tamilnadu, India, in the field of Cryptography and Network Security. Presently he is working as Lecturer, Department of IT, Salalah College of Technology, Salalah, Oman. He has 13 years of teaching experience and 3 years of research experience. He has participated in many national level conferences and workshops, published papers in five international conferences proceedings and published eight papers in international refereed journals. s. He is a member of CSI, IAENG, IACSIT, CSTA and many online forums. He has completed Oracle Certification at Oracle University. His research interests are in cryptography and network security, information security, software engineering and database management system.

