

Secure Data Transmission by Combining Genetic Algorithm and Steganography Techniques with Visual Cryptography Technique

Aayasha Kausar, Deepty Dubey

M.Tech scholar, Dept. of Computer Science & Engg..CSIT, Durg (C.G.), India

Associate Professor, Dept. of Computer Science & Engg., CSIT, Durg (C.G.), India

ABSTRACT: Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Steganography is method of hiding information behind multimedia file such as text, image, audio, video. The current work proposes a scheme that uses the combined approaches of Genetic Algorithm, Steganography, and Visual Cryptography for secure transmission of data over network. 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.

KEYWORDS: Cryptography, Genetic Algorithm, Steganography, Visual Cryptography.

I.INTRODUCTION

Security, integrity, non-repudiation, confidentiality, and authentication services are becoming the most challenging issues in today's age of information technology. For secure communication means of electronic cryptography is used. Cryptography is concerned with encoding and decoding of information to ensure the security. [2]

A. GENETIC ALGORITHM

Genetic algorithms are evolutionary algorithms based on the notion of natural selection [4]. A genetic algorithm has proven to be reliable and powerful optimization technique in a wide variety of applications. It can be applied to both texts and images. Genetic algorithm is secure since it does not utilize the natural numbers directly. The results obtained for generating keys using genetic algorithm should be good in terms of coefficient of autocorrelation. Generally genetic algorithm has two basic functions namely Crossover and mutation [5]. Crossover is genetic process where random bits of parent genes are swapped in order to generate offspring. There are many types of crossover techniques such as single point crossover, two point crossovers, and uniform crossover [6]. In this paper approach of two point crossover technique is used. Figure1 shows two point crossover approaches where child chromosomes are produced from parent chromosomes.

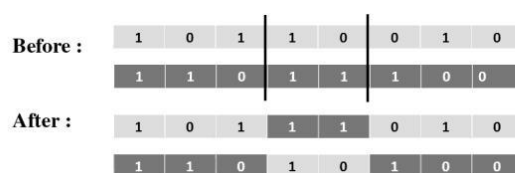


Figure 1: Two Point Crossover

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Mutation shows genetic diversity. In this process the generated offspring is having properties of both its parent chromosomes i.e. the genes of both the parents are randomly incorporated in the offspring. There are many types of mutation such as flipping of bits, boundary mutation, uniform mutation and Gaussian mutation. In this paper flipping of bit technique is used.

B. VISUAL CRYPTOGRAPHY

The basic idea of visual cryptography is that secret image is divided into several parts called shares, which separately reveal no information about the secret image. By stacking these shares directly, secret image can be revealed. Visual cryptography is a new technique which provides information security which uses simple algorithm unlike the complex, computationally intensive algorithm used in other technique like traditional cryptography. This technique allows Visual information to be encrypted in such a way that their decryption can be performed by the human visual system, without any complex cryptographic algorithms [3].

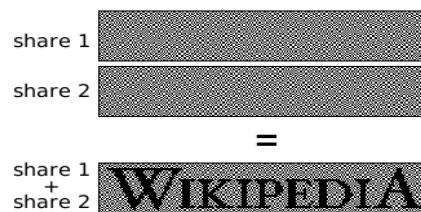


Figure 2: Visual Cryptography Technique

We can achieve Visual Cryptography Scheme (VCS) by one of the following access structure schemes.

1. **(2, 2) - Threshold VCS scheme**- This is a simplest threshold scheme that takes a secret message and encrypts it in two different shares.
2. **(n, n) -Threshold VCS scheme**-This scheme encrypts the secret image to n shares such that when all n of the shares are combined will the secret image be revealed.
3. **(k, n) Threshold VCS scheme**- This scheme encrypts the secret image to n shares such that when any group of at least k shares are overlaid the secret image will be revealed.

C. STEGANOGRAPHY

Steganography is the science of embedding information into the cover like text, video, and image. Steganography can be divided into 5 types:

1. Text Steganography
2. Image Steganography
3. Video Steganography
4. Audio Steganography
5. Protocol Steganography

D. LSB TECHNIQUE

The simplest and most common type of Steganography is LSB (least significant bit). The one's bit of a byte is used to encode the hidden information.

Example: Suppose we want to encode the letter A (ASCII 65 or binary 01000001) in the following 8 bytes of a carrier file.

```
01011101  11010000  00011100  10101100  11100111
10000111  01101011  11100011
```



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Becomes

01011100 11010001 00011100 10101100 11100110
10000110 01101010 11100011

II. LITERATURE REVIEW

Moni Naor and Adi Shamir (1995) proposed visual cryptography technique. Visual cryptography scheme is perfectly secure and very easy to implement. It extends image into a visual variant of k secret sharing problem. Any k of them can see the image but any k-1 of them gain no information about it [1].

Dr. Dilbagh singh, Pooja Rani, Dr. Rajesh Kumar (2013) suggested a genetic algorithm design for cryptography for enhancing the security. In the model the concept of genetic algorithm has been incorporated within cryptography algorithm to get an optimized solution and within minimum possible time [7].

In the technique used by Sindhuja K, Pramela Devi S.(2014) the Symmetric Key encryption technique is combined with Genetic algorithm. The GA functions are applied on the intermediate cipher to produce the final cipher text. The proposed algorithm has basic two steps, substitution followed by genetic crossover and mutation [8].

Swati Mishra, Siddharth Bali (2013) presented public key cryptography using Genetic Algorithm. In this paper Pearson's Coefficient of auto-correlation was used to calculate the fitness of key. Purely random and non-repeating final keys were obtained by application of GA which increased the key strength and security [9].

Chandramathi S., Ramesh Kumar R., Suresh R., and Harish (2010) presented an overview of visual cryptography. In this paper they provide an overview of emerging Visual Cryptography (VC) and related security research work done in this area [3].

III. PROPOSED METHODOLOGY

The data is first encrypted using advanced encryption technique 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. Decryption process is reverse of it.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

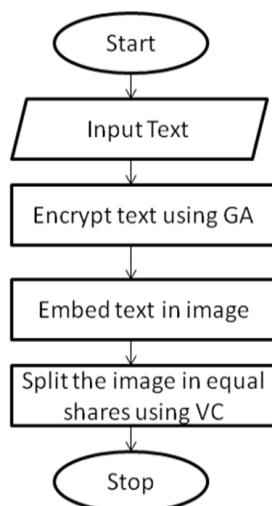


Figure 3: Advanced Encryption Technique

The proposed work will be divided into following phases:

Phase1: Data encryption using Genetic Algorithm.

Phase2: Encrypted data hiding using LSB Steganography.

Phase3: Applying Visual cryptography for secure image and data transfer.

IV. CONCLUSION

The proposed algorithm provides better result in terms of security. It is concluded that the security features of genetic algorithm are highly optimized using Steganography and visual cryptography. Visual cryptography also ensures the secure transmission of image over the internet. The future work could be toward adding public key encryption and also face recognition facility for the user to introduce more security.

REFERENCES

1. Moni Nair and Adi Shamir, Visual cryptography Weizmann Institute Israel (1995)
2. Douglas, R. Stinson, Cryptography- Theory and Practice, CRC Press, 1995
3. Chandramathi S., Ramesh Kumar R., Suresh R. And Harish S., An overview of visual cryptography, vol.1, issue 1, 2010
4. S., N. Sivanandan, S. N. Deepa, Introduction to Genetic Algorithm, Springer Verlag Berlin Heidelberg, 2008
5. M. Mitchell, An Introduction to Genetic Algorithm, The MIT Press, Cambridge, USA, 1999 [6] Harsha Bhasin, Ramesh Kumar, 6. Neha Kathuria, Cryptography using cellular Automata, International Journal of Computer Science and Information Technology, Vol. 4(2), 2013
7. Dr. Dilbag Singh, Pooja Rani, Dr. Rajesh Kumar, To Design a Genetic Algorithm for Cryptography to Enhance the Security, IJNET, Vol.2(2), 2013
8. Sindhuja K, Prameela Devi S, A Symmetric Key Encryption Technique Using Genetic Algorithm, IJCSIT, Vol.5(1), 2014
9. Swati Mishra, Siddharth Bali, Public Key Cryptography Using Genetic Algorithm, IJRTE, Vol.2(2), 2013
10. Genetic Algorithm in Cryptography, Bethany Delman, MS Thesis, 2004
11. Sonia Goyat, Cryptography Using Genetic Algorithms, IOSR Journal of Computer Engineering (IOSRJCE), Vol.1 (5), 2012

BIOGRAPHY

Aayasha Kausar, female obtained the B.E. degree in Computer Science & Engineering from Chhattisgarh Institute of Technology, Rajnandgaon, Chhattisgarh, India, in 2012. Currently she is pursuing M.Tech from Chhatrapati Shivaji Institute of Technology, Durg, and Chhattisgarh, India. Her current research interest is in Cryptography.



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Mrs. Deepty Dubey, female obtained the B.E. degree in Computer Science & Engineering from Shri Shankaracharya College of Engineering & Technology, Bhilai, Chhattisgarh, India, in 2005, the MTech. degree in Computer Science & Engineering, Rungta College of Engineering & Technology, Bhilai, and Chhattisgarh, India. in 2010. She is currently an Associate Professor in Chhatrapati Shivaji Institute of Technology, Durg, and Chhattisgarh, India. Her current research interests are in Cryptography and Cloud Computing.