Research Journal of Computer and Information Technology Sciences _____E-ISSN 2320 – 6527
Vol. **4(4),** 16-18, April **(2016)** *Res. J. Computer and IT Sci.*

Secure Data Transmission "Integration of Genetic Algorithm and Visual Cryptography Technique"

Aayasha Kausar* and Deepty Dubey
Department of Computer Science and Engineering, Chhatrapati Shivaji Institute of Technology, Durg, Chhattisgarh, India
angel.aaysha@gmail.com

Available online at: www.isca.in, www.isca.me
Received 24th February 2016, revised 17th March 2016, accepted 12th April 2016

Abstract

Integrity, security, non-repudiation, confidentiality, and authentication services are the imperative elements in data security. Presently days the security of information draws much attention, particularly when these information are send through the communication network or put away in memory. Cryptography is a technique for sparing and transmitting information in a specific form so that those for whom it is proposed can read it and process it. For secure data transmission this work presented a system which uses genetic algorithm, steganography along with visual cryptography. Genetic algorithm is used for encryption where plain text is converted into cipher text then it is hidden in LSB pixels of an image using Steganography technique. Visual cryptography technique is then used to divide the image into multiple shares to provide security and reliability for data transmission over network. Digital signature is used for authentication.

Keywords: Cryptography, Genetic Algorithm, Steganography, Digital Signature, Visual Cryptography.

Introduction

Cryptography: Cryptography is the method of making communication unreadable to everybody with the exception of the proposed receiver(s). It is the investigation of techniques for sending data in confused form so that just proposed beneficiaries can understand and read the data. Cryptography gives the efficient solution for secure sensitive data in an extensive number of application, for example, internet security, data security, diplomatic and military communications security, etc. using the processes of encryption/decryption. Encryption and decryption are the key concept of cryptography[1].

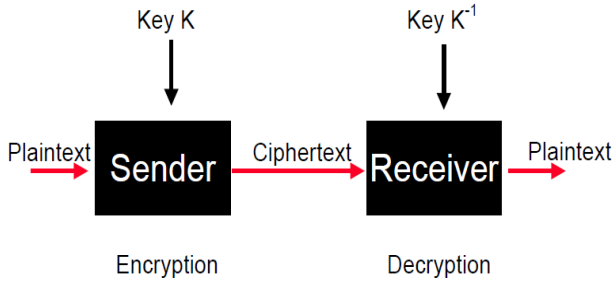

Figure-1
Encryption and decryption

Steganography: The word steganography is originated from the Greek words stegos significance cover and grafia significance writing[2]. It defining as covered writing. In picture steganography the information is hidden behind pictures. Steganography is art and science of secret communication. It is the process of encoding the secret data in a manner such that the existence of the data is invisible.

Visual Cryptography: Visual cryptography is a cryptography procedure that permits visual data (pictures, content, and so forth.) to be scrambled in a manner that decoding can performed by human visual framework. No need of any complex cryptographic calculation. Visual cryptography was presented by Moni Naor and Adi Shamir. They have given a visual mystery sharing plan, where a picture was separated into n offers in a manner that all n offers required to decode the picture, and any n –1 offers uncovered no data about the first picture.

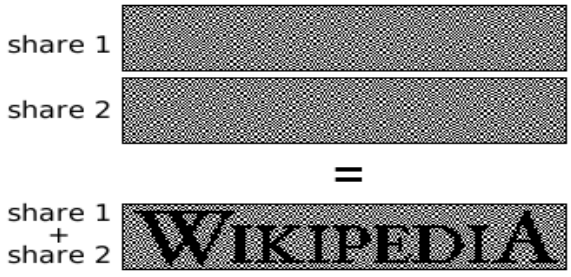

Figure-2
Visual cryptography

Genetic Algorithm: Genetic algorithms are adaptive evolutionary algorithms. It is based on the natural selection[3]. A Genetic algorithm has turned out to be effective and dependable improvement procedure in a wide assortment of uses. It can be applied to texts and images. Since Genetic algorithm does not utilize the natural numbers directly so it is secure. A simple GA

uses following operators to transform a population into new population[4]:

Crossover: Crossover is a process of joining two chromosomes to form a new chromosome. It is a genetic operator. From parents the newly chromosome is generated called child chromosome. Crossover-rate affects the number of crossovers.

Mutation: Mutation is process of changing one or more bit values in a chromosome. After crossover operation it is performed on child.

Selection: Selection is process of selecting best chromosomes for the process of crossover. The chromosome with more fitness value will be considered better.

Digital Signature: Digital signature is message authentication technique that gives the authority to the creator of a message to attach a code that act as signature. By taking the hash estimation of the message signature is made. Hash of message is scrambled with sender's private key.

Literature Review

Naor and Shamir have given a Visual cryptography, a new type of cryptographic technique. This technique is very easy to implement and perfectly secure. They have given visual secret sharing technique, where a picture was separated into n shares in a manner that all *n* shares required to decrypt the picture, and any $n-1$ shares revealed no information about the original picture[3].

Genetic algorithms are adaptive evolutionary algorithm. It is based on the idea of natural selection. A genetic algorithm is very powerful and reliable optimization technique in a wide variety of applications. It can be used for both texts and images. Since Genetic algorithm does not utilize the natural numbers directly so it is secure[6].

A paper entitled "Cryptography Using Genetic Algorithm" has been published by Sonia Goyat. They have given distinctive methods of cryptography to demonstrate that the Genetic algorithm based techniques are as good as the other mathematical techniques[7].

For Printing and Scanning Visual cryptography is given by Yan, Jin and Kankanhalli. In their paper, they have given the solution for problem of precise alignment for printing and scanning visual cryptography sharing. They have given experimental results. These results show that their technique can be useful for print and scan applications[8].

Proposed Methodology

The proposed methodology can be divided into following parts: i. Data encryption using Genetic algorithm. ii. Encrypted data hiding using LSB technique. iii. Applying Visual cryptography to secure image. iv. Attach Digital Signature to ensure Authentication.

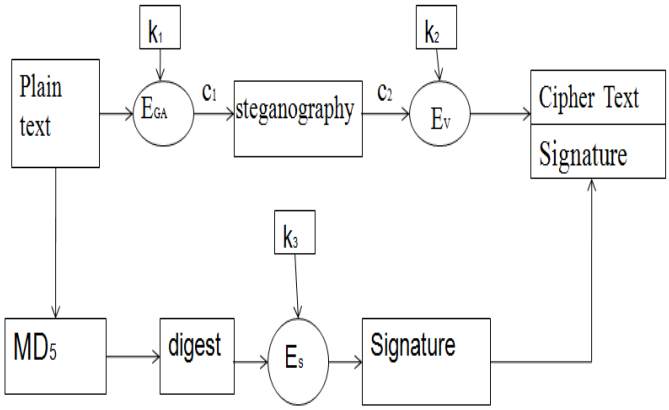

Figure-3
Confidentiality and authentication for sender side

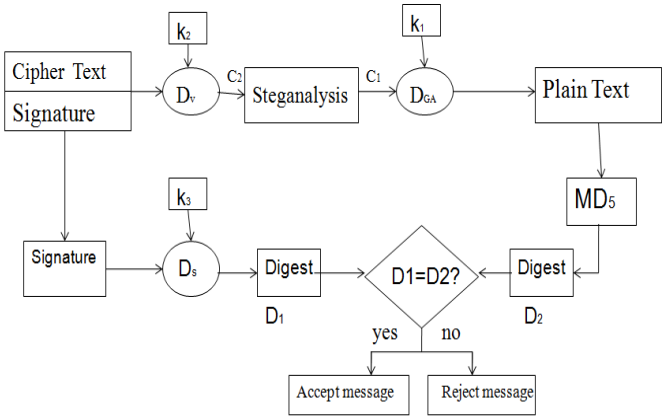

Figure-4
Confidentiality and authentication for receiver side

The data is first encrypted using Genetic Algorithm. The encrypted data is then embedded in the image using Steganography. Multiple shares of single image are created using Visual Cryptography technique. Until and unless the destination end or user has full share of images it's hard to decrypt. Digital signature is attached to ensure authentication. Decryptiion process is reverse of it.

Conclusion

Data security is one of the important fields of research and researchers also showing their interest in developing technique which provides high security to the data. The proposed system provides high security to data. It also ensures confidentiality, authentication, non-repudiation and integrity. The proposed system can be implemented using different encryption algorithm in future as needed. The proposed system can also be implemented using any number of encryption algorithms but the security should be taken into consideration.

References

1. Douglas and Stinson R. (1995). Cryptography- Theory and Practice. CRC Press, Newyork, USA.

2. Anderson R. and Petitcolas F. (1998). On the limits of steganography. *IEEE Journal of Selected Areas in Communications*, 16(4).

3. Naor M. and Shamir A. (1995). Visual Cryptography. In proceeding of advances in cryptography Eurocrypt, Springer-Verlag, Berlin, 1-12.

4. Sivanandam S.N. and Deepa S.N. (2008). Introduction to Genetic Algorithm. Springer Verlag, Berlin Heidelberg, New York.

5. Mishra S. and Bali S. (2013). Public Key Cryptography Using Genetic Algorithm. *International Journal of Recent Technology and Engineering (IJRTE),* 2(2), 150-154.

6. Sindhuja K. and Devi P.S. (2014). A Symmetric Key Encryption Technique Using Genetic Algorithm. *International Journal of Computer Science and Information Technology,* 5(1), 414-416.

7. Goyat S. (2012). Cryptography Using Genetic Algorithms (GAs). *IOSR Journal of Computer Engineering,* 1(5), 06-08.

8. Yan W., Jin D. and Kankanhalli M.S. (2012). Visual Cryptography for Print and Scan applications. International Symposium on Circuits and Systems, 5.

9. Singh D., Rani P. and Kumar R. (2013). To Design a Genetic Algorithm for Cryptography to Enhance the Security. *International Journal of Innovations in Engineering and Technology (IJIET),* 2(2), 380-385.

10. William S. (2011). Cryptography and Network Security (5^{th} edition), Noida, India, Dorling Kindersley.