International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue III, March 2018- Available at www.ijraset.com

Genetic Algorithm Based Steganography

Mr. A. A. Hipparkar[1], Mr. Ganesh Nale[2], Mr. Aditya Mohite[3], Mr. Sanket Chitnis[4], Mr. Sadik Attar[5]
[1, 2, 3, 4, 5,] *Ug Student, Computer Science And Engineering, Pes's College Of Engineering, Phaltan, India* [2-5]

Abstract: ***Steganalytic methods are used to check if an image contains a hidden message or not. After examining the image characteristics in between stego image (the image that contains a secret message) and cover image (the image that does not contain a secret message) a steganalytic system identifies the stego image. We use genetic algorithm based technique to develop a stego image by modifying grey values of cover image by generating desired statistic characteristic for producing the stego image. This stego image can pass through the steganalytic system without being detected.***

Keywords: Genetic Algorithm (GA), Steganography, Fitness Function, Cross-over, Mutation, Stego-image, Cover-image, Spatial-Domain steganalytic System(SDSS).

I. INTRODUCTION

Steganography is an old method of hiding secret messages within other carriers in such a way that only the recipient knows the existence of the message [1].

It differs from cryptography which encodes messages, so that nobody can read it without the specific key. Another technique, digital watermarking, is concerned with issues related to copyright protection and intellectual property and therefore a watermark usually contains the information regarding the carrier and the owner [2, 3].

We have used Genetic algorithm to implement the steganographic system that will not be detected by a steganalytic systems. For steganographic systems, the basic need is that the stego-object should be perceptually indistinguishable to the degree that it does not raise any doubt about security.

In other words, the hidden information introduces only little bit modification to the cover-object and most common attackers tries to analyze the statistical features of stego- image.

II. PROBLEM DEFINITION

Since the security is measure issue now a days in steganography of image, we have to provide the security to our stego-image. Hence we are going to implement the Genetic Algorithm based methodology for breaking the steganalytic system. Here we are trying to break the SDSS

III. PROPOSED SYSTEM

The Genetic Algorithm (GA) is a flexible approach which provides a randomized, parallel, and global search based on the technique of natural selection and genetics for finding solutions of a problem.

GA starts with randomly selected genes as the first generation, called Population. Every individual in the population related to a solution in the problem domain is called a Chromosome.

An objective, called fitness function, is used to assess the quality of each chromosome. The chromosomes of best quality will survive and generate a new population of the next generation. By using the three operations: reproduction, crossover and mutation we recombine a new generation to find the best solution. The process is continued until a predefined condition is met or a predefined number of iterations are reached.

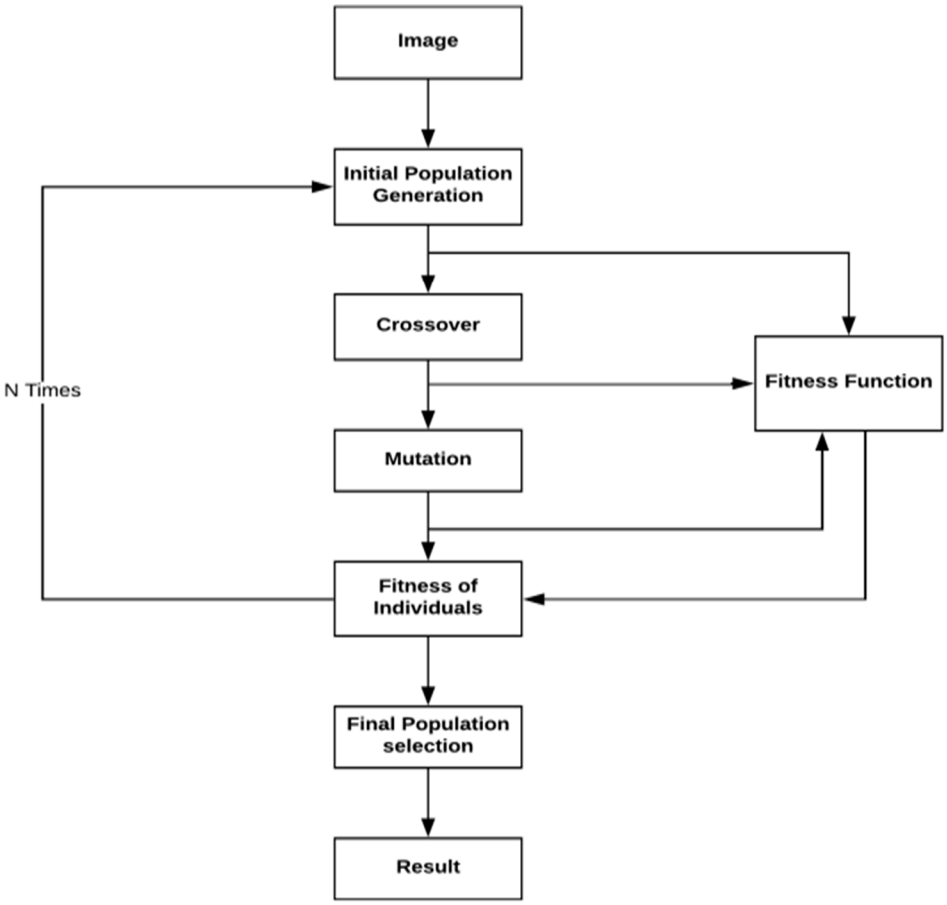

Fig: Flow Chart for Genetic Algorithm [4].

A. Operations Performed on Cover-Image

1) Fitness function: It is used to determine fitness for all chromosomes. If any chromosome exhibits the fitness function as f(x) = x then it has highest ideal fitness in population. Fitness(x) is calculated as: f(x) = min [abs(x-red), abs(x-green), abs(x-blue)]

2) Crossover: Crossover is a process of combining 2 chromosomes to form another chromosome Crossover is as follows:

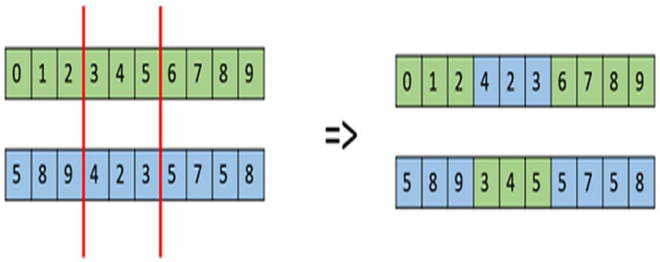

Fig: Process of Crossover [4].

3) Mutation: Altering the genes of given chromosomes so that we give a fair chance for population to evolve and not work repeatedly with the same chromosomes. Mutation is computed as: Mutation(x) = x ± (mutation rate * (x))

4) Advanced Encryption Standard (AES): It is a symmetric key algorithm and fully open for public security. We have used key having size 16 bits. We have made a provision to read the text file and apply the encryption on the data containing in that file.

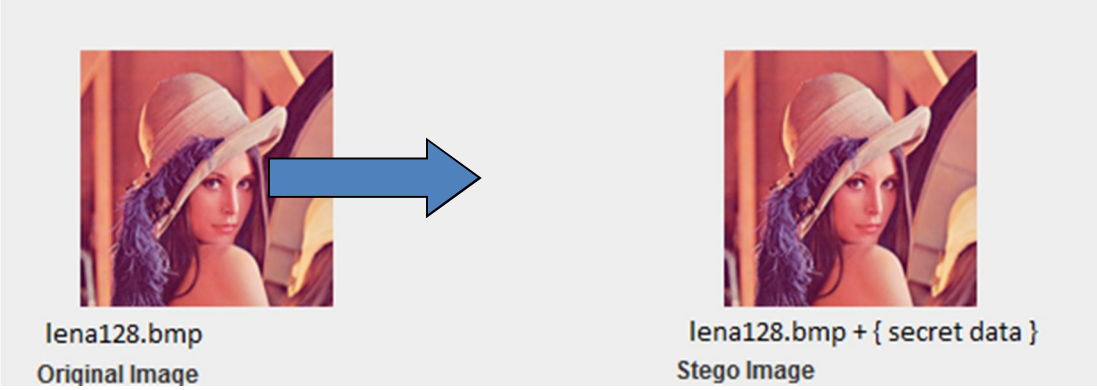

Fig: Process of Generating Stego-Image

B. Algorithm for breaking SDSS

If statistic features of an image varies after hiding data, then it will lead to easily detect that image containing hidden data. For this purpose we are using SDSS that allow to choose a position for coefficient such that it will not lead to variation in the statistic features and allow only little bit modifications [5][6].

C. Analysis of Stego Image and Original Image

By using SDSS we can compare stego image and original image and it will analyses the total number of red, green and blue pixels modified, mean squared error (MSE), peak signal to noise ratio (PSNR).

IV. LITERATURE SURVEY

Least significant bit [2]: Least Significant bit (LSB) Proposed by Dumitrescu, S. W. Xiaolin and Z. Wang which is simple and most commonly used approach for image steganography. Least significant bit of some or all bytes are replaced by the bit of hidden message. Considering a 24-bit image, a bit of each red, green and blue color can be used, since they are each represented by a byte. Single pixel is storing 3 bits of hidden message.

A. For example, grid of 3 pixels of a 24-bit image shown as follows

(00101101 00011100 11011101)
(10100111 11000101 00001101)
(11010010 10101101 01100011)

1) Advantages

a) It is easy to implement and it is also difficult to detect by human
b) It works well in case of high payload, and carries one bit of the secret message per byte of pixel data.

2) Disadvantages

a) The integrity of the hidden message can easily be destroyed due to vulnerability by randomizing the LSBs of the image.
b) Although the attacker may not be aware about stego-image, but such actions would destroy the secret message.

B. Digital Watermarking [3]

A digital watermark allows piece of information that is to be hide directly in media contents, in such a way that it is invisible and inaudible to a human observer, but easily detected by a computer. This makes watermarks suitable for several applications including Signatures, Fingerprinting, Broadcast and Publication Monitoring, Authentication, Copy control, Secret communication.

1) Advantages:

a) The contents are irremovable from the watermark so it can identify the author of copyrighted work uniquely
b) Embedding of watermark is easy
c) Image tampering can be detected easily.

V. FUTURE SCOPE

The capacity to hide large amount of data in the cover image or file is wide scope for enhancement in steganographic system. Currently it can use only certain amount of data bits in cover without degrading the cover file, so there will be demand to hide large amount of data. Compression of huge amount of data and storing it in small file can lead to large scale steganography.

VI. CONCLUSION

We are using GA- Based algorithm for generating stego image for breaking steganalytic system. We are using fitness function to evaluate the quality of each chromosome in order to generate stego image that can be pass through inspection of steganalytic system.

REFERENCES

[1] Yi-Ta-Wu and Frank Y. Shih "Genetic Algorithm Based Methodology for Breaking the Steganalytic System," Part B: CYBERNETICS, Vol. 36, No. 1, February 2006.

[2] F. M. Shelke, A. A. Dongre, P.D. Soni "Comparison of Different Techniques for Steganography in Images," Dept. Computer. Sci., P. R. Patil College of Engineering, Amravati, India, Feb 2014.

[3] I. J. Cox. J. Bloom, M. Miller and I. Cox, "Digital Watermarking: Principles and practice," New York Morgen Kaufmann 2001.

[4] “Principles of Soft Computing” by Dr. S. N. Sivanandam and Dr. S. N. Deepa.

[5] A. Westfeld and A. Ptzmann, "Attacks on steganographic systems, breaking the steganographic utilities" EzStego, Jsteg, Steganos, and S-tools and some lessons learned, in Proc. 3rd Int. Workshop on Information Hiding, Dresden, Germany, September 1999.

[6] H. Farid, "Detecting Steganographic Message in Digital Images," Dept. Computer Sci., Dartmouth College, Hanover, NH, Tech. Rep. TR2001-412, 2001.