Steganography using Genetic Algorithm along with Visual Cryptography for Wireless Network Application

Mrs.G.Prema[1]
Department of ECE,
Mepco Schlenk Engineering College,
Sivakasi, India.

S.Natarajan[2]
Department of ECE,
Mepco Schlenk Engineering College,
Sivakasi, India.

Abstract— **Image steganography is an emerging field of research for secure data hiding and transmission over networks. The proposed system provides the best approach for Least Significant Bit (LSB) based steganography using Genetic Algorithm (GA) along with Visual Cryptography (VC). Original message is converted into cipher text by using secret key and then hidden into the LSB of original image. Genetic Algorithm and Visual Cryptography has been used for enhancing the security. Genetic Algorithm is used to modify the pixel location of stego image and the detection of this message is complex. Visual Cryptography is used to encrypt the visual information. It is achieved by breaking the image into two shares based on a threshold. The performance of the proposed system is experimented by performing steganalysis and conducting benchmarking test for analysing the parameters like Mean Squared Error (MSE) and Peak Signal to Noise Ratio (PSNR). The main aim of this paper is to design the enhanced secure algorithm which uses both steganography using Genetic Algorithm and Visual Cryptography to ensure improved security and reliability**.

Keywords—**steganography, visual cryptography, genetic algorithm, steganalysis.**

I. INTRODUCTION

Hiding information by embedding secret data into an innocuous medium is often referred to as steganography. Steganography can be applied electronically by taking a message (a binary file) and some sort of cover (often a sound or image file) and combining both to obtain a "stego-object". The RS analysis is considered as one of the most famous steganalysis algorithm which has the potential to detect the hidden message by the statistic analysis of pixel values [1]. The process of RS steganalysis uses the regular and singular groups as the considerations in order to estimate the correlation of pixels [2]. The presence of robust correlation has been witness in the adjacent pixels. But unfortunately using traditional LSB replacing steganography [3], the system enders the alteration in the proportion in singular and regular groups which exposes the presence of the steganography. Ultimately, it will not be so hard to decrypt the secret message. Both the topic of steganography and visual cryptography has been considered as a distinct topic for image security. Although there are extensive researches based on combining these two approaches [4] [5] [6], but the results are not so satisfactory with respect to RS analysis. Other conventional methods of image security has witnessed the use of digital watermarking extensively, which embeds another image inside an image, and then using it as a secret image [7]. The use of steganography in combination visual cryptography is a sturdy model and adds a lot of challenges to identifying such hidden and encrypted data. Fundamentally, one could have a secret image with confidential data which could be split up into various encrypted shares. Finally when such encrypted shares are reassembled or decrypted to redesign the genuine image it is possible for one to have an exposed image which yet consists of confidential data. Such types of algorithms cannot persists without possessing an appropriate characteristics in the visual cryptography procedure. The ground for this is that if the rebuilding method or even the encoding method changes the data exists in the image, then the system would accordingly change the encrypted information which makes the system feasible for extracting the encrypted data from the exposed image The steganalysis is the process to expose the confidential message even certain uncertain media. There are various attacks reported on Least Significant Bytes substitution of picture elements or bit planes [8][9]. Various histogram as well as block effect has also been reported in the prior research work [10]. But certain RS steganalysis work has been reported as most concrete and appropriate technique to other conventional substitution steganography [11], which uses regular and singular groups as the elementary parameters to estimate the association of the pixels. In order to prevent RS analysis, the impact on the association of the pixels will be required to be compensated. Such types of compensation might be accomplished by adjusting other bit planes.

By doing such attempt, the implications towards security will be almost computationally impossible. For such reason, various optimization algorithms can be deployed employed in secure data hiding to identify the optimal embedding positions. The main aim of the proposed model is to design a feasible RS resistance secure algorithm which combines the use of both steganography and visual cryptography with the goals of improving security, reliability, and efficiency for secret message.

II. RELATED WORK

Ghascmi ct al.. [12] proposed a novel steganography scheme based on integer wavelet transform and Genetic algorithm. Umamaheswari [13] compress the secret message and encrypt it by the receiver's public key along with the stego key and embed both messages in a carrier using an embedding algorithm. Shyamalendu Kandar [14] proposed a technique of well known k-n secret sharing on color images using a variable length key with share division using random number. Anupam [15] describes how such an even-odd encryption based on ASCII value is applied and how encrypted message converting by using Gray code and embedding with picture can secured the message and thus makes cryptanalyst's job difficult.

III. PROPOSED SYSTEM

The proposed work is basically a framework designed in MATLAB with two modules e.g. Steganography using Genetic Algorithm and Visual Cryptography. The proposed system model of the Steganography using Genetic Algorithm and Visual Cryptography is shown in the Figure 1. An input image is accepted as cover image which is used to hide the secret message. An input image is accepted as cover image for the input message in plain text format. After embedding the secret message in LSB (least significant bit) of the cover image, the pixel values of the steg-image are modified by the genetic algorithm to keep their statistic characters. The experimental results should prove the proposed algorithm's effectiveness in resistance to steganalysis with better visual quality. The user can select their targeted information in terms of plain text for embedding the secret message in LSB of the cover image. The implications of the visual cryptography will enable the pixels value of the steg-image to keep their statistic character. LSB steganography has low computation complexity and high embedding capacity, in which a secret binary sequence is used to replace the least significant bits of the host medium. This is also one of the strong algorithms which keeps the information proof from any intruder channel.

In a pure steganography framework, the technique for embedding the message is unknown to Intruder and shared as a secret between Alice and Bob. However, it is generally considered that the algorithm in use is not secret but only the key used by the algorithm is kept as a secret between the two parties, this assumption is also known as Kerchoff's principle in the field of cryptography. The secret key, for example, can be a password used to seed a pseudo-random number generator to select pixel locations in an image cover-object for embedding the secret message (possibly encrypted).Intruder has no knowledge about the secret key that Alice and Bob share, although she is aware of the algorithm that they could be employing for embedding messages.

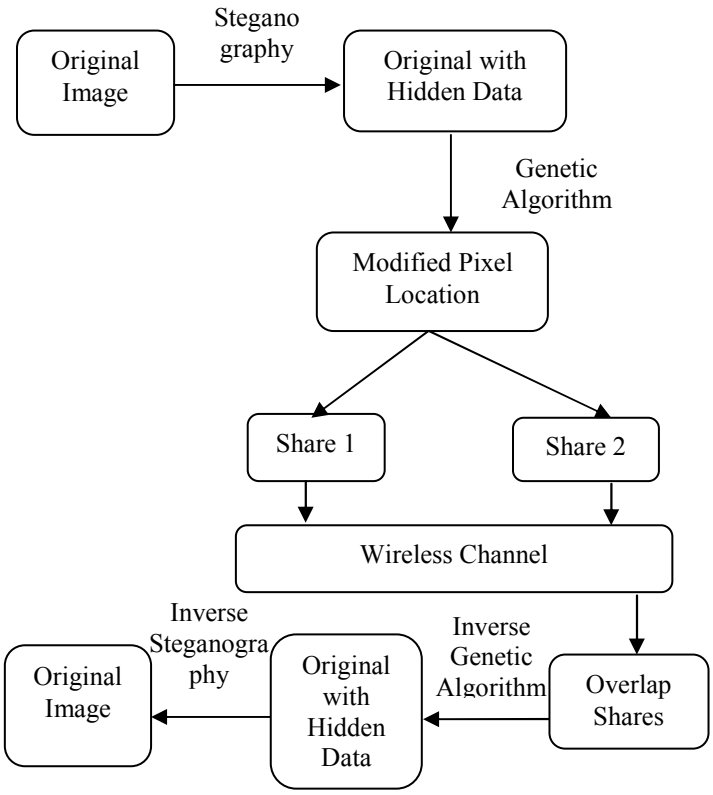

Figure 1. Proposed System Model

IV. ALGORITHM DESCRIPTION

The simplest way to hide binary data on an image is to use a lossless image format (such as a Bitmap) and replace the least significant bits of each pixel in scan lines across the image with the binary data. This is not secure as an attacker can simply repeat the process to quickly recover the hidden information. This technique, known here as "BlindHide" because of the way it blindly hides information, is also not

good at hiding – the initial portion of the image is left degraded while the rest remains untouched.

The proposed project work consist of mainly two algorithms which are (i) Steganography using Genetic Algorithm (ii) Visual Cryptography with Threshold. The application initiates with Steganography module where the cover image will be encrypted to generate Stego image. The stagographic image generated in this module will act as an input for visual cryptographic module.

Algorithm: Steganography
Input: Cover Image
Output: Stego Image

Step 1: Read the cover image.
Step 2: Find out the pixel values of cover image.
Step 3: Read the secret data character wise.
Step 4: Convert each character into its equivalent ASCII code.
Step 5: ASCII code is converted into binary values.
Step 6: Enter the secret key.
Step 7: Secret data is converted into cipher data.
Step 8: The stream of 8-bits (cipher data) are embedded into LSB of each pixel of the cover image.
Step 9: To apply Genetic Algorithm in the stego image the pixel location should be modified.

Algorithm: Visual Cryptography
Input: Stego-Image
Output: Encrypted Shares

Step 1: Read Stego-Image generated.
Step 2: The stego image is breaked into three layers namely split-1, split-2, split-3 these three files are containing the hidden data and to get the hidden data these three files have to be reconstructed perfectly.
Step 3: The re-assembled picture and the extracted data will be gained again.

The proposed scheme is based on standard visual cryptography as well as visual secret sharing. The implementation of the algorithm yields in better result with insignificant shares when stego images are normally with light contrast. It can also be seen that the algorithm gives much darker shares in gray output the proposed scheme is based on standard visual cryptography as well as visual secret sharing. The implementation of the algorithm yields in better result with insignificant shares when stego images are normally with light contrast. It can also be seen that the algorithm gives much darker shares in gray output. This algorithm gives better results in terms of image quality and stegnalysis.

V. IMPLEMENTATION AND RESULTS

The project work is designed on 64 bit Windows OS with Core i3 Processor with 4 GB RAM and 1.80GHz using Matlab Platform. The original image is in PNG format of 5.28 KB whereas 2012 OLYMPIC GAMES HELD AT LONDON as a plaintext message shown in Figure 2.

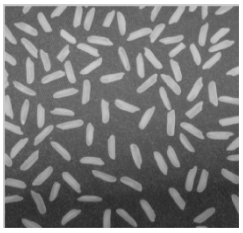

Figure 2. Original Image

The original message is embedded into the image by using LSB insertion method. The resultant image is called as stego image shown in Figure 3. Then apply genetic algorithm to modify the pixel location and detection of message is complex.

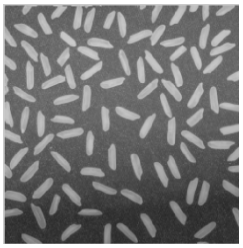

Figure 3.Stego Image

Then apply visual cryptography scheme stego image is splitted into two shares based on threshold. The shares of the stego image is shown in Figure 4.

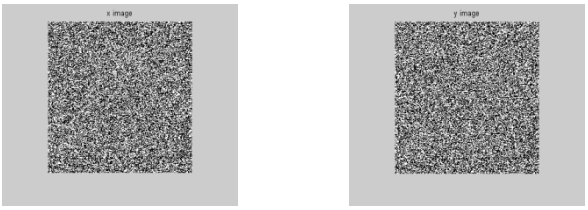

Figure 4. Shares of Stego Image.

It is almost impossible for anyone who will attempt to decrypt the encrypted data within that image to reveal if the secret shares which they posses are set of all encrypted shares or certain secret shares are missing.

VI. PERFORMANCE ANALYSIS

The performance of the proposed system is experimented by performing stegnalysis and conducting benchmarking test for analysing parameters like Mean Squared Error (MSE) and Peak Signal to Noise Ratio.

Cover image : rice.png
Size : 256*256
Mean Square Error (MSE) : 0.0678
Peak Signal-to-Noise Ratio (PSNR): 59.8188db

After applying Genetic Algorithm the measured performance is shown in below

Mean Square Error (MSE) : 0.794
Peak Signal-to-Noise Ratio (PSNR): 39.4011db

After applying genetic algorithm all the pixel location are altered. Due to the change the pixel location MSE and PSNR values are increased.

VII. CONCLUSION

The proposed system has discussed implementation of securely using steganography using genetic algorithm along with visual cryptography. It can be concluded that when normal image security using steganographic and visual cryptographic technique is applied, it makes the task of the investigators unfeasible to decrypt the encoded secret message. The security features of the steganographic are highly optimized using genetic algorithm. The proposed system is highly resilient against RS attack and optimally used for gray scale output in visual secret shares making it highly compatible for real-time applications. The future work could be towards the enhancing visual cryptography scheme for gray scale image in various platform.

REFERENCES

[1] Fridrich, J., Goljan, M. and Du,R, Reliable Detection of LSB Steganography in Colour and Grayscale Images, Proceedings of ACM Workshop on Multimedia and Security, Ottawa, October 5, 2001, pp.27-30.

[2] Sathiamoorthy Manoharan, an empirical analysis of rs steganalysis, proceedings of the third international conference on internet monitoring and protection, IEEE computer society Washington, 2008.

[3] Rita Rana, Dheerendra Singh, Steganography-Concealing Messages in Images Using LSB Replacement Technique with Pre-Determined Random Pixel and Segmentation of Image, International Journal of Computer Science & Communication Vol. 1, No. 2, July-December 2010, pp. 113-116.

[4] Singh, K.M.; Nandi, S.; Birendra Singh, S.; ShyamSundar Singh, L.; , Stealth steganography in visual cryptography for half tone images, Computer and Communication Engineering, International Conference, 2008.

[5] Jithesh K , Dr. A V Senthil Kumar , Multi Layer Information Hiding - A Blend Of Steganography And Visual Cryptography, Journal of Theoritical and Applied Information Technology, 2010.

[6] Hsien-Chu Wu; Chwei-Shyong Tsai; Shu-Chuan Huang;, Colored digital watermarking technology based on visual cryptography, Nonlinear Signal and Image Processing, IEEE-Eurasip, 2005.

[7] R. Chandramouli, Nasir Menon, Analysis of LSB Based Image Steganography techniques, IEEE-2001.

[8] Arezoo Yadollahpour, Hossein Miar Naimi, Attack on LSB Steganography in Colour and Grayscale Images Using Autocorrelation Coefficients, European Journal of Scientific Research ISSN 1450- 216X Vol.31 No.2 (2009).

[9] Qing zhong Liu, Andrew H. Sung, Jianyun X, Bernardete M. Ribeiro,." Image Complexity and Feature Extraction for Steganalysis of LSB Matching", The 18th International Conference on Pattern Recognition (ICPR'06) 0-7695-2521-0/06 $20.00 © 2006 IEEE.

[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, 2002.

[11] J. Fridrich, M. Goljan, and R. Du. Detecting lsb steganography in color, and gray-scale images. IEEE MultiMedia, pages 22–28, 2001.

[12] Ghascmi E shanbchzadch J and ZahirAzami B, " A Steganography method based on Integer Wavelet Transform and Genetic Algorithm International Conference on Communications and Signal Processing (ICCSP) pp 42 45,2011.

[13] Dr.M.Umamaheswari Prof. S.Sivasubramanian S.Pandiarajan, Analysis of Different Steganographic Algorithms for Secured Data Hiding, IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.8, August 2010.

[14] Shyamalendu Kandar, Arnab Maiti, Variable Length Key based Visual Cryptography Scheme for Color Image using Random Number, International Journal of Computer Applications . Volume 19– No.4, April 2011.

[15] Anupam Kumar Bairagi, ASCII based Even-Odd Cryptography with Gray code and Image Steganography: A dimension in Data Security, ISSN 2078-5828 (Print), ISSN 2218-5224 (Online), Volume 01, Issue 02, Manuscript Code: 110112.

[16] G. Simmons, "The prisoners problem and the subliminal channel" *CRYPTO*,pp. 51-67, 1983.

[17] Katzenbeisser, S. and Petitcolas F.A.P. *Information hiding* techniques for steganography and digital watermarking. Artech House, Norwood, MA 02062, USA, 1999.

[18] Aderemi Oluyinki, Some improved genetic algorithms based on Heuristics for Global Optimization with innovative Applications, Doctorial thesis, 2010.

[19] Talal Mousa Alkharobi, Aleem Khalid Alvi, New Algorithm for Halftone Image Visual Cryptography, IEEE 2004.

[20] Chin-Chen Chang; Iuon-Chang Lin; , A new (t, n) threshold image hiding scheme for sharing a secret color image, Communication Technology Proceedings, ICCT 2003.