ISSN:0975-9646

A Survey on Steganography Techniques & Genetic Algorithm based Steganography in Image Masking

Farheen Fatima, Shashwat Shukla, Brahma Hazela

Department of Computer Science & Engineering,

ASET, Amity University Lucknow,India

***Abstract*— This paper gives a review of the different steganography techniques that have been used so far. Right from basic steganography to the three layer security steganography algorithm, it has helped us in undergoing a secure communication. For the purpose of exchanging secret message we have also used genetic algorithm based steganography techniques. Different steganography techniques have been compared in order to infer the benefits of each of them. Adaptive segmentation and filtering is done on the pixels in order to make the process of selecting the masking area of the cover image easy, thus encouraging random selection process of pixels. Further, use of genetic algorithm has helped in getting a better quality image after embedding a secret message on it. Also its operations i.e. reproduction, crossover and mutation has played a vital role in making optimal choice for selecting the targeted pixel area.**

***Keywords*— steganography, random selection process, adaptive segmentation, genetic algorithm.**

I. INTRODUCTION

From the time wireless network came into existence, it has worked really well in exchanging information over internet. With this ease of exchange of information, arises a strong need of security. And when it comes to share secret information it is necessary to share it through the most secretive and secure channel. Steganography, a technique often referred as invisible communication has come a long way in fulfilling the above need for exchanging secret information. It has helped in hiding the private data in image, audio, video and text. There are different techniques under steganography that have helped in embedding the secret data in such a way that the change is not apparent. Similarly there is genetic based steganography that has helped in finding out optimal solution for selecting the area to embed the information in a much easier manner. The upcoming sections will help in understanding the data hiding techniques more clearly.

II. STEGANOGRAPHY TECHNIQUES

A. Introduction

Basically, steganography stands for invisible communication. It helps in transferring the secret data from one end to the other end in the most reliable manner. We can say it's a masking technique that masks the private data and transfers it to the receiver ensuring the security of the information. The security has increased from normal methodology to three layer security. Since, here we are dealing with images so we have used bitmap images for masking.

B. Adaptive Segmentation

Here we randomly select an area of a cover image and apply adaptive segmentation technique, where we select the random number of uniform or non-uniform pixels according to certain values of some allocated keys. This helps in adaptive filtering which in turn makes it easy to select the area targeted for hiding information. Further the file is compressed with lossless compression and the secret file is encrypted. In the fig1 given below we can see the result of adaptive segmentation.

Fig1. Adaptive segmentations in a cover image using uniform and non-uniform segmentations

III. EXISTING STEGANOGRAPHY TECHNIQUES

There are several existing techniques of steganography that have contributed in information hiding. They can be divided into two categories namely spatial domain steganography and frequency domain steganography. We have separately shown the tables for both types of techniques in order to make the difference between them more apparent. All the techniques have their own share of advantages. The tables given below depict the process of masking private data through various steganography techniques.

Table 1: Spatial Domain Steganography Technique

Steganography Technique	Features	Advantages
Least Significant Bit Substitution Algorithm	The LSBs of the cover image are embedded directly on the cover image.	Simplicity and high perceptual efficiency.
Pixel Value Differencing	It sub divides the cover image into blocks. Hides the data by changing the difference between two connecting pixels	It gives results with more quality and better imperceptibility
Grey Level Modification	The data is mapped by modifying grey level value of pixels by using mathematical functions.	It has high hiding capacity and low computation
Prediction Based Steganography	Pixel values are predicted with the help of predictor. Remove loopholes of other techniques by using prediction error values.	It helps improve hiding capacity and visual quality.
Quantization Index Modulation	It modulates an index with embedded information and then applies quantization process.	It has high embedding capacity and it's a highly robust technique

Table 2: Frequency Domain Steganography Technique

Steganography Technique	Features	Advantages
Discrete Wavelet Transformation Technique	It divides the cover image into four sub bands. Entropy coders locate the transform coefficients and locate them.	It has multi resolution nature, makes it quite suitable for scaling image coding. Can be applied with other transforms namely curvelet transform, contourlet transform etc.
Discrete Cosine Transformation technique	It is best suited for JPEG images. Every block of DCT is quantized.	Works well on high frequency area.

a. Lena

b. Lake

Cover images

a. Lena

b. Lake

Stego images

IV. Genetic Algorithm Based Steganography Technique

A. *Introduction*

Genetic Algorithm is an approach that helps in finding any solution in the most optimized way. It consists of different operations i.e. reproduction, crossover, mutation. These operations selecting the best individual from the pool of information based on any fitness function. This process continues until we obtain the most appropriate solution. Thus it helps in making new generation of outputs in order to get the best suitable solution for any given problem.

B. *Methodology*

As we know there are techniques like steganalysis as well where RS-analysis plays a significant role in analysing the existence of steganography, therefore there are chances of RS-attack as well. In order to combat such attacks Genetic algorithm incorporates an RS-attack free approach. It also helps in getting the better visual quality of the image. In this approach the secret message is converted into a binary string. This binary string replaces the LSB of the selected area of the cover image.

Initially a block of image is selected randomly and then it is sub divided followed by labelling of blocks. Now different operations of genetic algorithm are applied which helps in transforming an optimization on the chromosome evolution. After reproduction, crossover and mutation, the individuals with largest fitness function are selected and the secret message is embedded on them. The experimental results of the above methodology can be seen in fig2 where we compare cover images and stego- images.

V. Conclusions

The techniques of information hiding discussed in this paper have proven successful to a great extent for the purpose of sharing secret information. The security measures taken have produced desirable results. It has been observed that the selection of the area for steganography in any image has become easy and productive to a large extent, thus making these approaches quite preferable for any further masking of information in order to maintain the integrity of any secret communication.

References

[1] J.Fridrich, M.Golijan, and D.Hogea, “Detecting lsb steganography in color amd gray-scale images”, IEEE Multimedia, pp. 22-28,2001.

[2] Nameer N and EL-Emam, “Hiding large amount of data with high security using steganography algorithm”, Journal of Computer Science 3(4),ISSN 1549-3636,2007.

[3] C.T.Hsu, J.Wu, and L.Hidden, “Digital Watermarking in images”, IEEE Trans. Image Processing, pp. 58-68,1999.

[4] Shen Wang, Bian Yang, and Xiamu Niu, “A secure steganography method based on genetoc algorithm”, Journal of Information Hiding and Multimedia Signal Processing, Volume 1,Number 1, ISSN 2073-4212, January 2010.

[5] Ahn, L.V., and N.J. Hopper, “Public-key steganography”, Springer-Verlag Heidelberg,In Lecture notes in Computer Science, Vol. 3027/2004 of Advances in Cryptology-EUROCRYPT 2004, pp: 323-341, 2004.

[6] Moulin, P. and J.A. O’Sullivan, “Information-theoretic analysis of information hiding”, IEEE Trans. On Info. Theory,49:563-593,2003.

[7] Pavan, S.,S. Gangadharpalli and V.Sridhar, “Multivariate entropy detector based hybrid image registration algorithm”, IEEE Intl. Conf. on Acoustics, Speech and Signal Processing, pp:18-23,2005.

[8] Amin, P., N. Liu and K. Subbalakshmi, “Statistically secure digital image data hiding”, IEEE Multimedia Signal Processing MMSP05,China,2005.

[9] Zhang, X. Wang, S., Qian, Z., and Feng, G., “Reversible fragile watermarking for locating tampered blocks in JPEG images”, Signal Processing,90(12), 3026-3036, doi;10,1016/j.sigpro,2010.

[10] Rongsheng, X., Keshuo, W., and Shunzhi, Z.’ “An improved emi-fragile digital watermarking scheme for image authentication”, Paper presented at the Anti-counterfeiting,Security,Identification, IEEE Internatinal workshop,2007.