A Review on Steganography Techniques and Genetic Algorithm used in Information Hiding

Farheen Fatima¹, Shashwat Shukla², Brahma Hazela³

¹Dept. of Computer Science & Engineering
ASET, Amity University Lucknow
Lucknow, India

Abstract—in the present scenario of the internet world, with the extreme necessity of data transmission, there comes a huge need of data protection. The secret information required by any organization is hidden using cryptography and steganography techniques. The various techniques of steganography that are used by far include three layers of protection which is done by segmenting the image through random selection of pixels. This brings in picture the main case and sub case of the selected byte. Another important aspect is steganalysis that has contradicted steganography to a great extent. But then comes the optimized algorithm, genetic algorithm. It helps in modifying the pixel values so that the hidden message doesn’t even come into existence for any intruder. This approach triggers on conversion of secret message into a binary string and then applying all the operations of genetic algorithm namely reproduction, cross-over and mutation in order to find out the best pixel area to embed the hidden data. These approaches have proved worthy for exchanging secret messages.

Keywords—steganography, random selection of pixels, genetic algorithm, segmentation

I. INTRODUCTION

With the rising need of ease of exchanging information, wireless network have come a long way in accomplishment of this need. Now when it is comes to transmitting any secret information, there arises instant need of security. Steganography is the term that deals with the hiding of information. It hides the information using any cover medium i.e. digital images, audio or video files. This process of hiding data should be done in a way that no one can detect its existence. There are different approaches of hiding information. In one of the process of invisible communication we can use three layer securities by adaptive image filtering and segmentation. In order to select the pixel area we adopt random selection method and embed the secret message there. Further this selection is done on the basis of main cases and subcases which are applied to the selected byte. We take good case of the size of the image and compress it to encrypt the secret file.

Another approach for this is hiding information using Genetic Algorithm. This approach is basically derived from steganalysis, where one can determine the existence of steganography. In order to assure that no intruder come across the existence of the hidden information we use Genetic Algorithm. The secret message is converted into a binary string and the alterations are done in the LSB of the selected area. This approach helps in producing better visual quality of the image and also ensures to decrease the chances of existence of steganography. Both these approaches are explained in the upcoming sections.

II. STEGANOGRAPHY TECHNIQUE

A. Basic Steganography

Till now a lot of work has been done using steganography technique. In general we can divide these techniques into two basic forms. The first one is the one in which the source image pixels are directly been embed with the secret message; this approach is coined as spatial domain steganography technique. The other technique is the one in which we deal with altering the frequency coefficients; this approach is coined as frequency domain steganography technique. As discussed by Nameer et al.[2] for hiding the data a three layer high security approach is used. The new LSB steganography technique is the one that differs from other traditional LSB techniques where taking a 24-bit color image could only embed 3 bits of data for each red, green and blue color components. Thus, this issue of inserting more secret information in more space came into existence.

B. New Steganography Algorithm

The new steganography algorithm came with the three layer security. The first layer worked on encrypted password using DES algorithm. The second layer worked on protecting the segmentation password and the third layer helped in securing steganography algorithm. A new concept for segmentation of image which stated that the cover image should be segmented randomly in uniform or non-uniform segments with respect to their passwords. This technique was implied on BMP image that gave lossless compression to the selected image. After segmentation comes pixel selection, where the random pixels are selected on the basis of color characteristic contained in that particular area. These concepts are introduced in order to obtain reduction in the noise of stego-image. The
The steganography algorithm used here, ensures that it provides the following:

- Robustness against the different inevitable attacks.
- Enough space for embedding secret message.
- No chance of detection of the existence of steganography.
- Conformity of extracting password securely at receiver’s end by doing proper scanning of segmented pixel.

The use of main case and sub case helps in organizing the pixel architect in the best possible way so that more information can be hidden.

III. GENETIC ALGORITHM BASED STEGANOGRAPHY

A. Basic idea of the approach

Genetic algorithm focuses on providing optimal solution to any problem by selecting data from a pool of information. The operations used in genetic algorithm i.e. mutation, cross-over, reproduction play a significant role in finding optimal solution for any problem. Previously genetic algorithm based steganography has been used on color images. This has been further extended by using frequency domain approach and embedding the secret message using Discrete Fourier Transform (DFT), z-transform, wavelet transform. The work, done by Shen et al.[4] has given good solution for obtaining better visual quality stego-image as well as masking a secret message which could be RS-attack free. It focuses on refusing the RS-analysis on any hidden data by making the stego-image appear as a normal image i.e. leaving no chance of doubts for the intruder to get confirmation of existence of steganography.

B. Working

Initially a block of pixel is selected. The values of the bits of the selected pixels are adjusted in such a manner that only the second and third lowest bit planes are modified. It is done so because changes in the higher bit plane could lead to the changes quite prominently noticeable. Now the selected blocks of stego-image are labeled and the whole process of bit selection gets started, using the three most important operations of genetic algorithm namely reproduction, cross-over and mutation. Now the individuals with higher fitness function are liable to be selected to the breed of the next generation. Now the secret message is converted into binary string and the selected LSB is replaced by this binary string. Thus, the secret message is embed in the selected block of image. This approach ensures to preserve the quality of the image as well as it leaves no clue of the existence of steganography, as it preserves the correlation between the adjacent pixels of the stego-image without making any change apparent.

This approach focuses on following:

- To preserve the quality of image even after steganography.
- To make sure that the image stays RS-attack free.
IV. CONCLUSION

The discussed algorithms have proved effective in embedding the secret message by solving the process of selection of desired pixel in an optimized way. Thus, maintaining the quality of the image and preserving its security, which is the most important issue while hiding any private or secret data, the above discussed approaches have helped us in a very productive way.

REFERENCES