

A Novel Approach for Data Security for Cloud Data using Image Steganography and Genetic Algorithms

M.Seshubhavan¹, S.Asha Varma² and Davuluri Suneetha³

^{1,3}Associate Professor,CSE Dept, NRI Institute of Technology, Pothavarapadu,AndhraPradesh,India

²Assistant Professor,CSE Dept, NRI Institute of Technology, Pothavarapadu,AndhraPradesh,India

Abstract—Cloud Computing is a powerful, flexible, cost efficient platform for providing IT services over the Internet. However Cloud Computing has various levels of risk factors because services are maintained by third party vendors and the most important information is handled by third party, so harder to maintain the security. Steganography is the one of the technique to provide security for secret data in inserting an image or video. In the most of the steganographic algorithms secret data is inserted in Least Significant Bit of an image but the hackers easily detect the algorithm and hack the secret data easily. In this paper proposed an approach based on the heuristic genetic algorithm for hiding secret data in the original image and instead of considering only Least Significant Bit and we also consider Most Significant Bit with the help of Image Segmentation technique. The proposed approach will be tested and analyzed for various color and gray scale images of different sizes for different length of secret messages. The performance of the proposed approach will be analyzed with various parameters like PSNR, MSE and the results are good compared with existing algorithms.

Index Terms— Heuristic Genetic Algorithm, Image Segmentation, PSNR, MSE.

I. INTRODUCTION

In Cloud Computing environment, one of the vital parameter is to providing security for user's secret data. We have so many approaches like cryptography, Steganography and watermarking hiding strategies, with the help of this techniques we can hide the secret data in an image. Those techniques are suffered with some problem because in this environment data is maintained by third party from different locations of different users with different formats. In cloud environment data is accessed by third party and it is difficult to maintain the security. So it is necessary to have novel method which can have the capability of embedding data securely before placing into the cloud environment. For this in the proposed approach Steganography technique has chosen and image segmentation is utilized for maintaining of data secrecy.

Steganography is the art and the science to hide the secret data in the form of text, audio and video in an image (cover image). In other words, steganography is a one of the way to hide the secret data from unauthorized persons or which cannot know the presence of secret data for unauthorized persons or hackers.

There are several algorithms to hide the secret data in an image to protect it from unauthorized hackers. This paper introduce a new approach which will hide the secret data in LSB and MSB bits of the image with an heuristic genetic algorithm and image segmentation technique. Also, this proposed algorithm is used for

protecting secret data of any users against steganalysis methods. Steganalysis is nothing but identifying hidden secret data from an original image.. For steganography generally have two phases

1. Techniques before inserting a secret data
2. Techniques after inserting a secret data

In first phase the activities like increase the statistical irregularity of the image. In second phase it will increase the statistical feature of image by using genetic algorithms. So that, the RS get failed to identify the hidden image. The rest of the paper is organized is as follows. In section 2 the previous related work is discussed. The section 3 contains proposed method and section 4 presented the results.

II. RELATED WORKS

There are two types of data hiding are available using images spatial domain and frequency domain. In spatial domain inserting secret message in the least significant bit (LSB) of image pixel. This method is very simple for implementation but less secure because the algorithm is known to all the users and it has low robustness for against some security attacks. In frequency domain inserting secret message in the frequency coefficients of the image. This mechanism overcomes the problem of spatial domain implementation because it has better robustness with the help of DWT coefficients and wavelet coefficients.

In Pelham Ghasemi et al[1]. presents a genetic algorithm based mapping approach to insert in discrete wavelet transform coefficients of the original image. In this technique use optimal pixel adjustment process is applied after inserting the secret message into the image. The main reason behind applying OPAP is to decrease the error ratio between the original image and the stego image. In this we use frequency domain in order to improve the robustness of the steganography technique. With the help OPAP we get the optimal mapping function to reduce the error difference between original and cover image.

In J.K.Mandal et al [2]. proposed another genetic algorithm based approach called DEGGA. In this method the main focus is to place a large amount of hidden data and the results are compared with other existing methods. In this approach use spatial domain and the message is dividing into small blocks. Mutation is applied in embedding process. In this method various statistical parameter are used to identify the exact locations of the image pixel for inserting the secret data. This proposed algorithm have provide better improvements in PSNR, MSE value and also this approach will reduce the error ratio and improve the better robustness.

In Wang et al [3]. suggest another approach for inserting sensitive data in an image basically in this there is no approach for embedding data in the original image. But for providing security for secret data we use least significant bit of the image is used and the pixel values are changed using the genetic algorithm so RS algorithm fail to detect the steganalysis.

In Vijay Kumar sharama et al[5]. proposed another novel genetic algorithm to insert secret data into the original cover image. In this the data is inserted into the least significant bit of the image after embedding the pixels values are changed into the character codes using genetic algorithm and the algorithm performance was analyzed using various parameters like PSNR ,MSE and it provides better results compared to the various existing algorithms.

In Lifang Yu et al[4]. proposed an approach which consists of two parts. In one part adaptive LSB steganography technique is used and in second part visibility of the stego image has been improved. For this they use genetic algorithm which will minimize the error ratio and improve in the robustness of the original image. Experimental results are showed in spatial domain and results are compared with various existing algorithms and improvement in the error ration is showed.

II. BACKGROUNDS

A. Least Significant Bits and Most Significant Bits:

In the proposed approach [6], we will use LSB and MSB bits consideration because it is easy to access and simple to extract the LSB and MSB from an image. Generally an image is converted into binary image which consist of 1's and 0's. Each and every individual pixel is represented by their various characteristics like brightness, quality of an image. The simple steganography algorithm directly insert secret message into the Least Significant Bit but it can easily detect the hackers. So in this extract the LSB and MSB bits from an original image in order to hide the secret data.

III. PROPOSED METHOD

Many of the recent approaches simply insert the secret message in the original image directly or change in the neighboring pixels of an image, it will leads to change in the some of the characteristics of an image. So in the proposed method tries to find out suitable pixels locations in the original image without changing the characteristics of the original image. And the proposed method also reduces the noisy level and error ratio of the original image after inserting secret message into it.

In this proposed approach, the first is to extract the LSB and MSB of the whole original image and place in the array in the form of 0's and 1's. Also the secret message is encrypted with AES encryption algorithm obtains then key, and that one also placed in the same format in another array. To find the suitable pixel location in original image use genetic algorithm. Here data is in the form of string so genetic algorithm is unable to find out so the segmentation is the solution. Each string is divided into segments based on the Lblock and Rblock size. After segmentation the blocks are applied to genetic algorithm to find out the suitable pixels.

Extraction of the secret message from stego image is much easier, for extracting the secret message LSB and MSB of the stego image are extracted and segmented the blocks.

Phase 1: Inserting a secret message

This phase can be implemented by executing the following sequence of steps:

1. Input the cover image
2. Convert the cover image into gray scale image
3. Read the secured secret data into the file and encrypt using AES Encryption algorithm and obtain the key.
4. Prepare the whole image LSB, MSB and secret message as array of 0's and 1's
Extract LSB pixels of the cover image and store them in array STRL
Extract MSB pixels of the cover image and store them in array STRR
Combine STRL and STRR into single array STRF
5. Convert the secret key into binary form of 0's and 1's and store them in STRM
6. Divide the STRF and STRM into segment of block of Lblock and Rblock length
7. Apply these segments to genetic algorithm as initial population and begin the execution of genetic algorithm
8. Rearrange the bits of the selected pixels of STRF with the blocks of STRM and insert the Address block
9. Insert the secret data in the address block locations of the original cover image
10. The obtained image after embedding the secret data is called stego image

Phase 2: Extraction of secrete message from stego image

The stego image is the source for the extraction process. The reverse process is performed to extract the encrypted secret key and the decryption process is performed using the same key.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

The proposed approach is used to insert secret data in the selected pixels of the cover image, which meets the requirements without changing the characteristics of the original image and produce better results. The images are taken from the data set <http://sipi.usc.edu/database/>. We have tested for different types of images like color images and gray scale image with various length size key values and Lblock(8), Rblock(10) values for analyzing the process and shown in figures 1 to 2.



Fig 1.Original image



Fig 2. Image after embedding secret message(key length=16)

V. CALCULATION OF PSNR (PEAK SIGNAL TO NOISE RATIO) AND MSE (MEAN SQUARE ERROR)

In order to calculate the efficiency the two important measurements are Peak signal to Noise ratio and Mean Square Error. The PSNR is the quality measurement between original cover image and stego image higher the PSNR better the quality. The MSE is the error between the original image and the stego image

$$\text{PSNR} = 10 \log_{10}(\text{MAX}_i^2 / \text{MSE}) \quad (1)$$

$$\text{MSE} = \sum_{m,n} [I_1(m,n) - I_2(m,n)]^2 / M * N \quad (2)$$

VI. COMPARISON TABLES

It presents comparison between the previous existing algorithms and proposed algorithm. It shows clearly that the calculated values are better than previous existing algorithm for different images. MATLAB tools are used for analyzing/evaluating the results for various images.

TABLE I. OBTAINED PSNR AND MSE VALUES

Cover Image(512*512)	PSNR	MSE
Minni	67.56	0.0034
Home	62.34	0.0021
lady	71.59	0.0039

VII. CONCLUSION

In this paper we proposed an algorithm to embed the secret message into original image before placing the data into the cloud environment. It provides a better quality ratio with less noise ratio for different images of different key length. The quality of the proposed algorithm was analyzed with the parameters of PSNR and MSE.

REFERENCES

- [1] Elham Ghasemi, "Capacity Image Steganography depends on Genetic Algorithm and Wavelet Transform, S.I. Ao et al. (eds.), Intelligent Control and Innovative Computing, Lecture Notes in Electrical Engineering 110, DOI 10.1007/978-1-4614-1695-1_30.
- [2] Ran-Zan Wang, "Image hiding using LSB and GA", 2015, Published in Elsevier
- [3] J. K. Mandal, "Embedding technique for gray scale images" ICSE2016
- [4] Shen Wang, "Steganography method using genetic algorithm" Journal of Information Hiding and Multimedia Signal Processing c 2017 ISSN 2073-4212. Volume 1, Number 1, January 2017
- [5] Vijay, "Performance improvement of LSB by reducing steganalysis probability" International Journal of Information and Communication Technology Research, Volume 1 No. 4, August 2015.
- [6] Suneetha "EDGE Based Steganography for Cloud Data" International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 16 (2017) pp. 5565-5569.