Reducing Visual Discrepancy in Steganography

S.UMA MAHESWARI

Department of CSE, Thiagarajar College of Engineering, Madurai, Tamil Nadu, India

Abstract

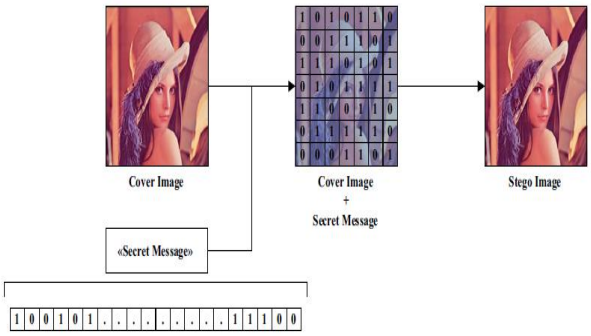
From the past decade many data hiding algorithms are widely used in information security. In data hiding applications, optimization techniques are utilized in order to improve the success of algorithms. The genetic algorithm is one of the largely using heuristic optimization techniques. The problem with genetic algorithm is the computational time. To overcome this, in this paper, chaotic maps are used to improve the data hiding technique based on the genetic algorithm. Peak signal-to-noise ratio (PSNR) is chosen as the fitness function. Different sized secret data are embedded into the cover object using random function of MATLAB and chaotic maps. Randomness of genetic is performed by using different chaotic maps. The success of the proposed method is presented with comparative results. It is observed that gauss, logistic and tent maps are faster than random function for proposed data hiding method.

Keywords: genetic algorithm, PSNR, logistic map.

1. Introduction

1.1 Steganography

Steganography simply takes one piece of information and hides it within another. Computer files contain unused or insignificant areas of data. Steganography takes advantage of these areas, replacing them with information. The files can then be exchanged without anyone knowing what really lies inside of them. An image of the space shuttle landing might contain a private letter to a friend. A recording of a short sentence might contain your company's plans for a secret new product. Steganography can also be used to place a hidden trademarking in images, music, and software, a technique referred to as watermarking. At the same time, moves by various governments to restrict the availability of encryption services have motivated people to study methods by which private messages can be embedded in seemingly innocuous cover messages.



2. Literature survey

This paper analyses the various methods on the steganography based on the spatial domain and transform domain techniques.

In Tahir Ali et al's[1] Method usage of all pixels of the cover image can be carried but message bit is stored in LSB of one of the three-colour components, RGB based on the parity of three LSB's of R, G, B components of 24-bit colour image. Here the method uses the concept of parity check for recovering and hiding secret information or data Each 24 bit colour image has RGB components on 8-bits each initially it collects LSB of three components and form a group of three bits.The embedding method depends on the parity bits and message bits generated by the LSB of each colour components. Result state that method can hide huge volume of data in a single RGB image with relatively small changes in input image pixel value.

In Mamta Juneja et al's[2] Proposed a new hybrid feature detector technique to improvise an approach for Information Security in RGB Colour Images for extracting smooth and edge areas of an image by integrating Canny edge detection and Enhanced Hough transform edge linking method, and for hiding messages two Component based LSB Substitution method for hiding encrypted data in edges areas and Adaptive LSB substitution technique for hiding messages in smooth areas. Enhanced security level for hidden messages and resistance to various attacks is provided along with it by using Advanced Encryption standard (AES) and Random Pixel Embedding Technique.

In Pallavi Das et al's [3]Paper proposes a new image steganography method of by using single cover image to hide the multiple secret images using LSB substitution method. Based on the described method, in a primary colour matrix one of the secret image is embedded in random manner using LSB substitution method. The 24 bit cover image is used composed of RGB 8 bits each all three components are separated to from matrix later red pixel are separated into odd and even terms and form matrix. Later the bits of secret image are embedded in LSB of red pixel even matrix and LSB+1 pixel of odd matrix other secret images are stored in green and blue pixel matrix thus new matrix forms image to transmit reverse process is used for extraction Results reveal that the proposed method has speeder computation level compared to other techniques, low error, and satisfactory visual quality of the image.

In Masoud Nosrati et al's[4] Research paper Steganography in Image Segments using Genetic Algorithm is based on the before embedding hiding techniques it helps to find accurate places in carrier image to store the data with the fewer changes of bits. In order to achieve it segmentation is carried out to convert

message strings and LSB's to the blocks for carrying the genetic algorithm. They key file was created later after locating the exact places to embedded data, the key file is used for message extraction purpose too. The proposed method analysis determines that it offers an efficient method in the field based on least changes in sample image and histogram confirms it.

In S. Thenmozhi et al's [**5**] Demonstrate a new method based on DWT, In the proposed method the secret image is initially scrambled using the chaos theory (Heron map)and the embedded in high coefficients obtained from DWT of the cover image and then the encryption and decryption process is carried out during the decryption process IDWT is used for the image, decryption process is just reverse of the encryption. The result analysis shows that method has high capacity and satisfactory security has the secret message cannot be known without the initial values of heron map, And even the correlation coefficient r is calculated in order to determine the distinguished factors for encrypted image the obtained values state that proposed algorithm is better than previous existing algorithms.

In [6],A new steganography algorithm has been proposed to improve the payload capacity and to reduce the visual discrepancy. In this approach the secret bits were embedded in the middle frequencies of the quantization table and thus more payload was embedded.

3 Proposed system

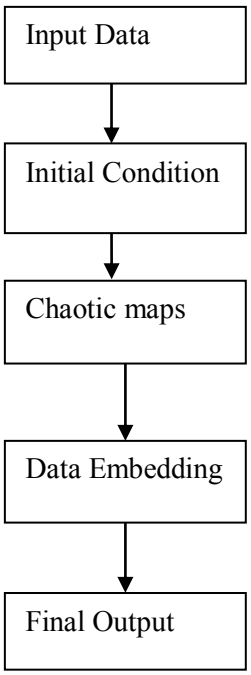
Optimization techniques are used to solve some complex problems. There are some limitations to the optimization techniques used in solving complex problems. In this paper, the data hiding problem is optimized using genetic algorithm. In the genetic algorithm steps, single point crossover operator is applied and the mutation point is randomly selected. PSNR, which is a visual quality metric, is used as fitness function. Row, column and layer information of image are used for generating the population. For 512 × 512 × 3 sized image, individuals consist of 20 bits (log2512 × 512 × 3bits). The genetic algorithm is used to embed secret data into the best indices. Random function of MATLAB and chaotic maps, which are mentioned in Sect. 3, are applied for testing the randomness of the genetic algorithm.

Proposed system advantages

The proposed data hiding algorithm hide data without loss of image quality

- Provide suitable solution with high PSNR

3.1 Design of proposed system



3.2 Dataset collection

UCID - Uncompressed Color Image Database

The UCID dataset currently consists of 1338 uncompressed TIFF images on a variety of topics including natural scenes and man-made objects, both indoors and outdoors. All images were taken with a Minot Image 5 digital colour cameras which, in contrast to many other models, also allows images to be captured in uncompressed form. We set all camera settings to automatic as this resembles what probably most average users would do.

The UCID database is available for fellow researchers and can be downloaded from http://vision.doc. ntu.ac.uk/. We are currently still working on expanding the image set, our aim is to provide a database with ground truth of tens of thousands of images.

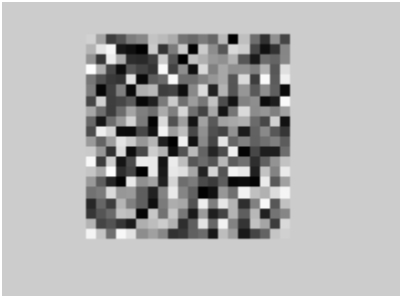
3.3 Algorithm of proposed system

Step 1: Obtain pixels of cover image
Step 2: Determine size of the individuals for $m \times n \times k$ size image
$X = \_\log 2\ m \times n \times k$
Step 3: Generate × bits sized four random individuals using chaotic maps or random function of MATLAB.
Step 4: Calculate PSNR value for individuals in the population
Step 5: Store two individuals that have the best PSNR value.
Step 6: Generate four new individuals from these individuals according to genetic algorithm
steps.
Step 7: Update population with new individuals.
Step 8: Obtain PSNR value after update.
Step 9: Store individuals that are over the threshold value.
Step 10: Remove repeated individuals.
Step 11: Repeat steps 4–10 until reaching the number of iteration or required error value.

4 Experimental results and discussion

4.1 Calculation of PSNR value

PSNR VALUE

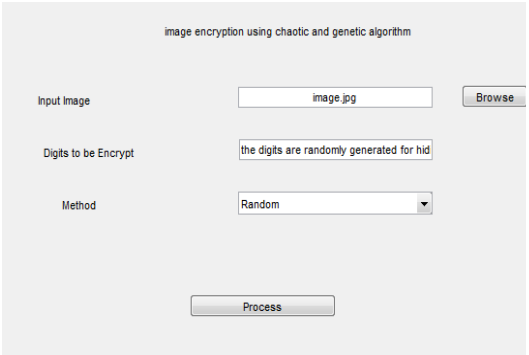


```
p1 =

    7.7577

p2 =

    7.4700

p3 =

    7.7691

p4 =

    7.8410
```

4.3 Random generation


```
THE PSNR OF IMAGE IS:
   70.9776

THE BER OF IMAGE IS:
    0.0013
```

4.2 Encryption



4.4Chaos


```
THE PSNR OF IMAGE IS:
   82.0224

THE BER OF IMAGE IS:
   1.0204e-04
```

5 Conclusion

In this work, We dealt with the techniques for steganography as related to color image. A new and efficient stenographic method for embedding secret message into images without producing a major changes has been done in our project. This property enables the method to avoid steganalysis. This method is also capable of extracting the secret message without the cover image. Also, the researchers can hide a large number of char inside the selected cover image. Experimental results showed that the proposed method gave the best values for PSNR, which means that there is no difference between the original and the Stego images. The limitations in our project is when we do encryption process ,we have to combine the sequences of input image ,logistic map sequence and Arnold sequence ,so the size of the encrypted image may increase. When Com-pared with proposed method our method is more efficient and highly secured ,because in proposed method they used one map for encryption .In our method we use two maps for encryption .The Quality of the image also increased ,which gives high PSNR in our method.

References

[1]. Tahir Ali Amit Doegar **"**A Novel Approach of LSB Based Steganography Using Parity Checker" International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 1, January 2015

[2]. Mamta Juneja and Parvinder Singh Sandhu (2014) "Improved LSB based Steganography Techniques for Colour Images in Spatial Domain" International Journal of Network Security, Vol.16, No.6, PP.452-462, Nov. 2014

[3]. Pallavi Das, Satish Chandra Kushwaha, Madhupama Chakraborty" Data Hiding Using Randomization and Multiple Encrypted Secret Images" the IEEE ICCSP 2015 conference.

[4]. Masoud Nosrati ,Ali Hanani,Ronak Karimi "Steganography in Image Segments using Genetic Algorithm" IEEE2015 Fifth International Conference on Advanced Computing & Communication Technologies.

[5]. S. Thenmozhi,M. Chandrasekaran "A Novel Technique for Image Steganography Using Nonlinear Chaotic Map" IEEE Intelligent Systems and Control (ISCO), 2013 7th International Conference on 4-5 Jan. 2013

[6]. Hemalatha.J, Kavitha Devi M.K., Geetha.S. ″Enhancing the JPEG image steganography security by RSA and attaining high payload using advanced DCT replacement method and modified quantisation table", International Journal of Business Intelligence and Data Mining.DOI: 10.1504/IJBIDM.2019.10010131

[7]. Bhowal K, Pal AJ, Tomar GS, Sarkar PP (2010) Audio steganography using GA. In: International conference on computational intelligence and communication

[8]. Caponetto R, Fortuna L, Fazzino S, Gabriella M (2003) Chaotic sequences to improve the performance of evolutionary algorithms. IEEE Trans EvolComput 7:289â˘A ¸S304

[9]. Dasgupta K, Mondal JK, Dutta P (2013) Optimized video steganography using genetic algorithm (GA). ProcediaTechnol 10:131â˘A ¸S137 13. Drâ˘A ´ Zeo J, Pâ˘A ´ Zetrowski A, Siarry P, Taillard E (2006) Metaheuristics for hard optimization. Springer, Berlin Elattar EE (2015)

[10]. A hybrid genetic algorithm and bacterial foraging approach for dynamic economic dispatch problem. Int J Electrical Power Energy Syst 69:18â˘A ¸S26

[11]. Elshoura SM, Megherbi DB (2013) A secure high capacity full-gray-scale-level multi-image information hiding and secret image authentication scheme via Tchebichef moments. Sig Process Image Commun28:531â˘A ¸S552