ISSN:0975-9646

Combine use of Steganography and Visual Cryptography for Secured Data hiding in Computer Forensics

Ravindra Gupta, Akanksha Jain, Gajendra Singh

Sri Satya Sai Institute of Science & Tech.
Sehore, Madhya Pradesh, India

***Abstract*—The proposed system highlights a novel approach for creating a secure steganographic method and visual cryptography for data hiding in computer forensics. Although there has been an extensive research work in the past, but majority of the research work has no much optimal consideration for robust security towards the encrypted image. The proposed method encodes the secret message in least significant bits of the original image, where the pixels values of the encrypted image are modified by the genetic algorithm to retain their statistic characters, thereby making the detection of secret of message difficult. Use of Genetic algorithm has compelled the system for enhancing the security. The proposed system hides data in a real image and achieve its detection after under went to visual cryptography. 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 for improving security, reliability and efficiency for secret message. The implementation is done in java platform which shows that the proposed system has better resilienc by considering the steganalysis.**

Keywords-Steganography, Visual Cryptograhy, Genetic Algorithm, RS Analysis

1.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 renders 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 re-assembled 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 charecteristics 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.

The remaining section of the paper is designed as follows. Section-II discusses about related work which is followed by proposed system in Section-III. Section IV discusses about Algorithm description, Section V discusses about implementation and results, followed by description of performance analysis in section VI. Section VII discusses about conclusion summarizing the entire proposed work.

2. RELATED WORK

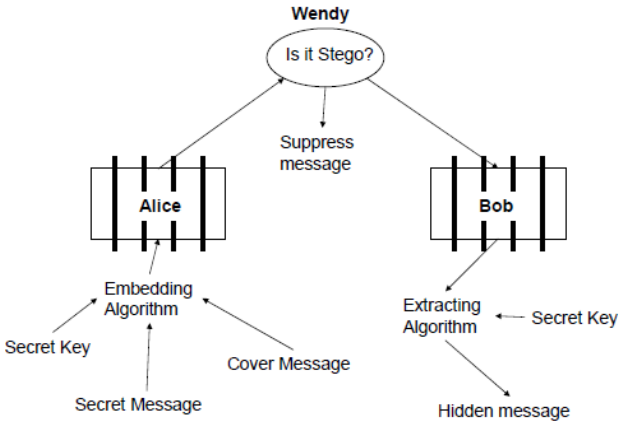
Ghascmi ct al.. [12] proposed a novel steganography scheme based on integer wavelet transform and Genetic algorithm..

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.

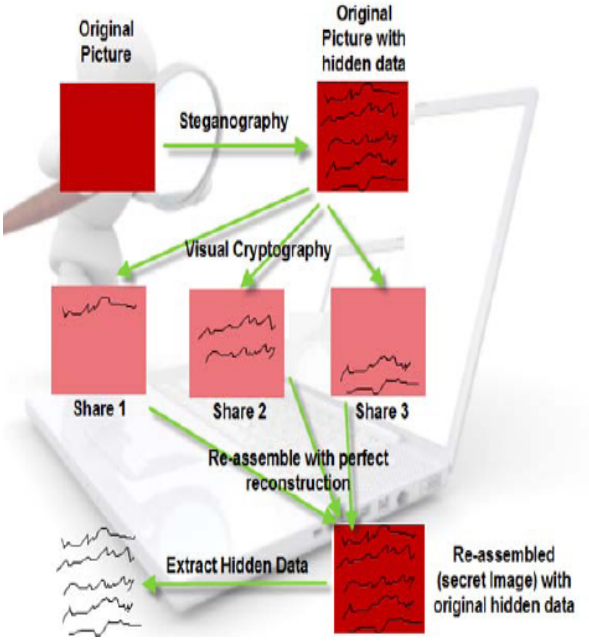
3. PROPOSED SYSTEM

The proposed work is basically a framework designed in java swing with two modules e.g. Steganography using Genetic Algorithm and Visual Cryptography. 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 visual cryptography 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.

In a *pure steganography* framework, the technique for embedding the message is unknown to Wendy and shared as a secret between Alice and Bob.



However, it isgenerally 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)[16]. Wendy 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.



4. 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 *x* 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 *blind*ly *hide*s information, is also not good at hiding – the initial portion of the image is left degraded while the rest remains untouched.

A tool known as "Hide and Seek for Windows 95" [17] attempts to get around the security issues in BlindHide by randomly distributing the hidden information across the image. A more modern version of this algorithm, dubbed "HideSeek", is used here. HideSeek uses a random seed (provided by hashing a password) to pick the order in which it will write to the pixels. HideSeek is much more secure than BlindHide, but does not necessarily leave the image in a better condition. The noise introduced by HideSeek is randomly placed and often causes the resulting stego-image to look speckled. The noise left behind by both HideSeek and BlindHide is much more noticeable to the naked eye in large blocks of colour – where a single modified pixel stands out amongst its uniform neighbours. This is expressed explicitly by the Laplace formula [18]. The Laplace formula simply measures the difference between a pixel and its four touching

neighbours. The magnitude of the formula increases with the colour variation and this can be used to detect steganography by counting the number of pixels at a given magnitude. Untouched images are more likely to contain a large number of pixels with zero magnitudes since there is no reason for small random variations to occur in large blocks of colour. Stego images often contain small variations, and can be detected easily.

The proposed project work consist of mainly two algorithms which are (i) Steganography using Genetic Algorithm and (ii) Visual Cryptography with pseudorandom number. 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

```
Read input image (Cover image)
Read the plain text message
Authentication using password
Switch (encode_alg)
    Case-1: Implement BattleSteg;
            break;
    Case-2: Implement BlindHide;
            break;
    Case-3: Implement FilterFirst;
            break;
    Case-4: Implement HideSeek
            break;
Convert image to double precision
Embed the message in the cover image based on percentage
Generate random message
Apply uniformly distributed Pseudorandom integers
    msg = randi([0 round(255*perc/100)],size(I));
//perc= Embedd the message in the cover image based on percentage
I = I+msg;
Divide image into 8 x 8 blocks
Apply the non-positive flipping F-
Generate random 0 and 1s
        Change LSB as per flipping
Apply non-negative flipping F+
Generate random -1 and 0 s
Change LSB as per flipping
Calculate_correlation
Initialize maximum chromosome
Flip second lowest bit randomly for number of time
PSNR = snr(Chrom-Cn)
//Cn=Correlation for non-negative flipping
fitness = alpha*(e1+e2)+PSNR
If fitness>maxfitness //maxfitness=0 is initialized
maxfitness = fitness;
Chrommax = Cp;
//Cp= Correlation for non-positive flipping
crossover = crossover+1;//crossover=0 is initialized
end
replace chromosome with new one
```

Algorithm: Embedding process

1. *for i* = 1....,*l(c) do*
2. $s_i \leftarrow c_i$
3. *end for*
4. *generate random sequence* k_i *using seed k*
5. $n \leftarrow k_1$
6. *for i* = 1....,*l(m) do*
7. $s_n \leftarrow c_n \leftrightarrow m_i$
8. $n \leftarrow n + k_i$
9. *end for*

Algorithm: Extraction process

1. *generate random sequence* k_i *using seed ki*
2. $n \leftarrow k_1$
3. *for i* = 1.....*l(m) do*
4. $m_i \leftarrow LSB(c_n)$
5. $n \leftarrow n + k_i$
6. *end for*

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

1. *Read Stego-Image generated*
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 then*
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 applied technique uses allocation of pseudorandom number as well as exchange of pixels. One of the contrast part of this implementation is that while decrypting, the stego-image will be morphologically same compared to the cover image with respect to the shape and size thereby preventing pixel expansion effect [19]. 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 both gray as well as colored output.

5. IMPLEMENTATION AND RESULTS

The project work is designed on 32 bit Windows OS with Dual Core Processor with 2 GB RAM and 1.80GHz using Java Platform. The original image is in JPEG format of 5.28 KB whereas the plaintext message is of size 569 bytes as shown in Fig 1.

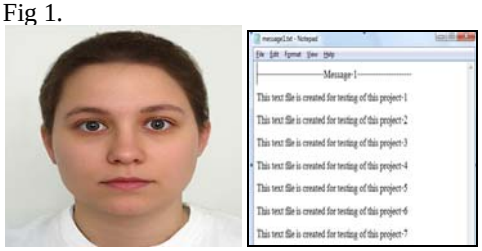


Fig 1. Cover Image (L) and Plain Text Message (R)

The encryption process is carried out using genetic algorithm deploying use of BattleSteg, BlindHide, Filter First, and Hide Seek algorithm. The encryption can also assist to give the output of a stego image of PNG format of 85.4 KB as shown in Fig 2 and for preventing RS analysis, it can also show the image in complete black pixels for blind steganalysis, where the embedded image is also in same PNG format.

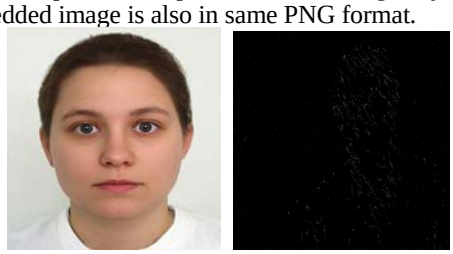
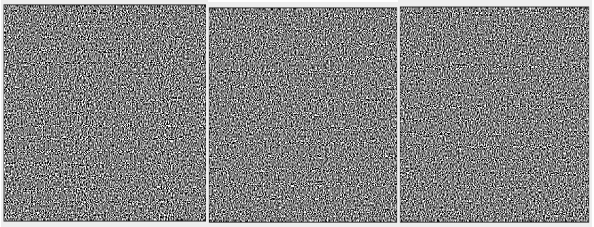


Fig 2. Stego Image (L) and Result of Blind Steganalysis(R)

The proposed method encrypts secret message which is very minimal per block of image. The process only encrypts 1bytes in an 8x8 blocks while other conventional techniques uses 1 bit in each pixels. Therefore this methodology can be used for encrypting secret message per block of image which significantly enhances the performance and retains a best quality of image during encryption. The important factor regarding the proposed system is that it does not depend on the data encryption in the LSB of the pixel values. The technique always attempt to evaluate the optimal confidential image elements where the layer of the cover image picture elements value is equivalent in the elevated layers of the image thereby retaining the superiority of the image which makes it completely resistant against RS attack.

The stego-image generated from the steganographic module will be then subjected to our visual cryptography module which generates 3 secret shares as shown in Fig 3. The proposed visual cryptographic module will be extended to work both for grayscale as well as colored image in the overlay image using threshold image hiding scheme [20]



(a) 1st ES (b) 2nd ES (c) 3rd ES

Fig 3 Encrypted Shares

The encrypted shares generated in grayscale are as follows

Fig 4 Grey scale Encrypted Share

The merit of the proposed technique is that a client can chose the location of the secret image in order to allocate to a confidential intensity and thereby the system incurs a supple and cooperative to the client's selection. Although, this methodology might not be visualized a optimal secure compared to other methods as certain levels of the confidentiality can yet be exposed even if the user do not have possession of all the secret shares, but 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.

6. PERFORMANCE ANALYSIS

The performance of the proposed system is experimented by performing steganalysis and observing the chances of RS analysis. The performance is defined by 3 factors-(i) Understanding RS analysis parameters for both overlapping and non-overlapping groups of pixels, (ii) Laplace Graph with frequency variation corresponding to Laplace value. and (iii) conducting benchmarking test for analyzing parameters like Average Absolute Difference, Mean Squared Error, Laplace Normalization, Laplacian Mean Squared Error, Signal to Noise Ratio, Peak Signal to Noise Ratio, Normalized Cross-Correlation, and Correlation Quality.

Table 1. RESULTS OF STEGANALYSIS

RS ANALYSIS
RS Analysis (Non-overlapping groups)
Percentage in red: 1.99381
Approximate length (in bytes) from red: 375.67826
Percentage in green: 4.79634
Approximate length (in bytes) from green: 903.73869
Percentage in blue: 8.84555
Approximate length (in bytes) from blue: 1666.70112
RS Analysis (Overlapping groups)
Percentage in red: 2.88103
Approximate length (in bytes) from red: 542.85095
Percentage in green: 6.53665
Approximate length (in bytes) from green: 1231.65193
Percentage in blue: 10.47579
Approximate length (in bytes) from blue: 1973.87514
Average across all groups / colors: 5.92153
Average approximate length across all groups/colors: 1115.74935

The above discussed tables show the connection with image security along with image quality. As the visual quality of the resultant images in steganography is of superior quality, there is no requirement of using any external adjustment.

7. CONCLUSION

The proposed system has discussed implementation of securely using steganographic technique using genetic algorithm and visual cryptography using pseudorandom

number. 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 is highly optimized using genetic algorithm. The proposed system is highly resilient against RS attack and optimally used for both grayscale and colored output in visual secret shares making it highly compatible for real-time applications. The future work could be towards the enhancing the algorithm using neural network for the visual cryptography, so that the system can generate highly undetectable secret shares using certain set of training data which might be automatically generated and is disposed after the task has been performed. Such type of approach might render the most secure steganographic and visual cryptographic scheme.

REFERECE

[1] Fridrich, J., Goljan, M. and Du,R, Reliable Detection of LSB Steganography in Color 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 & CommunicationVol. 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 Color 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 Steganographyc 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 (0975 – 8887) 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] Maroney, C. Hide and Seek 5 for Windows 95, computer software and documentation, originally released in Finland and the UK, n.d. Downloadable from: http://www.rugeley.demon.co.uk/security/hdsk50.zip

[18] 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.