

THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

LSB Based Steganography Using Genetic Algorithm and Visual Cryptography for Secured Data Hiding and Transmission over Networks

Shruti Sekra

M. Tech. Department of Computer Engineering,
G. H. Rasoni Institute of Engineering and Technology, Pune, Maharashtra, India

Nikhil Korane

Pursing BE, G. H. Rasoni Institute of Engineering and Technology, Wagholi, Pune, Maharashtra, India

Swapnil Shitole

Pursing BE, G. H. Rasoni Institute of Engineering and Technology, Wagholi, Pune, Maharashtra, India

Abstract:

Steganography is a latest evolution of cryptography, wild variety of applications used cryptography as a part of hiding data with the help of encryption algorithm along with genetic algorithm, thus our paper is based on steganography using genetic algorithm along with visual cryptography for network. Using the Least significant bit (LSB) of the actual image, the choice of hiding data, as it has low computation complexity and high embedding capacity helps pixel values to be analyzed. Although there has been extensive researches in past but, there has been no such security for encrypted image thus in our system a security key has been provided for that particular encrypted image for hiding data to get a stego image, which actually holds the message. Genetic algorithm is used for modifying the pixel location of stego image to enhance the multilevel security and the detection of this becomes complex. Visual cryptography is used to make the shares of that modified pixel image and send it to the end user. The secret key is sent to the receiver. User who received the secret shares has to do reverse process to retrieve the image using the secret key.

Keywords: *Steganography, visual cryptography, genetic algorithm, stego image*

1. Introduction

Steganography is hiding information by embedding secret data into an innocuous medium. So we can say that it is art of communication. Its purpose is to hide the flow of communication, which is just opposite to the cryptography.

Digital images, videos, sound files, and other computer files which contain irrelevant information which can be use as cover to hide the secret message when a secret message is embedded in an image, a stego image is generated. It's important that image doesn't contain any detectable artifacts i.e third party should not be able to detect that hidden messages.

Once the message is detected then the steganographic tool becomes useless. The best method for hiding the data is that, the data is hided in the LSB of the image which can be done in steganography.

Fundamentally, there is an image which contains some encrypted data in it, is split into some shares and finally these shares are reassembled or decrypted at receivers end

The best embedding method of steganography is the hiding of data in LSB of the image. Actually it is the substitution of the steganography, where the right most bit of binary notation is replaced according to the embedded message.

The RS analysis is the best method of steganalysis algorithm to detect the hidden message after analyzing the pixel values.

Steganography and visual cryptography both topics are important for the image security. Although researches had done for these two approaches, but the results are not that much satisfactory as in RS analysis.

Some methods of image security use watermarking system, which embeds image inside another image and then uses it as the secret image.

The method of using steganography with virtual cryptography includes lots of challenges in identifying such hidden messages.

Fundamentally, the secret data is incrypted in the image and it is splits into shares. Finally these shares are reassembled or decrypted to get the real image and the confidential data seperatly.

The basic for this is that if the encoding part gets changed, the data still exist 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.

Following researches, the most popular method is assured as the "genetic algorithm" for robust security towards the encrypted image. In traditional genetic algorithm, the representation used is a fixed-length bit string.

2. Related Work

Ghascmict al.. [8] proposed a novel steganography scheme based on integer wavelet transform and Genetic algorithm.

Ravindra Gupta et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (3) , 2012,4366 - 4370

Umamaheswari [9] 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 [10] 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 [11] 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 system is basically consist of two module i.e. Steganography using genetic algorithm and visual cryptography. The system is embedded with the framework JAVA swing.

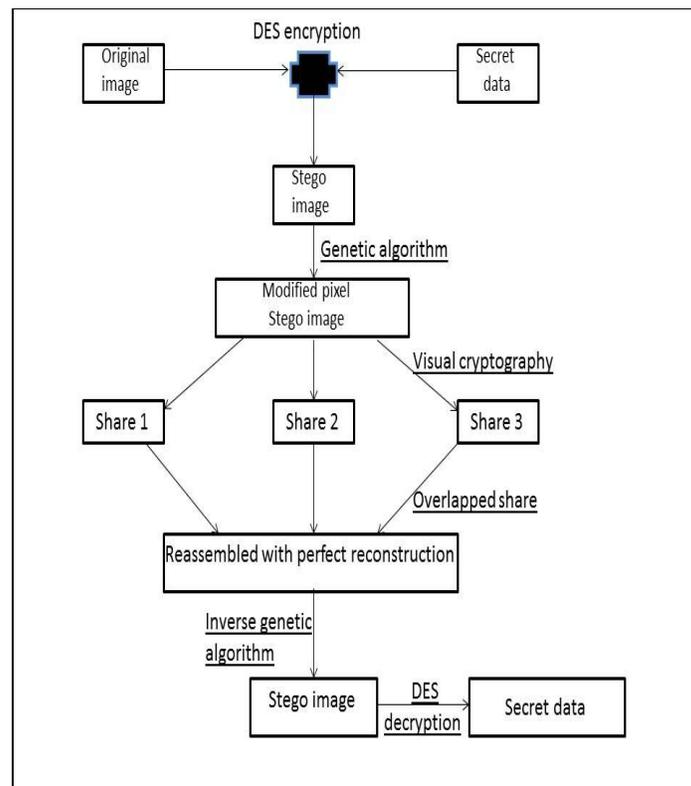


Figure 1

LSB steganography has high embedding capacity and has low computation complexity, in which a secret binary sequence is used to replace the least significant bits of the original medium.

First the secret data is encrypted in LSB of original image using DES encryption so as to get a stego image. Pixels location gets modified using Genetic algorithm then we will get modified pixel stego image.

further using visual cryptography stego image is splits into various shares and the secret key is embedded in each of the shares. And these shares are transmitted over wireless network.

Finally at receivers side shares are reassembled and reconstructed so that he will get the modified pixel stego image. And the inverse genetic algorithm will be applied on that modified pixel stego image ,to get the original stego image.

This algorithm also provides security from external entity and keeps the confidential data secure.

And finally the secret data gets separated from that stego image using DES decryption and will get confidential data.

4. Algorithm Description

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 stego 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
 1. Read Stego-Image generated
 2. The stego image is brokeed 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. 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.
- Set Theory Analysis
 1. Let S 'be the Document Analysis and Recognitions Using steganography.
 $S = \{ \dots \dots \dots \}$ Set S is divided into 6 modules
 $S = \{S1, S2, S3, S4, S5\}$
 $S1 = \text{admin}$
 $S2 = \text{user}$
 $S3 = \text{Keyword search module (KSM)}$
 $S4 = \text{View ranking of file (VRF)}$
 $S5 = \text{View file length and execution time}$
 2. Identify the inputs.
 $\text{Inputs} = \{X1, X2, X3, \dots \dots \dots Xn\}$
 $X1 = \text{Enter the file name or keywords to search}$
 $X2 = \text{Enter the image to search}$
 3. Identify the output as O .
 $\text{Outputs} = \{Y1, Y2, Y3, \dots \dots \dots Yn\}$
 $Y1 = \text{file}$ $Y2 = \text{image}$

5. Conclusion

In this paper we have studied the implementation of hiding the data in the image with the help of secret key using steganography and genetic algorithm along with visual cryptography.

It has concluded that the image which contains the hidden data is fully secure using steganography and visual cryptography ,and it also it makes difficult for external investigators to decrypt or read that hidden data.

The security features of steganography are more optimized since it uses the genetic algorithm .It can be used for color image output making it highly compatible for real-time applications.

Our scheme has shown less variation in the pixel of images which is desirable and good for the secret image, which improves more security and reliability.

It makes the system more efficient and simple by means of usability of keys. Further this method can applied to the 3D images as well with some secret key in it.

6. 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: 11011 on 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. Mrs. G. Prema and S. Natarajan, “Steganography using Genetic Algorithm along with Visual Cryptography for Wireless Network Application”, IEEE 2012.
6. R. Chandramouli, Nasir Menon, Analysis of LSB Based Image Steganography techniques, IEEE-2001.
7. 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).
8. Ghascmi E shanbchzadch J and Zahir Azami B, “ A Steganographic method based on Integer Wavelet Transform and Genetic Algorithm International Conference on Communications and Signal Processing (ICCSP) pp 42 45, 2011.
9. 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
10. 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
11. 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
12. Talal Mousa Alkharobi, Aleem Khalid Alvi, New Algorithm For Halftone Image Visual Cryptography, IEEE 2004
13. Aderemi Oluyinko, Some improved genetic algorithms based on Heuristics for Global Optimization with innovative Applications, Doctorial thesis, 2010