Steganography Using Genetic Encryption Along With Visual Cryptography

Shruti Sekra[1], Samta Balpande[2], Karishma Mulani[3]
G. H. Raisoni Institute of Engineering and technology, Wagholi, Pune, Maharashtra, India

ABSTRACT
Authentication login plays a major rule in today's world. Due to unavoidable hacking of the databases, it is always quite difficult to trust the information. The project work aims to solve the problem of authenticity. In this paper, we are proposing a technique utilizing image processing, Steganography and visual cryptography, and then dividing it into shares. In this project the message or the text file is taken as an input from the user which needs to get embedded in the image file. The image file can be of the extensions .jpg or .png. It focuses on hiding secret messages inside a cover medium (image). The most important property of a cover medium is the amount of data that can be stored inside it without changing its noticeable properties. There are many sophisticated techniques with which to hide, analyze, and recover that hidden information. This paper discusses an exploration in the use of Genetic Algorithm operators on the cover medium. Elitism is used for the fitness function. The model presented here is applied on image files, though the idea can also be used on other file types. Our results show this approach satisfied both security and hiding capacity requirements.

Keywords—Genetic Algirithm, Steganography, visual cryptography, Encryption, Decryption

I.INTRODUCTION

Steganography is a branch of information hiding. It embeds the secret message in the cover media (e.g. image, audio, video, etc.) to hide the existence of the message. Steganography is often used in secrete communication. In recent years, many successful steganography methods have been proposed. Among all the methods, LSB replacing method is widely used due to its simplicity and large ca-
pacity. The majority of LSB steganography algorithms embed messages in spatial domain, such as BPCS, PVD. In the LSB steganography, secret message is converted into binary string. Then the least signicant bit-plane is replaced by the binary string. The LSB embedding achieves good balance between the payload capacity and visual quality. However, the LSB replacing method ips one half of the least-signi_cant bits. Thus the artifacts in the statistics of the image are easy to be detected.
The basic structure of Steganography is made up of three components:
i. The Carrier image,
ii. The Message,
iii. The Key
The carrier can be a painting, or a digital image. It is the object that will „carry" the hidden message. A key is used to decode/decipher/discover the hidden message. This can be anything from a password, a pattern, a black-light etc.

Steganalysis is the method to reveal the hidden messages, even some doubtful media. The attacks on LSB replacing methods are most based on Chi-square analysis and the relationship of pixels or bit planes.

The genetic algorithm is used to estimate the best adjusting mode. By the adjustment, the artifacts caused by the
steganography can be eliminated and the image quality will not be degraded. Experimental results of another RS-resistent method are compared with the proposed one, and it is revealed that the proposed algorithm exhibits excellent security and image quality.

II. LITERATURE SURVEY

The simplest insertion method in steganography is LSB replacement steganography. In the LSB
replacement method, the least significant bit of the pixel values are replaced with the bit values of the message. The method of detecting the secret message hidden in the cover media through steganography is known as steganalysis. Steganalysis methods are of two types, one that attacks only color images or grayscale images and the other which attacks on both color and grayscale images. However, irrespective of the mentioned type of image, some of the steganalysis methods attack only on LSB embedding, while others attack on different methods which also include LSB embedding. Few of the steganalysis methods suspect the message hidden in the

image whereas few other steganalysis methods detect the length of the message hidden in the image.

Arezoo Yadollahpour and Hossein Miar Naimi proposed a steganalysis technique using autocorrelation coefficients in colour and grayscale images. They suggest that insertion of secret message weakens the correlation between the neighbour pixels and thereby enable one to detect the message.

Fridrich et al proposed an effective steganalysis technique popularly known as RS steganalysis, which is reliable even in the detection of non-sequential LSB embedding in digital images.

Andrew D Ker has proposed a general framework for structural steganalysis of LSB replacement for detection and length estimation of the hidden message. He suggests the use of previously known structural detectors and recommended a powerful detection algorithm for the aforementioned purpose.

Tao Zhang and Xijian Ping have proposed a steganalysis method for detection of LSB steganography in natural images based on different histogram. This method ensures reliable detection of steganography and estimate the inserted message rate. However, this method is not effective for low insertion rates.

III.PROPOSED SYSTEM:

The proposed system makes use of both stegnographic as well as visual cryptographic technique.Stegnography uses Genetic algorithm for providing security and the second protection lock used is visual cryptography.So combining both stegnography and visual cryptographic algorithm enhace double security to the system.

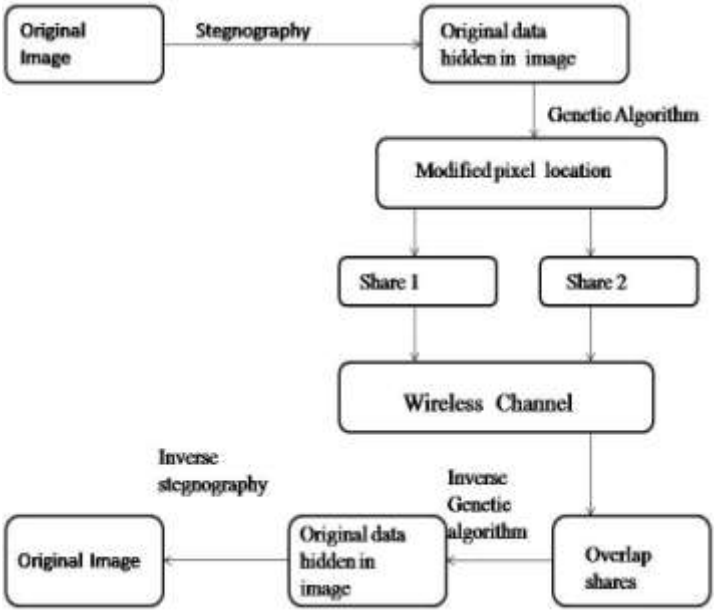

Fig.Proposed Model

1. Genetic Algorithm:

Genetic Algorithm (GA) is based on biological evolutionary theories and is often used to solve optimization problems. GA comprises of a set of individual elements (the population) and a set of biologically inspired operators. According to evolutionary theories, only the most suited elements in a population are likely to survive, generate offspring, and transmit their biological heredity to the new generations. GA's are much superior to conventional search and optimization techniques in high dimensional problem spaces due their inherent parallelism and directed stochastic search implemented by recombination operators.

In a genetic algorithm, a population of candidate solutions (called individuals, creatures, or phenotypes) to an optimization problem is evolved toward better solutions. Each candidate solution has a set of properties (its chromosomes or genotype) which can be mutated and altered; traditionally, solutions are represented in binary as strings of 0s and 1s, but other encodings are also possible. A part of the chromosomes is called a gene

Outline of the Basic Genetic Algorithm:

In Genetic algorithm we are using three operators i.e selection operator, crossover operator and mutation operator.

1. Selection operator: selection operator randomly chooses any one pixel of the image to modify.

2. Crossover Operator: In crossover operator whatever the pixels are chosen by selection operator, those pixels are shuffled by column and row shuffling.

3. Mutation Operator: In Mutation operator whatever the pixels are not modified in crossover operator, there values are modified.

2. LSB Algorithm:

LSB (Least Significant Bit) substitution is the process of adjusting the least significant bit pixels of the carrier image. It is a simple approach for embedding message into the image. The Least Significant Bit insertion varies according to number of bits in an image. For an 8 bit image, the least significant bit i.e., the 8th bit of each byte of the image is changed to the bit of secret message. For 24 bit image, the colours of each component like RGB (red, green and blue) are changed. LSB is effective in using BMP images since the compression in BMP is lossless. But for hiding the secret message inside an image of BMP file using LSB algorithm it requires a large image which is used as a cover. LSB substitution is also possible for GIF formats, but the problem with the GIF image is whenever the least significant bit is changed the whole colour palette will be changed. The problem can be avoided by only using the gray scale GIF images since the gray scale image contains 256 shades and the changes will be done gradually so that it will be very hard to detect. For JPEG, the direct substitution of steganographic techniques is not possible since it will use lossy compression. So it uses LSB substitution for embedding the data into images. There are many approaches available for hiding the data within an image: one of the simple least significant bit submission approaches is, Optimum Pixel Adjustment Procedure‟ . The simple algorithm for OPA explains the procedure of hiding the sample text in an image.

Step1: A few least significant bits (LSB) are substituted with in data to be hidden.
Step2: The pixels are arranged in a manner of placing the hidden bits before the pixel of each cover image to minimize the errors.
Step3: Let n LSBs be substituted in each pixel.
Step4: Let d= decimal value of the pixel after the substitution.
d1 = decimal value of last n bits of the pixel.
d2 = decimal value of n bits hidden in that pixel.
Step5: If (d1~d2)<=(2^n)/2
then no adjustment is made in that pixel.
Else
Step6: If(d1<d2)
d = d – 2^n.
If (d1>d2)
d = d + 2^n.
This,,d‟ is converted to binary and written back to pixel
This method of substitution is simple and easy to retrieve the data and the image quality better so that it provides good security.

3. Encryption and Decryption Algorithm:

The different symmetric encryption algorithms are

1. Data encryption standard
2. Advanced encryption standard

1. Data encryption standard (DES):

Data Encryption Standard‟ (DES) is also known as Data Encryption Algorithm (DEA). DEA takes 64 bits of plain text and 56 bits of key to produce 64 bits cipher
text block. The DES algorithm always functions on blocks of equal size and uses the permutations and substitutions in algorithm.
The data encryption algorithm uses 56 bit key so it is not possible for the defender
for analysing the key. So, the problem of Cryptanalysis is avoided using this
algorithm. But the drawback of the algorithm is Brute-force attack. This can be avoided using the Triple DES algorithm.
Triple DES:

Triple DES is an extension to the DES algorithm. Triple DES uses the same
approach for encryption as DES. 3DES takes three 64 bit keys which has a total
length of 192 bits. We can give more than one key that is two or three keys for
encryption as well as for decryption such that the security will be stronger. It is times stronger than the normal DES algorithm, so that this algorithm can avoid the brute force attack. The main drawback of using 3DES algorithm is that the number of calculations is high reducing the speed to a greater extent.

And the second drawback is that both DES and 3DES use same 64 block size to avoid security issues. "Advanced Encryption Standard" algorithms are used to avoid these limitations.
Advanced Encryption Standards:
Advanced Encryption Standards (AES) takes a block of size 128 bits as input and
produces the output block of same size. AES supports different key sizes like 128,
192 and 256 bit keys. Each encryption key size will change the number of bits and
also the complexity of cipher text.
The major limitation of AES is error propagation. The encryption operation and key generation both engage in number of non linear operations, so, for lengthy
operations it is not suitable.

IV.VISUAL CRYPTOGRAPHY

Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. Specifically, visual cryptography allows effective and efficient secret sharing between a number of trusted parties. As with many cryptographic schemes, trust is the most difficult part. Visual cryptography provides a very powerful technique by which one secret can be distributed into two or more shares. When the shares are xeroxed onto transparencies and then superimposed exactly together, the original secret can be discovered without computer participation.

1. VCS Algorithms

VCS Scheme normally involves two algorithms [4]:

- Algorithm for creating shares
- Algorithm for combining shares

One important functional requirement of any VCS system is size of shares which should be same as that of original image to prevent doubt for unauthorized user.

1.1 Algorithm for creating shares:

This algorithm divides secret image into n number of shares. The shares created by this algorithm will be in unreadable format such that it is impossible to reveal secret image. Single share cannot reveal the secret image. If these individual shares are transmitted separately through communication network, security is achieved.

1.2. Algorithm for combining shares:

This algorithm reveals the secret image by taking the number of shares as input. Some algorithm may take all shares as input and some other algorithm may take subset of shares as input. Decryption is done by merging shares which has taken as input.

DATA TRANSMISSION OVER NETWORK:

Wi‑Fi Protected Access (WPA and WPA2):

Wi‑Fi Protected Access encrypts information and makes sure that the network security key has not been modified. Wi‑Fi Protected Access also authenticates users to help ensure that only authorized people can access the network.

There are two types of WPA authentication: WPA and WPA2. WPA is designed to work with all wireless network adapters, but it might not work with older routers or access points. WPA2 is more secure than WPA, but it will not work with some older network adapters. WPA is designed to be used with an 802.1X authentication server, which distributes different keys to each user. This is referred to as WPA-Enterprise or WPA2-Enterprise. It can also be used in a pre-shared key (PSK) mode, where every user is given the same passphrase. This is referred to as WPA-Personal or WPA2-Personal.

VI.CONCLUSION AND FUTURE WORK

In the present world, the data transfers using internet is rapidly growing because it is so easier as well as faster to transfer the data to destination. So, many individuals and business people use to transfer business documents, important information using internet. Security is an important issue while transferring the data using internet because any unauthorized individual can hack the data and make it useless or obtain information un- intended to him.
The proposed approach in this project uses a new steganographic approach called image steganography. The application creates a stego image in which the personal data is embedded

and is protected with a password which is highly secured.

The main intention of the project is to develop a steganographic application that provides good security. The proposed approach provides higher security and can protect the message from stego attacks. The image resolution doesn't change much and is negligible when we embed the message into the image and the image is protected with the personal password. So, it is not possible to damage the data by unauthorized personnel.

Using Least Significant Bit algorithm in this project for developing the application which is faster and reliable and compression ratio is moderate compared to other algorithms.

The major limitation of the application is designed for bit map images (.bmp). It accepts only bit map images as a carrier file, and the compression depends on the document size as well as the carrier image size.

The future work on this project is to improve the compression ratio of the image to the text. This project can be extended to a level such that it can be used for the different types of image formats like .bmp, .jpeg, .tif etc., in the future. The security using Least Significant Bit Algorithm is good but we can improve the level to a certain extent by varying the carriers as well as using different keys for encryption and decryption.

VII.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] 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 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.

[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