Three Tier Approach for Secure Data Transmission by Using Steganography, Logistic Maps with Genetic Algorithm and Visual Cryptography

Vamsi Krishna.Y , Varuni.R.V, Shivaranjini.A
Department of Information Science, Sri Krishna Institute of Technology, Bangalore-90
yvnvk.1229@gmail.com , varuni.venus@gmail.com, satheight@gmail.com

ABSTRACT-With advancement of technology, providing security to the data being transmitted is becoming a challenging task. So this paper mainly focuses on enhancing the existing steganography technique with additional feature of visual cryptography for the purpose of securing data hidden in image which is being accomplished through a 3 layered approach, first layer deals with high degree randomization of pixel selection for, LSB based steganography with logistic maps to reduce image degradation. The resulting stego-image undergoes shuffling based on genetic algorithm which builds up the second wall of security. Visual cryptography forms the third layer of security where transparencies of image are transmitted.

Keywords—Genetic Algorithm, Image Security, Logistic Maps, Steganography and Visual Cryptography.

1. INTRODUCTION

The method of concealing confidential messages within a media file that may be picture, vedio clip, audio is steganography. The purpose of steganography is to avoid illegal accessors from differentiating between Data Embedded Image and Plain Image.

Spatial domain, transform domain, spread spectrum and model based steganography are the types of image steaganography. Spatial domain deals with replacement of pixel bits in the image with the secret data. One of the spatial domain steganographic technique is Least Significant Bit(LSB) method. Least Significant Bit(LSB), as the name indicates, is method where LSB of selected pixels are embedded with bits of private data. In this case since their is less degree of randomized pixel selection the selected pixels have higher degree of possibilities of being selected from particular region in the image which results in notifiable degradation in image, as a solution logistic maps has been introduced whose main purpose to randomize pixel selection which results in reduction of degradation in image quality. Genetic algorithm will be implemented on the resulting stego-image to modify and shuffle the pixel location which will be discussed in detail as part of proposed methodology. The image with modified pixel location for the purpose of strengthening the security is broken into two shares before transmitting over network, this constitutes visual cryptography. This method has gained significant importance in the field of biometric security, watermarking, remote electronic voting, bank customer identification.

This paper is organized into four sections. Section I gives brief introduction to the concepts discussed in this paper. Section II deals with related work .Section III deals with discussion of problems in existing system that motivated to come up with this proposal. Section IV describes the various modules involved in the proposed system. Conclusion and future enhancement are discussed in section V.

2. RELATED WORK

Hamidreza et al. [1] proposes genetic algorithm based steganography approach to identify optimal location for embedding data in the image. [2] Mansi S Subhedar discusses the issues in steganography. Anandi et al. [3] proposes various visual cryptography schemes for secret images. Shirish kumbar et al. [4] proposes the use of visual cryptography in various fields like biometric, DNA etc. Rehana Begum R.D et al.[5] proposes the integration of LSB based steganography using genetic algorithm and visual cryptography for secured data hiding . Gokul et al [6]. Proposes a combination of visual cryptography and LSB encryption. Jeyamala chandrasekaran et al. [7] introduces the concept of logistic maps for optimal pixel selection. Fridrich et al. [9] proposes RS algorithm to detect LSB based data embedding in grayscale images. He also proposes F5 algorithm for steganalysis of data hidden in JPEG images et al. [10]. Sonaz Abdulla et al. [11] proposes a new visual cryptography technique of dividing images into transperencies before it is sent over network to improve security. Divya james et al. [12] proposes a visual cryptography based solution for phishing problem. Amritha et al. [13] proposes a genetic algorithm based steganography technique using discrete cosine transformation.

3. EXISTING SYSTEM

The current systems are not capable of higher degree randomized pixel selection in cover image for data embedding. This causes notifiable amount of image distortion which is easily prone to suspection, of data transmission through image. The proposed system provides solution to this problem by applying logistic maps which increases the randomization of pixel selection . In existing systems, after employing visual cryptography, at the decoder end on overlapping the shares, the original stego image is exposed as shown in Fig.2 thus resulting in reduction of security of stego image.

This problem is overcome by employing genetic algorithm which involves crossover and mutation of pixels on the stego image before visual cryptography is applied. As a result, at decoder end, on stacking the transparencies shuffled stego image is obtained and not the original stego image. Thus this enhances the security provided to the image concealing the private data.

4. PROPOSED METHODOLOGY

Logistic equation

Logistic equation portrays complex and chaotic behavior. A study on logistic maps provided a suitable equation for the purpose of key generation:

(1) $x(n) = 2 * (2 - (5 * x(n-1))) * x(n-1)$

Logistic equations are of great importance due to the fact that, very minute change in decimal part of input displays a huge variation in output. Without implementation of logistic equation, the image degradation is visible since pixels are not much randomly selected as shown in Fig.1. In proposed system, logistic equation (1) is incorporated to generate highly random values that are mapped with the pixel positions in the cover image, thus resulting in selection of pixels that are widely distributed and highly random in the cover image for the purpose of embedding data which overcomes the problem of image degradation as shown in Fig.2.


Original image


Pixel selection


Resulting image

Fig.1 Pixel selection without logistic maps.


Original image


Pixel selection


Resulting image

Fig.2 Randomized pixel selection with logistic maps.

Genetic algorithm

Existing systems embed data in the image and this image is given as input to visual cryptography as shown in Fig.3, which divides the image into two shares (explained in detail in the following module) sends it over network. If hacker obtains access to both the shares during transmission, on overlapping these shares, the hidden data can be extracted, the solution to this is genetic algorithm. Genetic algorithms are the class of algorithms that provide solutions for optimization and search problems. Crossover and mutation are the types under genetic algorithm that are made use of in the proposed system. Crossover can be further classified i.e., column shuffling and row shuffling. Column shuffling involves interchanging the pixels of two columns. Similarly row shuffling interchanges the pixel of two rows. In this paper row shuffling follows column shuffling. Mutation is a technique where inversion of pixel is achieved. Thus integration of these two techniques greatly enhances security provided to the stego-image. This method is incorporated in the proposed paper as shown in Fig.4.When hacker overlaps the two shares he obtains shuffled stego image and not the original stego image.


Share 1 Share2 Stego image

Fig.3 Before implementing genetic algorithm.


Share 1 Share 2 Shuffled stego image

Fig.4 After implementing genetic algorithm.

Visual cryptography

The shuffled stego-image resulting from the previous module which is genetic algorithm if transmitted over

network any unauthorized individual who manages to access this image gets access to the whole image that contains the data this problem can be overcome by applying technique such as visual cryptography. Visual cryptography is a prominent technique that divides the image containing the message into two shares such that each of the share contains some part of data before transmitting over the network as shown in Fig.6. Thus provides security for the image containing the data. This method minimizes the risk of data being hacked by intruder. If the intruder manages to illegally access a share of the image during transmission, still the data cannot be revealed since it remains incomplete without the other share. This method is based on interpretation of pixels as binary bits. Each selected pixel is broken into eight subpixels, four pixels for each share. Once the shares are received at the receiver end, they are aligned by invoking reverse visual cryptography process to obtain the shuffled stego image.

Three Tier Approach for Secure Data Transmission by using Steganography, Logistic Maps with Genetic Algorithm and Visual Cryptography

The steps of the algorithm is as shown in Fig. 5

Sender Side Algorithm as shown in Fig.7

Input: Cover image, secret data
Output: Two shares of shuffled stego-image

Step1: Selecting random pixels through logistic maps.
Step2: Embedding secret data in previously selected pixels using LSB technique which is steganography.
Step3: Genetic algorithm is applied on resulting stego image which implements crossover and mutation.
Step4: Visual cryptography divides the shuffled stego image into two shares and sent through the network.

Receiver Side Algorithm as shown in Fig.8

Input: Shares of visual cryptography.
Output: Extraction of secret data.

Step1: Inverse visual cryptography method stacks the shares one over the other obtained at receiver end.
Step2: Output of the previous step is taken as input for inverse genetic algorithm to obtain original stego image.
Step3: Extraction of secret data from the stego image is achieved through inverse steganography process.

The overall design of the proposed system is depicted as shown below:

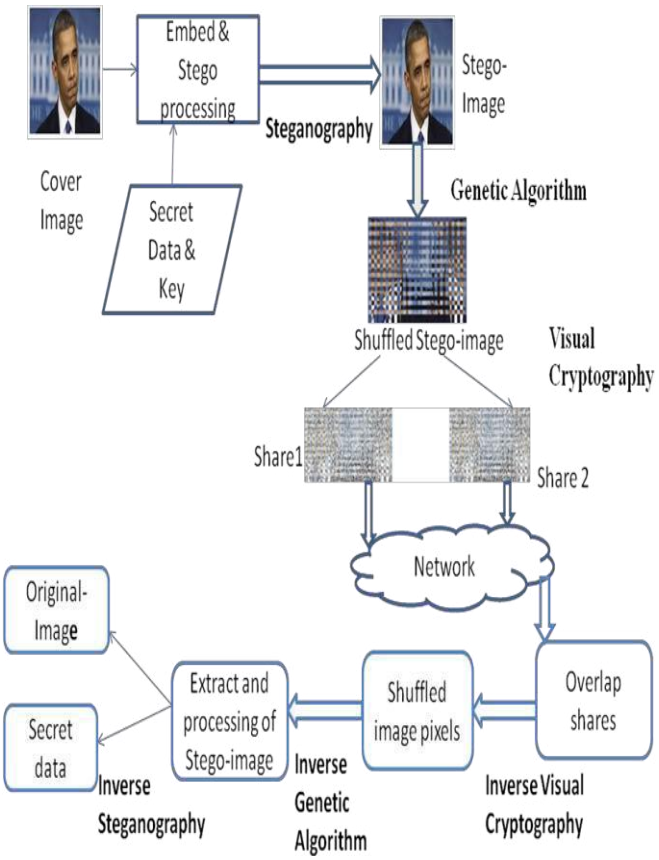

Fig.5 The Proposed Model

The following image depicts the working of simple visual cryptography without the application of genetic algorithm

Share 1 **Share 2** **Final**

Fig.6 Visual cryptography

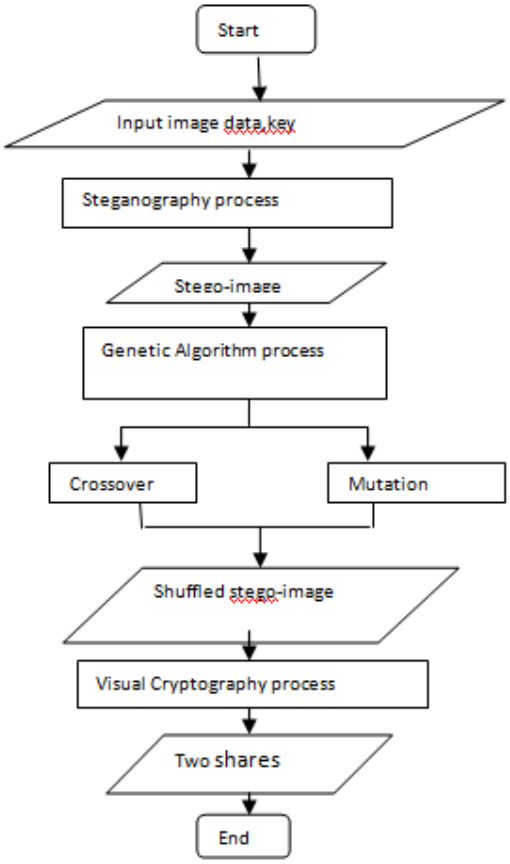

Fig.7 Sender side model

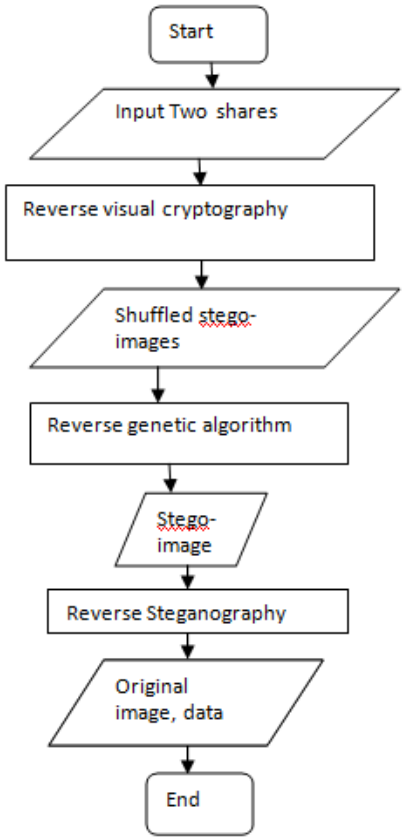

Fig.8 Receiver side model

5. CONCLUSION

This research focuses on enhancing the image security by adding a prominent feature which is visual cryptography to the existing system which integrates logistic maps for random pixel selection, LSB technique for data embedding, genetic algorithm to modify the pixel locations in stego-image.

Future work focuses on reduction of data loss due to imperfect alignment of transparencies and to minimize the interdependencies of shares during transmission.

REFERENCES

[1] Hamidreza Rashidy Kanan , Bahram Nazeri, –A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm, Expert Systems with Applications 41 (2014) 6123–6130.

[2] Mansi S Subhedar, Vijay.H.Mankar,– Current Status and Key issues in Image Steganography‖, Computer Science Review,13-14, 2014, pp95-113.

[3] Anandi,S.Satthiyaraj,‖ Embedded Visual Cryptography Schemes For Secret Images‖,(IJCSNS),vol.12,no.12,dec 2012.

[4] Miss.Shubhangi Rajanwar,Mr.Shirish Kumbar, Mr.Akshay Jadhav,Prof.Saba Siraj,‖ Visual Cryptography For Image Privacy‖,*(IJCST)vol.3* issue2,Mar-Apr2015.

[5] Rehana Begum R.D,Sharaya Pradeep,‖ Best Approach For LSB Based Steganography Using Genetic Algorithm And Visual Cryptography For Secure Data Hiding And Transmission Over Networks‖ ,*(IJARCSSE), vol.4* ,issue6, June2014.

[6] Gokul.M, Umesh Babu.R, Shriram K Vasudevan, Deepak Karthik,‖ Hybrid Steganography Using Visual Cryptography And LSB Encryption Method‖, *(IJCA),[0975-8887],vol59*,no.14,Dec2012

[7] Jeyamala Chandrasekaran , Girija Arumugam, Deepthi Rajkumar, ‖Ensemble Of Logistic maps With Genetic Algorithm For Optimal Pixel Selection In Image Steganography‖,*(ICECS),2015*.

[8] https://www.irjet.net/archives/V2/i5/IRJET-V2I5224.pdf

[9] Fridrich J .,Goljan M and Du R,‖Reliable Detection Of LSB Steganography In Color And Grayscale Images ‖, Proceedings of Workshop on Multimedia and Security, Ottawa,pp.27-30, october 5 2001.

[10] J. Fridrich,M.Goljan and D.Hogea,‖Steganalysis Of JPEG Images:Breaking The F5 Algorithm‖,In proc. Of the ACM Workshop on Multimedia and Security,2002.Sozan Abdulla, –New Visual Cryptography Algorithm For Colored Image‖, *Journal of computing, volume 2*,issue 4, April 2010 .

[11] Divya James, Mintu Philip, "A Novel Anti Phishing framework based on Visual Cryptography", IEEE, 2011.

[12] Amritha Khamrui,J.K mandal, A Genetic Algorithm Based Steganography Using Discrete Cosine Transformation (GASDCT),*International Conference on Computational Intelligence: Modeling, Techniques and Applications(CIMTA)*,2013,pp.105-111.

Author Profile

Y Vamsi Krishna is working as an Associate Professor in the Department of Information Science and Engineering. Has completed his Mtech from VTU with 10 years of experience in teaching .His area of interest is mainly in image processing and artificial intelligence for national and international conference.

Varuni R.V, born on 9th july,1994 pursuing B.E in information science. Studying at Sri Krishna Institute of Technology, Chikkabanavara, Karnataka, India. Areas of Interest are Robotics and Artificial Intelligence

Shivaranjini A, born on 15th october,1994 pursuing B.E in information science. Studying at Sri Krishna Institute of Technology, Chikkabanavara, Karnataka, India. Areas of Interest are Nano Technology and Artificial Intelligence