ISSN No. 0976-5697

Volume 2, No. 6, Nov-Dec 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Implementation of Crypto-Steganography System with Combining the Features of ASCII and LSB Technology

Prof. R. Venkateswaran*
Asst. Professor, GR Govindarajulu School of App. Comp. Tech. (PSGR Krishnammal College for Women) &.
Research Scholar-Ph.D, Karpagam University,
Coimbatore, TN, India
venky.mca@gmail.com

Prof. Dr. V. Sundaram
Director
Karpagam College of Engineering
Affiliated to Anna University
Coimbatore, TN, India
dr.vsundaram@gmail.com

Abstract: This paper shows the enhanced information security using proposed image_ Steganography model Proposed methodology shows that successfully using these Poly substitutions[1] method to evolve a new method for Encrypting and decrypting the messages with enhanced Security of Information. In poly-alphabetic substitution ciphers the plaintext letters are enciphered differently depending upon their placement in the text and finally it gives the result in the form of ASCII symbols. We can use Poly substitution method combining the features of Image_Steganography for text encryption by three keys with multiple Layers of security by using genetic keys. After this process, the encrypted file in the form of ASCII Symbols. is hidden in image file using LSB method, the same process is applied reversal to retrieve the source message by Genetic keys.

Keywords: Encryption, Decryption, Genetic Keys, Mono Substitution, Poly Substitution., Image Processing.

I. INTRODUCTION

The importance of information and communications systems for society and the global economy is intensifying with the increasing value and quantity of data that is transmitted and stored on those systems. At the same time those systems and data are also increasingly 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 the number of users, as well as the convergence of information and communications technologies, while enhancing the utility of these systems, also increase system vulnerability.

Security of information and communications systems involves the protection of the availability, confidentiality and integrity of those systems and the data that is transmitted and stored on them. Availability is the property that data, information, and information and communications systems are accessible and useable on a timely basis in the required manner. Confidentiality is the property that data or information is not made available or disclosed to unauthorized persons, entities and processes. Integrity is the property that data or information has not been modified or altered in an unauthorized manner. The relative priority and significance of availability, confidentiality and integrity vary according to the information or communication systems and the ways in which those systems are used. The quality of security for information and communication systems and the data that is stored and transmitted on them depends not only on the technical measures, including the use of both hardware and software tools, but also on good managerial, organizational and operational procedures.

Cryptography is an important component of secure information and communications systems and a variety of applications have been developed that incorporate cryptographic methods to provide data security. Cryptography is an effective tool for ensuring both the confidentiality and integrity of data.[1]

II. OBJECTIVES OF THE PROJECT

a. ***Authentication:*** This means that before sending and receiving data using the system, the receiver and sender identity should be verified.

b. ***Secrecy or Confidentiality:*** Usually this function (feature) is how most people identify a secure system. It means that only the authenticated people are able to interpret the message (date) content and no one else.

c. ***Integrity:*** Integrity means that the content of the communicated data is assured to be free from any type of modification between the end points (sender and receiver). The basic form of integrity is packet check sum in IPv4 packets.

d. ***Non-Repudiation:*** This function implies that neither the sender nor the receiver can falsely deny that they have sent a certain message.

e. ***Service Reliability and Availability:*** Since intruders, which may affect their availability and type of service to their users, usually attack secure systems. Such systems should provide a way to grant their users the quality of service they expect.

III. MOTIVATION FOR THE STUDY

The contribution of cryptography to research in Information security has been significant and issue in the web based applications. One reason is to hide it, or make it inaccessible for unauthorized users. Such codes are the subject of Cryptology.[2]

Another reason would be to compress the information in order to reduce the amount of space needed to store it.

A third reason is to increase safety and accuracy in the storage or transfer of information.

Fourth reason is there are legitimate governmental, commercial and individual needs and uses for cryptography; individuals or entities for illegal activities of their data may also use it

Finally Cryptography is an important component of secure information and communications systems and a variety of applications have been developed that incorporate cryptographic methods to provide data security.[2]

A. Cyrpography System:

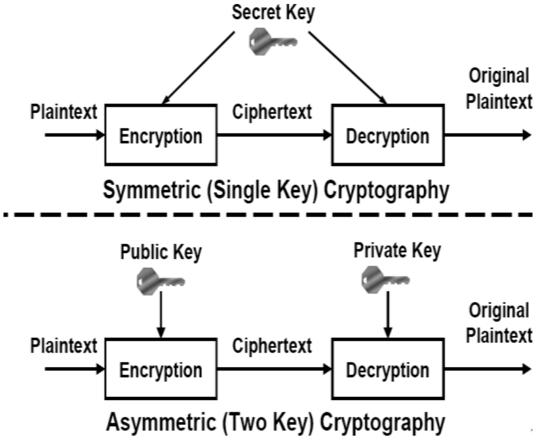


Figure 1: Symmetric and Asymmetric System Model

IV. TYPES OF SUBSTITUTIONS CIPHER

There are 4 kinds of substitution cipher; Mono - alphabetic, Homophonic, PolyGram, Transposition Cipher and Poly - alphabetic methods.

A. Caesar Cipher:

a. Good in theory but not so good in practice.

b. How to make the cipher more difficult can complicated?

c. Cipher text alphabets corresponding to the original plain text alphabets may not necessarily be 3 places down the order, instead, can be any places down the order.[3]

d. Thus, alphabet A in plain text would not necessarily be replaced with D. It can be replaced by any other alphabet.

e. Once the replacement scheme is decided, it would be constant and will be used for all other alphabets in given message.

f. English languages contain 26 alphabets. Thus, A can be replaced by any order in the English alphabet set (B through Z). Not make sense to replace A with A.

g. So, each alphabet have 25 possibilities of replacement.

i. The major weakness of Caesar Cipher is its predictability.

ii. Rather than using a uniform scheme, use random substitution. This means that in a given plain text message, each A can be replaced by any other alphabet (B through Z), each B can also be replaced by any other random alphabet (A or C through Z) and so on.

iii. The crucial difference, there is no relation between the replacement of B and replacement of A. That is, if decided to replace A with D, not necessarily replace each B with E – can replace B with other character.

iv. To put it mathematically, the cipher can have any permutation or combination of the 26 alphabets which means (26 x 25 x 24 x 23 x …2) or 4 x 1026 possibilities!

v. This is extremely hard to crack. It might actually take years to try out these many combinations even with the most modern computers.

B. Homophonic Substitution Cipher:

a. Very similar to Mono-alphabetic Cipher.

b. The difference between the 2 techniques is that replacement alphabet set in simple substitution technique is fixed (A with D..) whereas in the case of Homophonic, one plain text alphabet can map to more than one cipher text alphabet.[3]

c. e.g. A can be replaced by D, H, P, R; B can be replaced by E, I, Q, S….

d. Difficult to analyze compare with mono-alphabetic because the frequency didn't show the real usage of each alphabet.

C. Polygram Substitution Cipher:

a. Rather replacing one plain text alphabet with one cipher text alphabet at a time, a block of alphabets is replaced with another block.

b. Dividing plain text to a group of alphabet does it. This group can be 2 alphabets or more than that.

c. Play-fair Cipher and Hill Cipher are examples of cipher that used Polygram Substitution Cipher.

D. Poly-Alphabetic Substitution Cipher:

a. Leon Battista invented the Polyalphabetic Cipher in 1568. This cipher has been broken many times, and yet it has been used extensively. The Vigenere Cipher and Beaufort Cipher are the examples of it.

b. The cipher uses multiple one-character keys. Each of the keys encrypts one plain text character.

c. The first key encrypts the first plain text character, the second key encrypts the second plain text character and so on.

d. After all the keys are used, they are recycled. Thus, if we have 30 one-letter keys, every 30th character in the plain text would be replaced with the same key.

V. PROPOSED METHODOLOGY

In This method, the plaintext letters are enciphered differently depending upon their placement in the text. As the name poly-alphabetic suggests this is achieved by using several two, three keys and random keys combinations instead of just one.

***Stage1**: using ASCII substitution method*

VI. ALGORITHM

a. Take the example text " Welcome".

b. Take three key e1, e2, e3 and assign a character e1 be 'a' and e2 be 'D' and e3 be 's'.

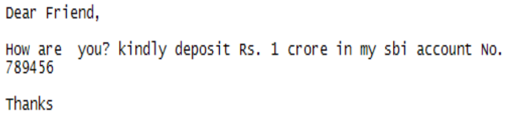
c. Let ASCII value of e1 be 1 and e2 be 2 and e3 be 3 and take the text , add ASCII value of e1 to value of first character, and e2 to second character and e3 to third character, alternatively add the value of e1 , e2, e3 to consecutive characters.

d. Three layers to be applied to each three consecutive letters and same to be continued thru the remaining text.

e. After adding ASCII value of all values of given text, the resultant text is an encrypted message, and it generate a combination of 3* (256 * 256 * 256) letters encrypted coded text with 128 bit manner. [7]

f. Finally takes the ASCII Symbols of of each updated character value in the given text and this process shown in Fig.

A. Input Information:

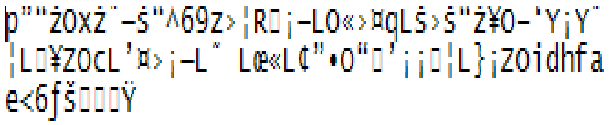


```
Dear Friend,

How are  you? kindly deposit Rs. 1 crore in my sbi account No.
789456

Thanks
```

B. Encrypted Information:



þ""żOxż¨–ś"^69z›¦R□¡–LO«›¤qLŚ›ś"ż¥O–'Y¡Y¨
¦L□¥ZOcL'¤›¡–L˝ Lœ«L₵"•O"□'¡¡□¦L}¡ZOidhfa
e<6fš□□□Ÿ

Method: Cyrpto-steganographic method Algorithm

The above Encrypted message is then is hidden in Image file using LSB with Masking method, The resultant stegano_object send to the receiver.

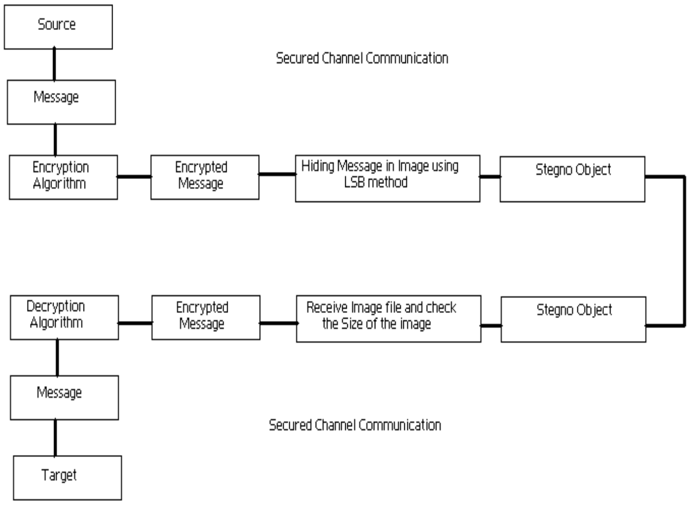

Source
Secured Channel Communication
Message
Encryption Algorithm
Encrypted Message
Hiding Message in Image using LSB method
Stegno Object
Decryption Algorithm
Encrypted Message
Receive Image file and check the Size of the image
Stegno Object
Message
Secured Channel Communication
Target

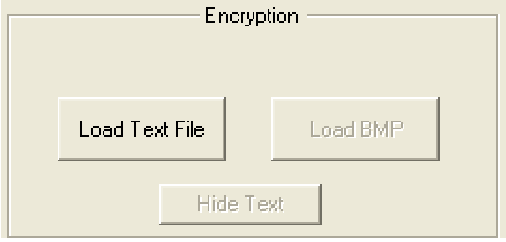
Figure 2: System Flow Diagram –Cyrptic-steganography method

In the receiver side, object is received and then the result is decrypted with substitutions cipher methods(ASCII). [7]

We can use substitution method combining the features of genetic Algorithms and cryptography for text encryption by 2 keys and 3 keys and even more then 3 keys to make the decryption process more complicated.

Stage 2 : Image Steganograpy[9] Encryption process

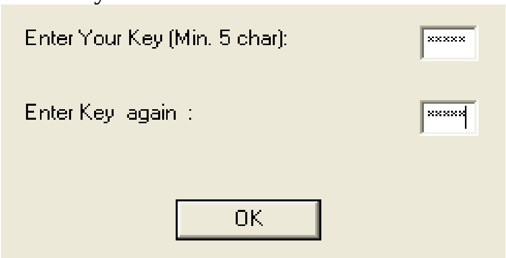
Select Image file, Encrypted Text



Select Image file using Load Bmp

SIZE : 103 KB (BEFORE HIDING DATA)

Select secret key



Enter Your Key (Min. 5 char): *****

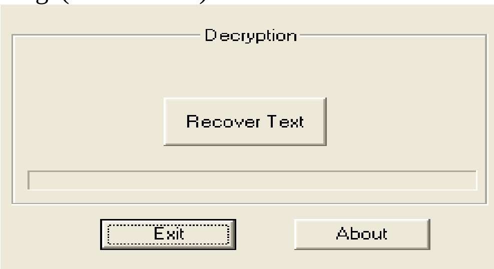
Enter Key again : *****

Output file (After hidden data)

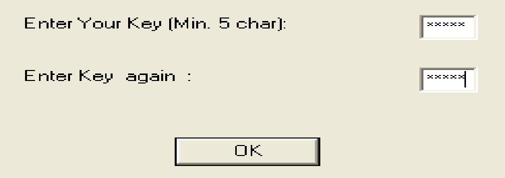
SIZE : 103 KB (After hiding data)

Image Steganograpy Decryption process[8]

Select Image(hidden Data) file



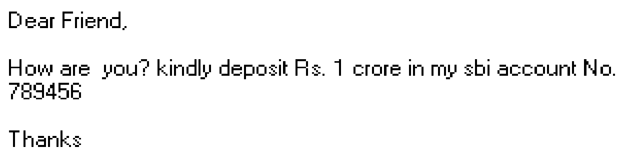
Input your Secret key



Enter Your Key (Min. 5 char): *****

Enter Key again : *****

Output file contain readable message



Dear Friend,

How are you? kindly deposit Rs. 1 crore in my sbi account No. 789456

Thanks

Figure 3

In substitution ciphers the plaintext letters are enciphered differently depending upon their placement in the text. As the name polyalphabetic suggests this is achieved by using several two, three keys and random keys combinations instead of just one, as is the case in most of the simpler crypto systems.

Using two keys, we take 2 keys e1,e2 and let the ASCII values of e1 be 1 and e2 be 2 and take the text, add ASCII values of e1 to first character and ASCII values of e2 to second character. Alternatively add the value of e1 and e2 to consecutive characters.

Encrypted message is then compressed; this file is hidden in Image file using LSB method, The resultant object send to the receiver.[9]

In the receiver side, object is received and then unzipped using the methods then the result is decrypted with substitutions cipher methods.

Poly substitution method(e-cipher) combining the features of genetic keys methods with features of Steganography with cryptography for text encryption by 2 keys and 3 keys and even more then 3 keys to make the decryption process more complicated.

VII.KEYWORDS

- **Encryption:** The process of putting text into encoded form
- **Genetic algorithm (GA):** Search/optimization algorithm based on the mechanics of natural selection and natural genetics
- **Key:** A relatively small amount of information that is used by an algorithm to customize the transformation of plaintext into cipher text (during encryption) or vice versa (during Decryption)
- **Key length:** The size of the key - how many values comprise the key?
- **Monoalphabetic:** Using one alphabet - refers to a cryptosystem where each alphabetic character is mapped to a unique alphabetic character
- **Mutation:** Simulation of transcription errors that occur in nature with a low probability - a child is randomly changed from what its parents produced in mating
- **Order-based GA:** A form of GA where the chromosomes represent permutations. Special care must be taken to avoid illegal permutations
- **Plaintext:** A message before encryption or after decryption, i.e., in its usual form which anyone can read, as opposed to its Encrypted form.
- **Polyalphabetic:** Using many alphabets - refers to a cipher where each alphabetic character can be mapped to one of many possible alphabetic characters
- **Population:** The possible solutions (chromosomes) currently under investigation, as well as the number of solutions that can be investigated at one time, i.e., per generation
- **Block:** A sequence of consecutive characters encoded at one time.
- **Block length:** The number of characters in a block
- **Chromosome:** The genetic material of an individual - represents the information about a possible solution to the given problem.
- **Cipher:** An algorithm for performing encryption (and the reverse, decryption) - a series of well-defined steps that can be followed as a procedure. Works at the level of individual letters, or small groups of letters.
- **Ciphertext:** A text in the encrypted form produced by some cryptosystem. The convention is for cipher texts to contain no white space or punctuation.
- **Crossover (mating) :** Crossover is the process by which two chromosomes combine some portion of their genetic material to produce a child or children.
- **Cryptanalysis:** The analysis and deciphering of cryptographic writings or systems.
- **Cryptography:** The process or skill of communicating in or deciphering Secret writings or ciphers
- **Cryptosystem:** The package of all processes, formulae, and instructions for encoding and decoding messages using cryptography.
- **Decryption:** Any procedure used in cryptography to convert cipher text (encrypted data) into plaintext.

- **Diagram:** Sequence of two consecutive characters.
- **Encryption:** The process of putting text into encoded form.
- **Fitness:** The extent to which a possible solution successfully solves the given problem - usually a numerical value.
- **Generation:** The average interval of time between the birth of parents and the birth of their offspring - in the genetic algorithm Case, this is one iteration of the main loop of code.
- **Genetic algorithm (GA) :** Search/optimization algorithm based on the mechanics of natural selection and natural genetics.
- **Mutation:** Simulation of transcription errors that occur in nature with a low probability - a child is randomly changed from what its parents produced in mating.
- **Trigram:** Sequence of three consecutive characters.
- **Unigram:** Single character.

VIII. CONCLUSION

The Proposed methodology will give the new area of research on cryptography with combined features of Steganography with reference to Substitution ciphers Methods. This new methodology for text encrypts and decrypt using E- Cipher Methods with reference to ASCII combining the features LSB code method is definitely an effective method and was implemented using C++ software tool , it works fine, shows no changes in before hiding text in images with after retrieving information from image file while compared with other cryptography information security systems.

IX. REFERENCES

[1]. AlekseyGorodilov,Vladimir Morozenko,'Genetic Algorithms for finding the key;s length and cryptoanalysis of the permutation cipher',International Journal of Information Theories and Applications vol.15/2008, PP- 94-99.

[2]. Bethany Delman,'Genetic Algorithms in Cryptography' M.S. Thesis Submitted in Rochester Institute of Technology, Kate Gleason College of Engg, July 2004. (ME Thesis published online)

[3]. Darrell Whitley,'A Genetic Algorthm Tutorial', Computer Science Department, Colorado State University, Fort Collins, CO 80523 PP. 1-37.(Unpublished)

[4]. Neal Koblitz, ,'A course in number theory and Cryptography', Springer-Verlag,((ISBN 3-540-94293-9), New York, INc, Second Edition, 1994.

[5]. Nalani N, G. Raghavendra Rao,' Cryptanalysis of Simplified Data Encryption Standard via Optimisation Heuristics;IJCSNS, Vol.6 No.1B, January 2006.PP 240-246.

[6]. Sujith Ravi, Kevin Knight,'Attacking Letter Substitution Ciphers with Integer Programming',Oct 2009,; Proquest Science Journals volume 33, issue 4, september 2009 ,
PP. 321-334.

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

[8]. Sujay Narayana1and Gaurav Prasad, two new approaches for secured image Steganography using cryptographic Techniques and type conversions, SIPIJ Vol.1, No.2, December 2010 PP 60 –73.

[9]. R.Amirtharajan, A Comparative Analysis of Image Steganography, International Journal of Computer Science , Volume 2 – No.3, May 2010 ,PP 41-47

Short Biodata of the Author

R. Venkateswaran received his professional degree MCA and MBA(IS) from Bharathiar University, Tamilnadu, India, He received his M.Phil from Bharathidasan University, Tamilnadu , India, and He is currently a PhD 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 a Asst. Professor of Computer Applications, GR Govindarajulu School of Applied Computer Technology, (PSGR Krishnammal College for Women), Coimbatore, Tamilnadu. He is the member of CSI, IAENG, IACSIT, and many online IT forums. He had published seven International Journals and Presented more papers in national and International conferences, seminars and workshops. His research interests are in Cryptography and network security, information security, Software engineering,

Dr. V. Sundaram received his professional degree M.Sc. in Mathematics from the University of Madras in the year 1967 and he received his Professional Doctoral Degree Ph. D in Applied Mathematics from the University of Madras in 1989. and He worked in PSG College of Technology & polytechnic, Kumuraguru College of Technology and also worked in Ibra College of Technology, Sultanate of Oman. He is currently working as Director, Department of Computer Applications in Karpagam College of Engineering, Tamilnadu, India , He is a research Guide for Anna university , Bharathiar university as well as Karpagam University in the field of Computer applications. He had organized 1 international conference and 4 national level conference/ seminars in the area of computer science. He published several papers in International Journals and Conferences and also published 13 books in the area of engineering mathematics and he is the life member of ISTE and ISIAM. His research interests are in Cryptography and network security, Applied Mathematics, Discrete Mathematics, Network etc.