MAJOR PROJECT

Synopsis

on

Image Steganography Using Genetic Algorithm And Visual Cryptography For Secure Data Hiding And Transmission Over Network

Under The Supervision Of

Mr. Shahzad Alam

Submitted By

Ankur Saldhi 11-CSS-10

Mohammad Amir Jamil11-CSS-33

ABSTRACT

A large number of commercial steganographic programs use the Least Significant Bit 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 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. 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 python platform which shows that the proposed system is highly secure and reliable.

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.

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 rightmost bit in a binary notation is replaced with a bit from the embedded message.

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.

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 subsequence 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.

PROPOSED METHOD

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. 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.
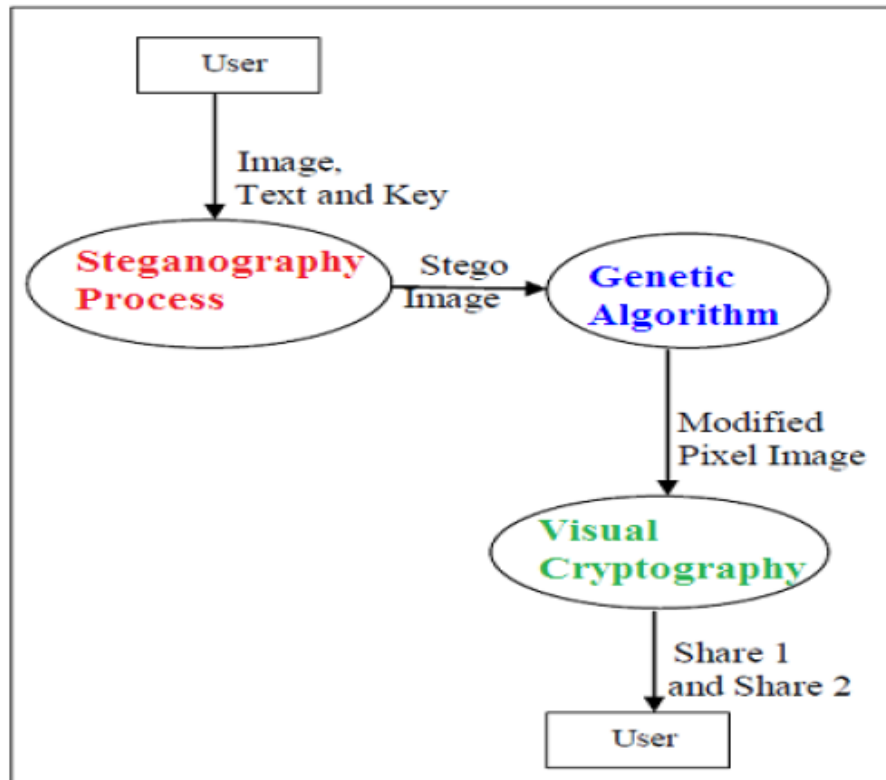
ENCRYPTION PROCESS
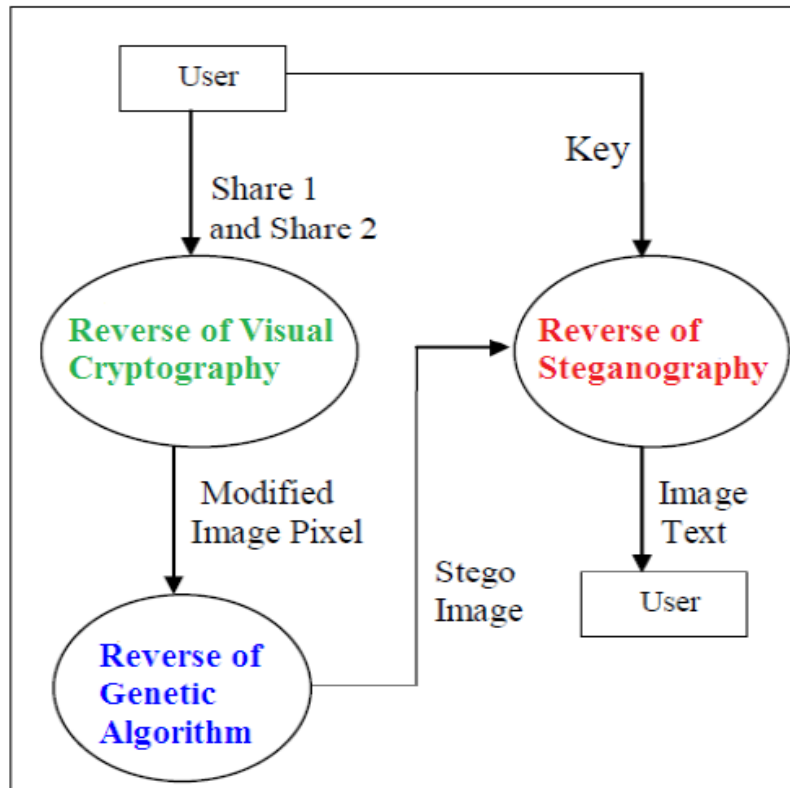
DECRYPTION PROCESS

Algorithmic 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.

PROGRAMMING ENVIRONMENT

PYTHON

Python is a widely used general purpose, high level programming language .Its design philosophy emphasizes code readability , and its syntax allows programmers to express concepts in fewer lines of code than would be possible in languages such as C++ or Java. The language provides constructs intended to enable clear programs on both a small and large scale.

Python integrated development environment supports multiple programming paradigms , including object oriented, imperative and functional programming or procedural styles. It features a dynamic type system and automatic memory management and has a large and comprehensive standard library.

Python interpreters are available for installation on many operating systems, allowing Python code execution on a majority of systems.

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 steganography*", IEEE Journal of Selected Areas in Communications, 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.*

Weblinks:

http://www.sciencedirect.com/
http://ieeexplore.ieee.org/Xplore/home.jsp