Use of Genetic Algorithm and Visual Cryptography for Data Hiding in image for Wireless Network

Yogita Patil
Student
Government College of Engineering,
Aurangabad

ABSTRACT
Steganography is method of data hiding behind multimedia file such as text, image, audio and video. For enhancing the security of data hiding and transmission over network, this paper proposed system which uses genetic algorithm along with Visual Cryptography. Plain text is converted into cipher text by using any cipher then it is hidden in LSB of image. Genetic Algorithm is used to shuffle pixel location of image so that detection of secret information become complex. Pixel locations are shuffled using Scan code algorithm. Visual cryptography is kind of encryption technique which divide secret image into multiple shares to ensure improved security and reliability.

General Terms
Secure data transmission.

Keywords
Cryptography, Genetic algorithm, Steganography, Visual cryptography, Wireless network.

1. INTRODUCTION
Steganography is art and science of hiding secret information behind the multimedia files such as text image audio or video so that no one apart from intended recipient knows existence of message. Electronically, stenography can be applied by taking a message in binary form and some sort of cover that may be image or audio file, after combining both the output is known as Stegno-image. The detection of stegnographically encoded package is called Steganalysis. There are Steganalysis techniques which has potential to detect the hidden message by the statistic analysis of pixel values such as RS Steganalysis. The process of RS Steganalysis uses the regular and singular groups as consideration in order to estimate the correlation of pixels [2]. It will be easy to decode the secret information of system which uses Traditional LSB replacing Steganography from the alteration in the singular and regular groups which implies the presence of Steganography.

Steganography and cryptography both are often confusing terms because they use to protect sensitive information. But the difference between both are Steganography involve only to hide information so that it appears no information hidden at all. Human senses are not trained to look for files that have information hidden inside of them.

Steganography especially when combined with cryptography is most powerful tool which enables people to transmit sensitive data over internet securely without possible eavesdropper even knowing there is a form of communication. Visual Cryptography is a kind of encryption technique use to hide data in images and splits the image into number of shares to transmit over network. The combined use of Steganography along with visual cryptography adds lots of challenges to identify such encrypted data but also it is possible for one to have an exposed image which consists of confidential data by reassembling or decrypting encrypted shares to regain image. Also the use of visual cryptography using colored images adds lots of challenges for intruders. Even though there are number of researches related to combination of this two techniques, results are not satisfactory with respect to many Steganalysis techniques. Because of such disadvantage such algorithms cannot persist without addition of some feature to visual cryptography process. Also there are various attacks reported on least significant bytes substitution technique. Various histogram as well as block effect has also been reported in the prior research work [3]. To prevent the impact of such Steganalysis techniques, the pixels locations needs to be shuffled in the image containing sensitive information. And the rearrangement or shuffling of pixel location can be accomplished by using genetic algorithms. Using genetic algorithms the system will become computationally impossible to break. Genetic algorithms are a family of computational models belonging to the class of evolutionary algorithms. In this system the rearrangement of pixels are done by using SCAN patterns generated by SCAN methodology.

This paper is organized into following sections. Section I will contains the introduction about Steganography, Visual cryptography, genetic algorithm. Section II contains the Literature review on some existing papers on Steganography. Section III will contain the description of proposed system. Section IV will give description of algorithms. Finally paper will be concluded.

2. LITERATURE SURVEY
The description of some Steganography techniques along with visual cryptography and genetic algorithms are given in following papers.

Image Encryption and Decryption Using SCAN Methodology is the technique proposed by Chao-Shen Chen and Rong-Jian Chen [4]. This paper proposed Image encryption and decryption techniques using SCAN patterns generated by SCAN Methodology. The encryption method is based on rearrangement of the pixels. The scanning path sequences fill in the original image. The SCAN is a language-based two-dimensional spatial-accessing methodology which can efficiently specify and generate wide range of scanning paths [4].

New Visual Cryptography Algorithm for colored image, is algorithm was proposed by Sozan Abdulla [5]. The proposed algorithm is for color image that presents a system which takes four pictures as an input and generates three images which correspond to three of the four input pictures [5]. For extended visual cryptography with better color quality it needs to establish sophisticated color mixing.

A Novel Anti Phishing Framework based on visual cryptography, is technique was proposed by Mintu Philip and

Divya James [6]. They proposed this technique to solve the problem of phishing. Here image based authentication using visual cryptography is implemented. This method provides additional security in terms of not letting intruder log into the account even when the user knows username of particular user.

Securing Visual cryptography shares using Public key encryption, is the technique proposed by Kulvindar Kaur and Vineeta Khemchandani [7]. The Paper proposed an approach for encrypting visual cryptographically generated image shares using public key encryption. RSA algorithm is used for providing the double security of secret document. Thus secret share are not available in their actual form for any alteration by the adversaries who try to create fake shares.

3. PROPOSED SYSTEM

The proposed system model of the application of data hiding in image using genetic algorithm and visual cryptography is as shown in the figure 1. The proposed system will be divided into four phases.

Phase I: Data Encryption using any Encryption algorithm

Phase II: Encrypted data hiding using LSB Steganography

Phase III: Genetic algorithm to shuffled modified image bits

Phase IV: Applying visual cryptography for securing the modified image.

The task of each phase is explained as below. The output of each phase will be feed as input to the next phase.

The data string consists of user credentials such as login id and password are encrypted before sending to server using any encryption algorithm. Then the cover image which will be used to hide secret message is taken as input. After taking cover image and encrypted credentials the LSB Steganography is used for encrypted data hiding. This step of embedding data in an image will not cause any significant difference in the image visibility. Data is secured using this Steganography, if any intruder sees the image; he/she will not know whether it's a data transfer or image transfer. LSB Steganography has high embedding capacity and low computation complexity, in which a secret binary sequence is used to replace the least significant bits of the host medium [1]. As there are several attacks against LSB, it is required to more secure so concept of genetic algorithm is introduced. Genetic algorithm is used to shuffle modified image bits and image bits are shuffled using scan code algorithm. Before transmitting this data over internet visual cryptography is applied for securing the modified image. Image is dividing into number of shares using visual cryptography and these shares are then sent to server.

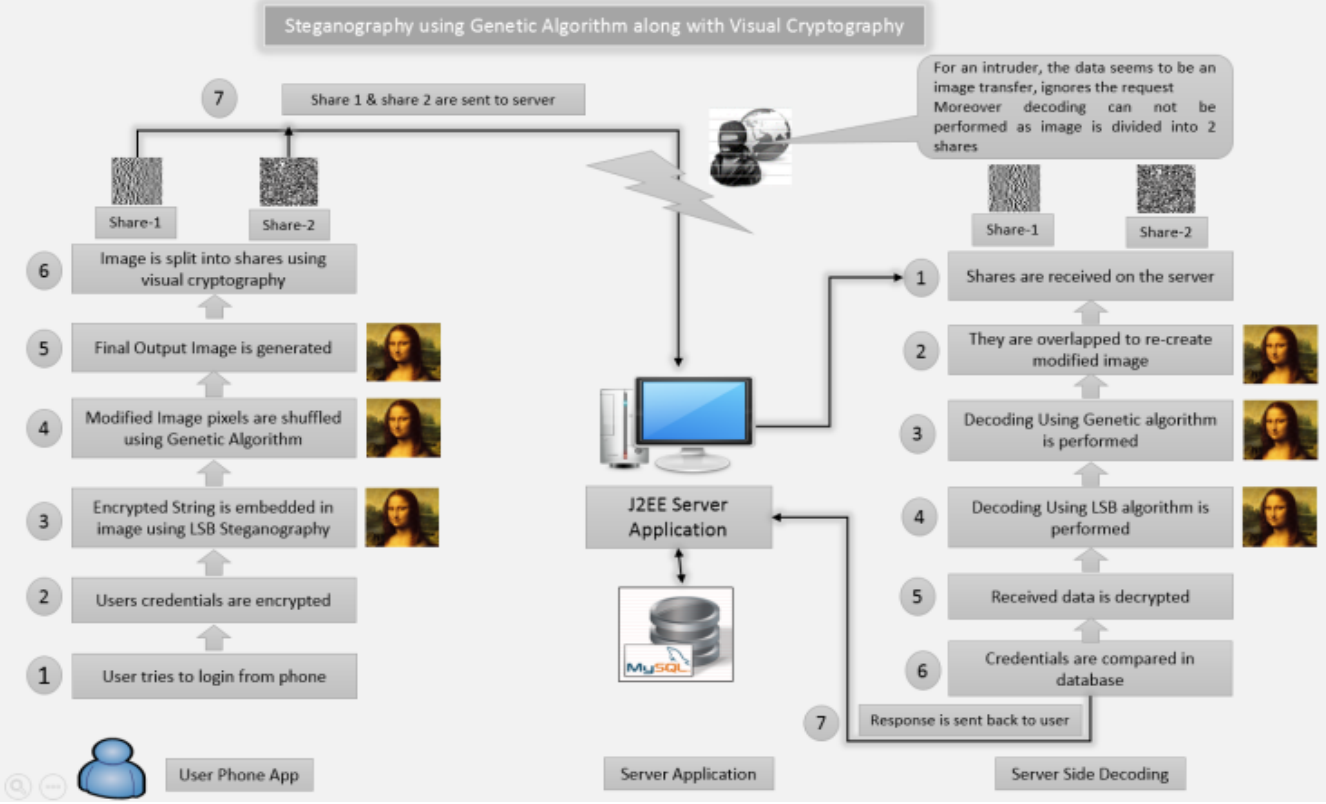

Fig 1: Steganography using genetic algorithm and visual cryptography

4. ALGORITHM DESCRIPTION

This section will discussed about algorithms. The proposed system will contain mainly two algorithms (i) Steganography using Genetic algorithm (ii) Visual cryptography algorithm.

The application will take credential to secure as input and will generate secured image as output containing secret data. This image is then feed as input to the visual cryptography algorithm.

Algorithm1: Steganography using genetic algorithm

Step 1: Read Encrypted user credentials.

Step 2: Read the image for hiding data.

Step 3: Find out the pixel values of that image.

Step 4: Encrypted string is embedded in image using LSB Steganography

Step 5: Modified image pixels are shuffled using genetic algorithm

Step 6: Image is divided into 8*8 blocks.

Step 7: Blocks are repositioned by the needed number of predefined scanning algorithm to shuffle image structure.

Algorithm2: Visual cryptography technique

Step 1: Read the output of Algorithm1 as input.

Step 2: This image file is first converted into a binary image

Step 3: Then each pixel in the secret image is broken into 8 sub pixels, 4 pixels in each share by selecting the random pixel

Step 4: This shares are then transmitted over network.

5. CONCLUSION

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

6. REFERENCES

[1] Mrs. G. Prema, S. Natarajan, "Steganography using genetic Algorithm along with visual Cryptography for Wireless Network Application", International conference on information communication and embedded systems (ICICES), 2013.

[2] 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.

[3] 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.

[4] Chao-Shen Chen, Rong-Jian Chen, "Image Encryption and Decryption Using SCAN Methodology", Proceedings of the Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'06), 2006.

[5] Sozan Abdulla, "New Visual Cryptography Algorithm For Colored Image", Journal of computing, volume 2, issue 4, April 2010.

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

[7] Kulvinder Kaur, Vineeta Khemchandani, "Securing Visual Cryptographic Shares using Public Key Encryption ", IEEE, 2012.

[8] Souvik Roy and P. Venkateswaran, "Online Payment System using Steganography and Visual Cryptography", Students' Conference on Electrical, Electronics and Computer Science, 2014.