Adaptive Image Steganography Using Pixel Intensity Difference

Dr. R.V. Patil[1], Abhinanadan Bharamgunde [2], Murtaza Mithaiwala[3], Darshan Hire[4], Yadnesh hande[5]

[1] *Professor, Computer Engineering, PDEACOEM, Maharashtra, India*
[2] *Student, Computer Engineering, PDEACOEM, Maharashtra, India*
[3] *Student, Computer Engineering, PDEACOEM, Maharashtra, India*
[4] *Student, Computer Engineering, PDEACOEM, Maharashtra, India*
[5] *Student, Computer Engineering, PDEACOEM, Maharashtra, India*

ABSTRACT

In the modern world used of digital liaise has become so popular and billions of people using it. For the secure liaise on sundry platform, web application as well as system application there is need of Internet. For this purpose, various techniques like data encryption/decryption, cryptography, Data hiding Algorithm. But this technique is not too secure and get hacked easily pinch the secret message. To ensure the high security of confidential data communication a new Technique was invented know as Steganography. In this paper, we are introducing a new steganography scheme which is very efficient with respect to data hiding capacity and distortion. The main approach for this algorithm is based on pixel intensity difference.

Keyword: - *Cryptography, Steganography, Pixel Intensity, hacker*

1. Introduction

A huge amount of confidential data is being lost every year during transmission by the intruders. Ciphering techniques are widely used to encrypt and decrypt data. But sometimes data encryption does not seem enough and hiding of the data itself is needed more. The technique used for this idea is called Steganography.

Image Steganography is the part of Steganography in which images are used for hiding the secret data. Though Steganography sense like Cryptography but there is some differences between them which split these two terms Cryptography always concern about keeping the content message secret but Steganography is concern about keeping the message secret

The terms which are important in Image Steganography are Image Quality after embedding the secret data and ability of the image to keep maximum confidential data as possible. There are so many algorithms and methods available for Image Steganography which gives the best implementation of Image Steganography. These algorithms have very well embedding capacity with minimum distortion compare to original image.

2. Related Work done

Various algorithms are present for image steganography. Many of the existing schemes has some limitations with respect to some factors. These factors are manipulation of image, embedding capacity, distortion, calculations.

One of the experimental work done Color Image Steganography based on Pixel Value Modification Method Using Modulus Function. In this proposed system introduce approach known as Pixel Value Modification (PVM) using modulus function.

Weiqi Luo, Fangjun Huang, Jiwu Huang have proposed [2] experimental work done Edge Adaptive Steganography Based on LSB Matching.

Thus, in this paper Adaptive Image Steganography Using Pixel Intensity Difference is proposed methodology that is to overcome the limitations of the "Least Significant Bit" Method the new technic for hiding the secret message was proposed known as "Least Significant Bit Matching Revisited". The paper extends the LSB Matching Revisited Scheme and proposes a new idea. It also overcomes the limitations of existing systems.

3. Proposed System Architecture

Proposed method cover image divided into three color planes (Red, Green, Blue), this scheme use modulus by 3 function. After dividing pixel value, we get separate M*N matrix. And pixel embedded into cover image by sequentially manner suppose,

1. 1st red secret pixel embeds into 1st pixel in red of cover image.
2. 1st green secret pixel embeds into 1st pixel in green of cover image.
3. 1st blue secret pixel embeds into 1st pixel in blue of cover image.

The paper extends the LSB Matching Revisited Scheme and proposes a new idea. According to the edge adaptive scheme the selection of the region for hiding secret data is based on following two factors:

1. The size of confidential data.
2. The difference between two successive pixels of the cover image.

Based on the smoother area and edges of the cover image, the sharper edge region is used to hide secret data, when embedding capacity of message is low. When the embedding capacity is get increased then additional region is selected for hiding secret data by adjusting some boundary conditions. According to the pseudorandom number generator some minor changes are done in the LSBMR method, if secret bit is not similar as LSB of the main image then one bit is increased or decreased randomly with respect to pixel value. The normal LSBMR approach deal with a single pixel or pair of pixel without examining the difference between pixels or neighbor pixels

4. Algorithm

1. Select cover image.
2. Scan cover image row by row (Raster scan), Convert cover image into binary format stored into buffer, and calculate pixel intensity difference pixel by pixel.
3. Covert secret data into binary format.
4. If pixel intensity difference is same, no embed secret data into cover image.
5. If pixel intensity difference is different then select low intensity pixel and embed data at LSB-bit, LSB-1 bit. And select contiguous higher intensity pixel embeds data only at LSB bit.
6. If pixel intensity difference is then repeat step 5 until secret data not completely embed.
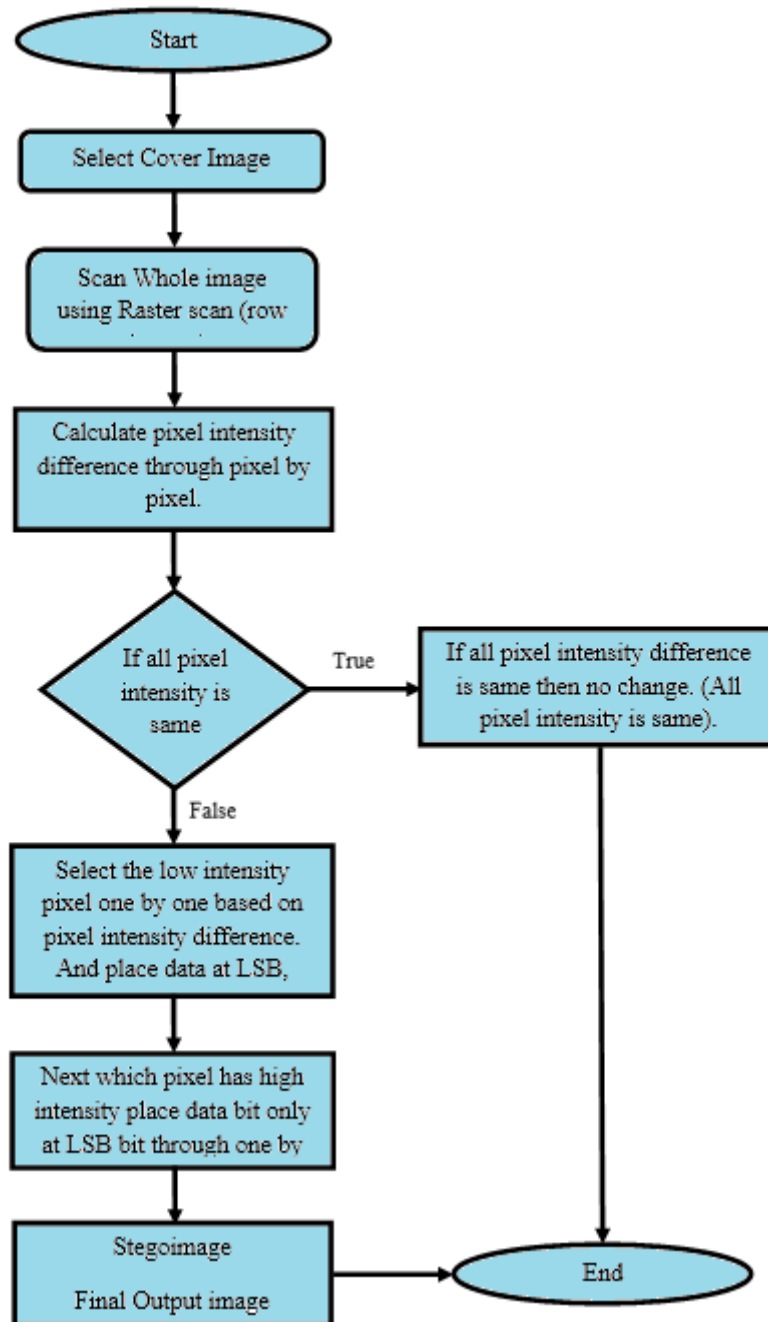
Fig(a): Flowchart of Algorithm

5. Expected Results

The proposed system will have The LSB approach replaces the least significant Bit of the pixel in the cover image. The earlier approaches used to hide the secret message for colored images leads to high noise in the stego-image due to this the secret information is susceptible to be detected. But our proposed method results in better

image quality, secure and reliable as we have sliced the image into three planes i.e. Red, green and blue and then insert the message in each plane on the basis of color sensitivity.

6. Future Scope

As per scenario of our algorithm we can improve the hiding process by applying the cryptographic techniques. There is lot of encryption and decryption techniques that we can apply on the algorithm. We can enhance our embedding capacity as well as security by applying encryption techniques.

Apart from this we can embed secret data into audio as well as video such as multimedia application. Also, the extraction of the image after embedding the data becomes more complicated due to change into the pixel values. So, the exact extraction of secret data should be done this will also come into future work.

7. Conclusion

We have designed a new method which overcomes the limitations of the existing schemes. The proposed scheme on adaptive image steganography provides more embedding capacity as well as less distortion of the image. Though this proposed method has some limitations it gives the expectable PSNR values which show the minimum distortion of image. So, this method is reliable and gives good results in Image Steganography.

8. References

[1] V. Nagaraja, Dr. V. Vijayalakshamib and Dr. G. Zayaraz[1], "Color Image Steganography based on Pixel Value Modification Method Using Modulus Function" IERI Procedia 4 (2013)17-24.

[2] Naddem Akhtar, Shahbaz Khan and PragatiJohri [2], "An Improved Inverted Image Steganography" ICICT 2014.

[3] Weiqi Luo, Fangjun Huang, Jiwu Huang [3] ,"Edge Adaptive Steganography Based on LSB Matching Revisited" IEEE Transactions on Information Forensics and Security Vol. 5,No. 2, JUNE 2010.

[4] R.S.Gutte, Y.D.Chncholkar, R.D. Lahane [4] "Steganography for two and three LSB's using extended substitution algorithm" ICTACT Journal on communication technology, March 2013

[5] Mehdi Hussain, Mureed Hussain, "A Survey of Imag Steganography Techniques", International Journal of Advanced Science and Technology (/JAST), Vo1.54, pp. 113- 123, May 20 13.