Volume 4, Issue 6, June 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Image Steganography Using Genetic Algorithm and Visual Cryptography for Secure Data Hiding and Transmission over Networks

Rehana Begum R.D
Department of Computer Science and Engineering
Channabasaveshwara Institute of Technology
Gubbi, Karnataka, India.

Sharayu Pradeep
Department of Computer Science and Engineering
Channabasaveshwara Institute of Technology
Gubbi, Karnataka, India.

Abstract— A large number of commercial steganographic programs use the Least Significant Bit(LSB) embedding as the method of choice for hiding data as it has low computation complexity and high embedding capacity but certain 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. Although there has been an extensive research work in the past, but majority of the work has no much optimal consideration for robust security towards the encrypted image. The proposed system provides the best approach for secure data hiding and transmission over Networks using LSB based steganography with Genetic Algorithm (GA) and Visual Cryptography (VC). The system here encodes the secret message in least significant bits of the cover image so termed as stego image by using a secret key. Genetic Algorithm and Visual Cryptography has been used for enhancing the security. Genetic Algorithm is used to modify the pixel location of stego image which is another protection lock for the secret message and image and the detection of this is complex. Visual Cryptography is further used to encrypt the modified pixel image by breaking it into two shares based on a specific threshold, later those encrypted shares and the secret key is separately sent to others using Network Socket Programming. User who received the secret shares has to do the reverse process to retrieve the Image and the secret message by using the secret key. The implementation is done in java platform which shows that the proposed system is highly secure and reliable.

Keywords— Steganography, Visual Cryptography, Genetic Algorithm, Steganalysis, Stego image.

I. INTRODUCTION

Steganography is the art of secret communication. Its purpose is to hide the very presence of communication as opposed to cryptography whose goal is to make communication unintelligible to those who do not possess the right keys [1]. Digital images, videos, sound files, and other computer files that contain Perceptually irrelevant or redundant information can be used as "covers" or carriers to hide secret messages. After embedding a secret message into the cover image a so – called stego-image is obtained. It is important that the Stego-image does not contain any detectable artifacts due to message embedding. A third party could use such artifacts as an indication that a secret message is present. Once message detection can be reliably achieved, the steganographic tool becomes useless. The best embedding methods of Steganography to hide a message is Least Significant Bit embedding : It is a Substitution method of Steganography where the right most bit in a binary notation is replaced with a bit from the embedded message. 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 [2]. The process of RS steganalysis uses the regular and singular groups as the considerations in order to estimate the correlation of pixels [3]. The presence of robust correlation has been witness in the adjacent pixels. But unfortunately using traditional LSB replacing steganography [4], 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 [5] [6], 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. 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.

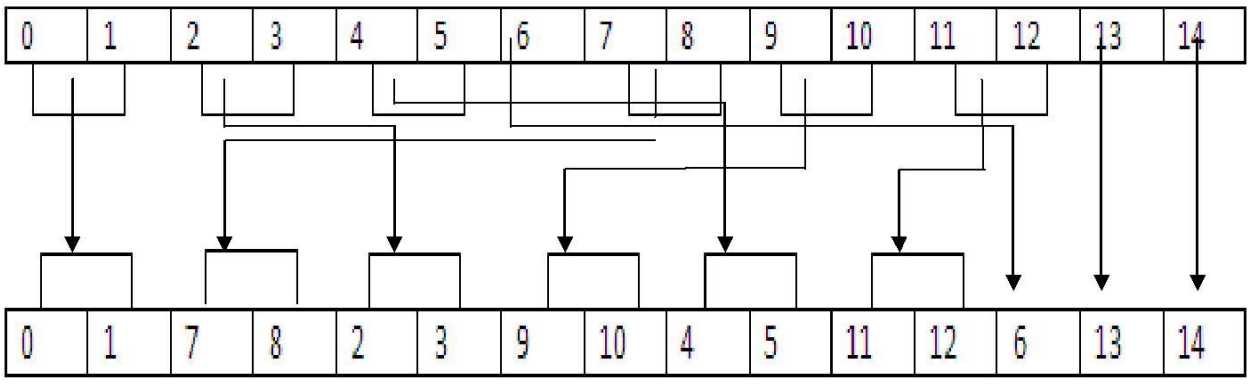
For such reason, various optimization algorithms can be deployed in secure data hiding to identify the optimal embedding positions. The most popular technique in evolutionary computational research has been the genetic algorithm which is the best optimal consideration for robust security towards the encrypted image. In the traditional genetic algorithm, the representation used is a fixed-length bit string. Each position in the string is assumed to represent a particular feature of an individual, and the value stored in that position represents how that feature is expressed in the solution. Usually, the string is "evaluated as a collection of structural features of a solution that have little or no interactions". The analogy may be drawn directly to genes in biological organisms. Each gene represents an entity that is structurally independent of other genes. The main reproduction operator used is bit-string crossover, in which two strings are used as parents and new individuals are formed by swapping a sub-sequence between the two strings.The main aim of the proposed model is to design an algorithm which combines the use of both steganography and visual cryptography with row column shuffling genetic algorithm with the goals of improving security, reliability, and efficiency for secret message.

II. RELATED WORK

Fridrich.J, Goljan.M and Du, R, Proposed Reliable Detection of LSB Steganography in Color and Grayscale Images described the method of choice for message hiding in 24-bit, 8-bit color and grayscale images. Shyamalendu Kandar proposed a technique of well known k-n secret sharing on color images using a variable length key with share division using random numbers. Ravindra Gupta, Akanksha Jain, Gajendra Singh presented the paper as Combine use of Steganography and Visual Cryptography for Secured Data hiding in Computer Forensics(2012) designed a feasible RS-resistance secure algorithm which combines the use of both Steganography and Visual Cryptography. Ghascmi ct al.. proposed a novel steganography scheme based on integer wavelet transform and Genetic algorithm.Talal Mousa Alkharobi, Aleem Khalid Alvi[4], proposed a New Algorithm for Halftone Image Visual Cryptography, for(2,2) VC and (3,3) visual secret sharing. Aderemi Oluyinki proposed Some improved genetic algorithms based on Heuristics for Global Optimization with innovative Applications, Doctorial thesis, 2010.

III. PROPOSED SYSTEM

The proposed system is basically a framework designed in Java swing with the Encryption and Decryption process of Steganography, Genetic Algorithm and Visual Cryptography. The overall encryption process is as shown in Figure. 1. An input image is accepted as cover image which is used to hide the secret message in plain text format and a Data hide key to make it secure. Using Key-Based Pixel Selection Algorithm the data is stored in the input image using LSB technique. LSB steganography has low computational complexity and high embedding capacity, in which a secret binary sequence is used to replace the least significant bits of the host medium. After embedding the secret message in LSB of the cover image, the pixel values of the stego-image are modified by the genetic algorithm to keep their statistic characters. This module is used to change the pixel positions of the stego image, which is another protection lock for the secret message and image. Using Genetic Algorithm's cross-over concept the column pixel shuffling happen first and then the row pixel shuffling as shown below.



Column pixel Shuffling for 2 columns

In this project we are using Color Image Visual cryptography. The output of Genetic Algorithm's Modified pixel Image is given as a input for Visual Cryptography module and which uses Color Image Visual Cryptography algorithm to divide the input image into two secret shares, Further shares and the key are separately sent to others using Network Socket Programming which is used for file and message transfer. User who received the secret shares has to do the reverse process means Decryption to retrieve the Image and secret message by using the data hide key sent by the sender through the interface as shown in Figure. 2.

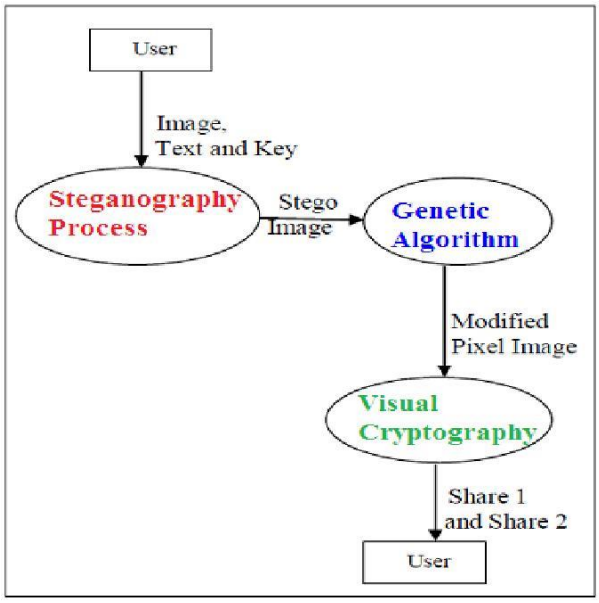


Figure. 1 Encryption Process

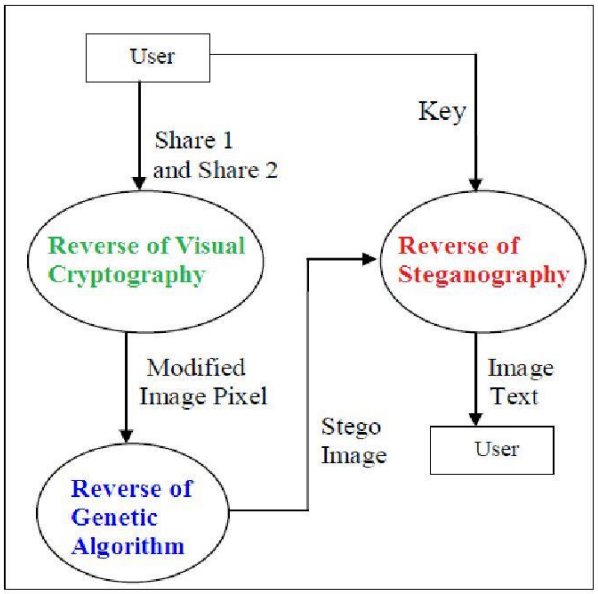


Figure. 2 Decryption Process

IV. ALGORITHM DESCRIPTION

The proposed project work consist of mainly three algorithms namely (i) Steganography (ii) Genetic Algorithm and (iii) Visual Cryptography. 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 after underwent to both row and column shuffling used by genetic algorithm.Genetic Algorithm is used to modify the pixel location of stego image which is another protection lock for the secret message and image. Using Genetic Algorithm's cross-over concept the column pixel shuffling happen first and the row pixel shuffling happens next and the detection of this message is complex.After shuffling process it is sent for further process which is known as visual cryptography to make it more secure.Visual cryptography is a method for protecting image-based secrets that has a computation-free decryption process [9]. In the (2, 2) VC scheme each secret image is divided into two shares such that no information can be reconstructed from any single share. These are all the strong algorithms which keeps the information proof away from any intruder.

STEGANOGRAPHY PROCESS

For Image Encryption this system uses two techniques one is XOR Operation and another one is Bit Rotation Operation.

For this operation system need to input

1. Image
2. Image Encryption Key
3. Secret Message

And the output will be Stego Image.

For Example if our Input Key is INDIA then from the input key, this system will generate an 8-bit Key Value (KV) by following method.

Bit(ASCII(I)) XOR Bit(ASCII(N)) XOR Bit(ASCII(D)) XOR Bit(ASCII(I)) XOR Bit(ASCII(A))

In Image the color channel R is going to hold the hidden data for that also we are changing only last 4 LSB. Since we are changing the last 4 LSB for only one color channel, there will not be any damage to the real image.

Example: if we are planning to hide a text A

Get the Encrypted value to hide by KV i.e. A (xor) KV

Let the output Binary value is 0101 1000 Split Binary part into A and B like that A = 0101 and B = 1000

Let R value in 1, 1 is 120 (R1) and R Value in 1, 2 is 91(R2) R1 = Binary (120) = 0111 1000
R2 = Binary (91) = 0101 1011

Replace last 4 bit in R1 by A and Replace last 4 bit in R2 by B After Conversion R1 = 0111 0101 and R2 = 0101 1000

Data Encryption Process:

Let A is a text to be hide, A ASCII Value is 65, Binary is 0100 0001 Let KV value is 1100 1100

Then A (XOR) KV = data to be hided Example.
A => 0100 0001

KV=> 1100 1100

➔

XOR output 1000 1101

Data Decryption Process:

Output ➔ 1000 1101

KV ➔ 1100 1100

➔

XOR output 0100 0001

GENETIC ALGORITHM:

Column Shuffling:

Step 1: Get width and height of Image
Let w=Width of image, h=Height of image, i=0, j=0;
Step2: mod=w mod 2, Rem=w-mod, x=0, s=Rem/2, v=0;
Step3: for j<h **then**
for i<w **then**
If i< Rem then
If v<8
Get the RGB pixel of x, j and write in to i and j position of an image x++;
Else
Get the RGB pixel of s,j and write in to i and j position of an image s++;
End if; v++;
If v==16
v=0; End if;
Else
Get the RGB pixel of i, j and write in to i and j position of an image End if; i++;
End for: j++;

Row Shuffling:

Step 1: Get width and height of Image
Let w=Width of image, h=Height of image, i=0, j=0;
Step2: mod=h mod 2, Rem=h-mod, x=0, s=Rem/2,v=0;
Step3: for i<w **then**
For j<h **then**
If j< Rem then
If v<8
Get the RGB pixel of i,x and write in to i and j position of an image x++;
Else
Get the RGB pixel of i,s and write in to i and j position of an image s++;
End if; v++;
If v==16
v=0; End if;
Else
Get the RGB pixel of i, j and write in to i and j position of an image
End if; j++;
End for: i++;

ALGORITHM FOR VISUAL CRYPTOGRAPHY

Step 1: Read Input Color Image I, Read Number of Share N
Step 2: Let W = Width of the Image
Let H = Height of the Image
Step 3: Create a Numeric Matrix R of Size [W, H]
Step 4: Fill the matrix with Random Number
For s = 1 to W
For q = 1 to H
R[s,q] = Generate Random number between 1 to N
Next q
Next s
Step 5: Let c = 1

Step 6: Create a new Share Image SI
Step 7: For s = 1 to w
For q = 1 to H
V = R[s,q]
If V = C then SI[s,q] = I[s,q] Next q
Next s
Step 8: Write all the content of SI in new Share
Step 9: if c < N then c = c+1, Go To Step 6
Step 10: Stop

The Implementation of the algorithm yields better result as compared to other approaches as it is simple and ease of use.

V. IMPLEMENTATION AND RESULTS

The project work is designed on 64 bit Windows OS with Core i3 Processor, 4 GB RAM and 1.80GHz using Java Platform. The original image is in PNG format of 5.28 KB whereas SECRET MESSAGE is in a plaintext Format as shown in Figure. 3.

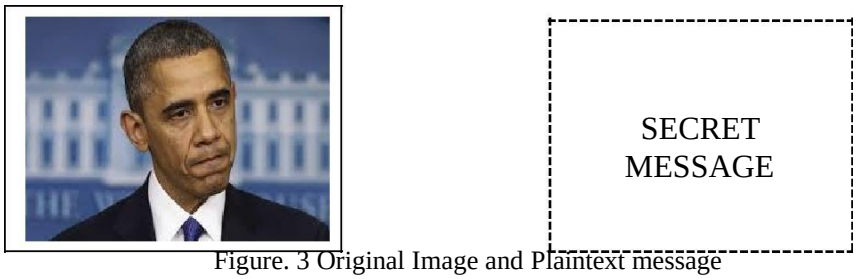


Figure. 3 Original Image and Plaintext message

The Original message is embedded into the image by using LSB insertion method. The resultant image is called as stego image. Genetic Algorithm is used to modify the pixel location of stego image which is another protection lock for the secret message and image. Using Genetic Algorithm's cross-over concept the column pixel shuffling happen first and the row pixel shuffling happens next and the detection of this message is complex as shown in Figure.4.

Figure. 4 Column and row pixel shuffling

Then after applying visual cryptography scheme, the stego image is spitted into two shares based on threshold. The shares of the stego image are shown in Figure.5.

Figure. 5 Shares of Stego Image.

User who received the secret shares has to do the reverse process and the data hide key to retrieve the Image and secret message.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. Hence we can prove that it is highly secure.

VI. CONCLUSION

In this paper we have discussed the implementation of hiding data in an image with a secret key using steganography and 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 steganography are highly optimized using genetic algorithm. The proposed system is highly resilient against RS attack and optimally used for color image output in visual secret

 shares making it highly compatible for real-time applications. Our scheme has shown less pixel expansion which is desirable and good for the retrieval of the secret image by improving security and reliability. It gives efficiency for secret message and the usability of key makes the system simple and yet confident. Further we can extend this work to use this technique with 3D images for creating the shares that have partial secret and reveal that secret by stacking to each other.

REFERENCES

[1] 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.

[2] Ravindra Gupta, Akanksha Jain, Gajendra Singh, "*Combine use of Steganography and Visual Cryptography for Secured Data hiding in Computer Forensics*" , International Journal of Computer Science and Information Technologies, Vol. 3 (3) , 2012,4366 – 4370.

[3] Fridrich, J., Goljan, M. and Du,R, *Reliable Detection of LSB Steganography in Colour and Grayscale Images*, Proceedings of ACM Workshop volume 02, Manuscript Code: 11011on Multimedia and Security, Ottawa, October 5, 2001, pp.27-30.

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

[5] R.J. Anderson and Petitcolas, F.A.P., "*On the limits of steg-anography*", IEEE Journal of Selected Areas in Communica-tions, Special Issue on Copyright and Privacy Protection **16** No.4 (1998) 474−481. Cryptography, Journal of Theoritical and Applied Information Technology, 2010.

[6] Mrs.G.Prema and S.Natarajan, "*Steganography using Genetic Algorithm along with Visual Cryptography for Wireless Network Application", IEEE 2012.*

[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] 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.

[11] 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.

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

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

[14] 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.

[15] 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.

[16] 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.P. Kumswat, Ki. Attakitmongcol and A. Striaew, "A New Approach for Optimization in Image Watermarking by Using Genetic Algorithms", *IEEE Transactions on Signal Processing*, Vol. 53, No. 12, pp. 4707-4719, December, 2005.

