THINK INDIA JOURNAL

ISSN: 0971-1260

Vol-22-Issue-17-September-2019

IMAGE STEGANOGRAPHY: A New Approach for Hiding Maximum Data in an Image Based On Block Mapping and Position Sorting

Nitin Kaul
Assistant Professor, School of Electronics and Electrical Engineering,
Lovely Professional university, Punjab

Abstract

Steganography is an art of hiding important information in another information which is not important. This branch of science provides a large scope of information security in terms of data transmission. When the data is being transmitted over the internet, there is always a possibility that it might get stolen, as digital data is hackable. Cryptography has proven very helpful in this context of providing high security. With the help of steganography, security level can be increased. The main concern in steganography is the capacity of a cover data to hide the secret data. The size of secret message image must be smaller than the size of cover image, as higher amount of secret data to be hidden can affect the quality of cover data. In this paper, an algorithm has been proposed to increase the capacity of the cover data to its maximum extent to hide the secret information. The algorithm hides the secret information which has the same size as the cover information. The algorithm has been implemented on images and contains the block mapping of both images (Cover and secret) using histogram equalization, and finding the best suitable area to embed the message.

Keywords: Pixel blocks overlapping, Histogram equalization, Position sorting, Mean Square Error, PSNR, Mean

1 Introduction

Nowadays, the digital communication is leading the communication path. Data transfer over internet, social media, mobile phones, has placed a lot of people under risk of losing their integrity. This makes the situation critical to work on information security more efficiently. Steganography can help in the situation where the data transfer over the digital media is concerned. Rather than sending the data in actual form, it can be concealed in a cover data. In steganography, the strength of algorithm is defined by two things- capacity and detectability. Steganography in images can be implemented in two ways; in spatial domain or in frequency domain. In spatial domain, the embedding of secret information is done directly in the pixels of cover image and in frequency domain image steganography, the cover image is transformed in the frequency domain using various transformation techniques, DCT, wavelet transform etc. and then the embedding is done [6]. Spatial domain provides better capacity and frequency domain provides better robustness [6]. Different strategies can be implemented to increase the security of the Steganographic data like by using cryptographic algorithms for encryption. This paper is concerned with the capacity

ISSN: 0971-1260

Vol-22-Issue-17-September-2019

parameter of the steganography research. The algorithm has used a concept of block mapping of secret and cover image for finding the best embedding position. Section 2 discusses the literature survey. In section 3, proposed methodology has been discussed followed by discussion of experimental result in section 4 and concluded in section 5.

2 RELATED WORK

Some of the research works referred during this research is mentioned in this section.

Cvejic, N and Seppnen, Tapio [1] presented an algorithm for incrementing the hiding potential in audio steganography. The method works in three steps, based on standard Least Significant bit (LSB) embedding, Minimum Error Re- placement (MER) and Error diffusion. The proposed algorithm embeds 4 LSB using standard LSB method, where LSB of host audio sample are replaced by 4 bits of additional information. They used MER to reduce the maximum embed- ding error upto 2k-1, and in order to decrease the perceptual artifact, they have used the error diffusion method. The result gave the close PSNR as compared to the standard LSB embedding method, and increased the capacity by 33%.

Nan-I, Wu and Hwang, Min-Shiang [2] presented a survey paper based on the comparison and analysis of various steganography techniques, their hiding capacity and imperceptibility. The author has showed the comparative analysis of simple LSB method and optimal LSB methods through Peak to Signal Noise Ratio (PSNR), and has shown that optimal LSB method has improved the stego image quality.

Shammim Ahmed Laskar, K. Hemachandran [3] presented an algorithm of steganography combined with cryptography. To increase the security, the author has used, transposition cipher, and for high capacity embedding LSB embedding method is used. In the implementation, author has taken cover image of 35 kb (sample 1), and 4267 bytes were embedded in it.

A. H. Ali, Mohd. R. Mokhtar, L.E. George [4] used fractal coding for enhancing the capacity of the audio for hiding data. Fractal coding is used to find the similarity between the cover and secret blocks in order to encode the secret data into a set of coefficients with minimum size. To increase the security, the author has used chaotic mapping to embed the data in cover data. The result showed that the algorithm achieved the hiding potential upto 80% in certain samples.

After analyzing the data hiding capacity from survey, this research paper got the motivation, as in all the papers, the research shows that the hiding capacity is increasing but not upto 100%. Keeping the two things in mind, capacity and security, this research paper has proposed an approach to increase the capacity by 100%.

3 PROPOSED ALGORITHM

The proposed technique has been implemented for hiding maximum amount of information a cover image can have. If there is a cover image of 100 x 100-pixel size, then by implementing this algorithm a 100 x 100-pixel size message image can be embedded in it. The principle

ISSN: 0971-1260

Vol-22-Issue-17-September-2019

behind this algorithm is that every image has some blocks of pixels which resemble some blocks in another image.

Figure 1: Images of same dimension m*n

In Fig 1, there are two images of same dimension m*n (where m is rows, n is columns) with a lot of similarity. The changes in brightness of both the images are almost same. In other words, the histogram of both the images is almost same. So the information present in the lighter area of one image can be stored in the lighter area of second image, and similarly darker area information can be stored in darker area of other image

3.1 METHODOLOGY

The implementation is done on images and block size of 1 x 8 i.e., a block of 8 pixels is considered. The implementation has been divided in four sections and individual results have been calculated. The results will be discussed in later section. In the algorithm (Fig. 2), secret image will be scanned over the entire cover image to find the better area for embedding process. The methodology used in the algorithm is discussed as follows:

3.1.1 Pre-processing of input

The algorithm required two inputs, cover image and secret image. RGB components of both the images were combined to give gray scale (Y) images given by (eq. 1)

$$Y = 0.299R + 0.587G + 0.114B \quad (1)$$

where R= Red component the input images
G = Green component of the input images
B = Blue component of the input images

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

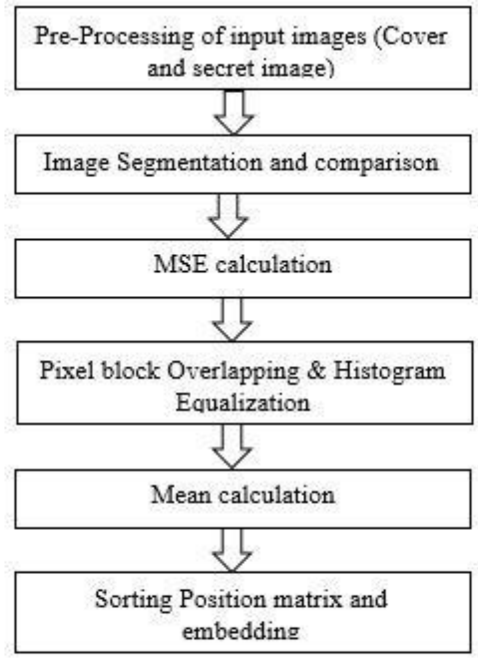

Figure 2: Algorithm of Proposed methodology

3.1.2 Image segmentation

The cover and hiding images were segmented into 1 x 8-pixel block. Every block of secret image was compared with every block of cover image by using Mean Square Error

3.1.3 Mean Square Error calculation

After dividing the images into pixel block, the MSE was calculated between the images given by (eq. 2). MSE is computed by taking the average of the square of intensity of the input cover image and the secret image pixels [5]

$$MSE = (\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2) / (m * n) \qquad (2)$$

The calculation of MSE was done between the first 8-pixel block of secret image and all the 8-pixel blocks of cover image. After comparing all the MSEs, a position matrix (P1) was created for every block of secret image with MSE in ascending order. This process was continued for all the 8-pixel blocks of secret image.

3.1.4 Pixel block Overlapping

Initially when the MSE was calculated between the different blocks, the blocks of cover image were not overlapped. i.e., first MSE was in between 1st 8-pixels of secret image and 1st 8-pixels of cover image, 2nd MSE was in between 1st 8 pixels of secret image and 9-16 pixels of

ISSN: 0971-1260

Vol-22-Issue-17-September-2019

cover image and so on. After getting the result by using that procedure, the blocks were overlapped and again MSE was calculated. The approach improved the result

3.1.5 Histogram equalization:

After implementing the block mapping and comparing images, another parameter was included in the algorithm, Histogram equalization. Histogram equalization is done to match the histograms of two images, which make the 2 images similar to each other to an extent. Histogram is one of the important feature when it is related to image enhancement. Histogram helps in predicting the appearance and intensity characteristics of an image. If the histogram is concentrated on the low side of the intensity scale, the image is mostly a dark image, and if the histogram is concentrated on the high side of the scale, the image is mostly a bright image [8]. Histogram equalization causes the shift in the luminance of the image i.e., it attempts to spread out the intensity level belongs to an image to cover the entire available intensity range [8] [9]. Histogram equalization flattens and stretches the dynamic range of the resultant image histogram and as a result, the enhanced image will optimally utilize the available display levels. This then results an overall contrast improvement [8] [10].

3.1.6 Mean

After the calculation of MSE and histogram equalization, the difference between mean of pixel block of secret image and minimum MSE block was calculated and then the difference was added to the secret image block. After the procedure, embedding was done according to sorted position matrix.

3.1.7 Creating position matrix for data embedding

After calculating and comparing all the MSE's of all the blocks of both the inputs, a new matrix was created having the position, where every individual block of secret image will be embedded. While creating the position matrix (P2), there was a problem of same embedding position for multiple blocks of secret image. This problem was sorted out by comparing the MSEs of different blocks of secret image as (Fig.3). After comparing the MSE, whichever block had the highest MSE of the two, was replaced by the second minimum MSE block position by using the position matrix (P1). The process was continued until all the secret image blocks had unique position to embed.

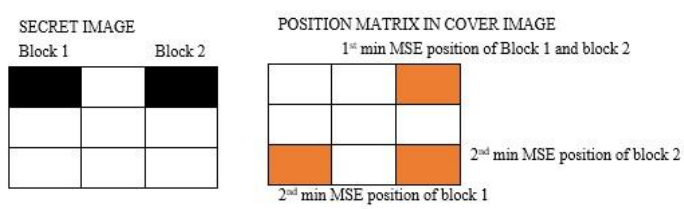

Figure 3: Position Matrix (P2) Sorting

ISSN: 0971-1260

Vol-22-Issue-17-September-2019

4 EXPERIMENTAL RESULT AND DISCUSSION

The implementation is done in MATLAB 2014a. The system configuration is Intel Core i3-5005Y CRP@ 2.00 GHz, 4GB RAM, 64 bit operating system. To check the quality of result, Peak Signal to Noise Ratio (PSNR) [7] was calculated by the function given in (eq.3):

$$PSNR = 10 * \log_{10} ((MaxI^2)/MSE) \quad (3)$$

Where MaxI = maximum possible pixel value of the image. PSNR is a mathematical tool to measure the quality of image based on the differences in pixels of two different images. [5]

For the experimentation, images of same size were considered. The cover images and secret images are given as follows:

Figure 4: Cover images

Figure 5: Secret Images

The result of four experiments are discussed as follows

4.1 Experiment 1

In the first approach, the MSE was calculated in between the first 1 x 8 block of pixels of secret image and every 1 x 8-pixel block of cover image. After finding the block with minimum MSE, that particular block of secret image was embedded in that block of cover image. The process continued for every 1 x 8-pixel block of secret image until entire secret image was embedded in the cover image. Fig 6 shows the stego image after experiment 1. The PSNR (Table 1) of the stego image is as follows:

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

Figure 6: 8-pixel Block Mapping

Image	PSNR(Result1)
Image1	38.7114dB
Image2	33.7625dB
Image3	35.6281dB

Table 1: PSNR of 8-pixel block mapping

4.2 Experiment 2

The procedure of second approach was also same, but in this approach, there was a modification in the process of calculating the minimum MSE by including the overlapping of block of pixels of cover image for MSE calculation. In the previous approach, the MSE of secret image block was calculated with every 8-pixel block of cover image without overlapping, i.e. first MSE was in between 1st 8-pixels of secret image and 1^{st} 8-pixels of cover image, 2nd MSE was in between 1st 8 pixels of secret image and 9-16 pixels of cover image and so on. But in this method, the 1st MSE was calculated between 1^{st} 8-pixels of secret image and 1st 8-pixels of cover image, 2nd MSE was in between 1^{st} 8-pixels of secret image and 2-9 pixels of cover image, and so on. Fig.7 shows the visual quality of stego image got increased by implementing this approach. By calculating MSE in overlapping procedure, PSNR was improved (Table 2), and is given as follows:

Figure 7: Pixel Block Overlapping method

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

Image	PSNR(Result1)
Image1	40.687 dB
Image2	36.9623 dB
Image3	36.0702 dB

Table 2: PSNR of Pixel block overlapping mapping method

4.3 Experiment 3

Figure 8: Histogram Equalization method

Result 3 (Fig. 8) show the improvement in PSNR after including histogram equalization. The MSE calculation was done by using pixel block overlapping method, but before that histogram equalization was implemented on the images to match the images upto the maximum extent. After implementing this process before calculation of MSE, the PSNR of the stego image was further improved and is given as follows:

Image	PSNR(Result1)
Image1	42.2715 dB
Image2	38.1491 dB
Image3	34.8203 dB

Table 3: PSNR of Histogram Equalization method

4.4 Experiment 4

Fig. 9 shows the result of fourth experiment which was calculated by including the mean function in the process. In this approach, the process of former approaches was used for histogram equalization and to find the MSE by using pixel overlapping method. After that the mean function was used to further improve the quality of embedding. The difference between mean of 8-pixel block of secret image and the block where minimum MSE was there for that particular block was calculated and then the difference was added to the block of secret image, and then embedding was done. This function improved the PSNR (Table 4) as described:

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

Figure 9: Histogram equalization and Mean function

Image	PSNR(Result1)
Image1	42.3253 dB
Image2	38.4465 dB
Image3	35.7372 dB

Table 4: PSNR of Histogram Equalization and Mean Function

Table 5 shows the comparison of PSNR of 8-pixel block mapping, Pixel block overlapping mapping method, Histogram equalization method and Histogram Equalization-Mean function method. Table 5 shows the improvement in the quality of image with the implementation of every parameter.

In the experimentation, the embedding capacity was maximum, as the secret images which were hidden were of same size as the cover images. This algorithm has used all the spaces present in an image to hide the secret information.

PSNR	Image 1	Image 2	Image 3
Experiment 1	38.7114 dB	33.7625 dB	35.6281 dB
Experiment 2	40.6873 dB	36. 9623 dB	36.0702 dB
Experiment 3	42. 2715 dB	38.1491 dB	34.8203 dB
Experiment 4	42.3523 dB	38.4465 dB	35.7372 dB

Table 5: Comparison of PSNR of 4 experiments

5 CONCLUSION

ISSN: 0971-1260

Vol-22-Issue-17-September-2019

In this paper, a new approach for hiding the maximum information in the cover image was proposed. The algorithm included four experimentations- pixel block mapping, pixel block overlapping method, histogram equalization and mean function. In the first approach, blocks of 8 pixels of secret image and cover image were mapped and similarity was found by using Mean Square Error. The quality of original image and stego image was found by using PSNR. In the second approach, overlapping of pixel block was done and the quality parameters were calculated. The overlapping increased the PSNR as shown in the results. In the third approach, overlapping method was used but before overlapping the block the histogram equalization of both the images was done. It further improved the PSNR. And finally in the fourth experiment, the Mean difference between the embedding block and the position block where it had to be embedded, was calculated and added in the embedding block, and then the embedding in cover image was done. Results showed that the PSNR improved in all the approaches. The complexity in the approach was the size of cover and secret image. As the size of both the images was same, finding the best suitable area to embed the information was a complex task. But the algorithm sorted out all the unique positions and implemented the embedding.

References

[1] Cvejic, N. and T. Seppanen, 2002. ”Increasing the capacity of LSB-based audio steganography”, Proceedings of the IEEE Workshop on Multimedia Signal Processing, Dec. 9-11, IEEE Xplore Press, pp: 336-338.

[2] Nan-I, Wu and Hwang, Min-Shiang, ”Data Hiding: Current Status and Key Issues”. International Journal of Network Security, Vol.4, No.1, PP.19, January 2007.

[3] Shammim Ahmed Laskar, K. Hemachandran, ”High Capacity data hid- ing using LSB steganography and Encryption”, International Journal of Database Management systems (IJDMS), Vol. 4, No. 6, December 2012.

[4] A. H. Ali, Mohd. R. Mokhtar, L.E. George, ”Enhancing the Hiding Capacity of Audio Steganography Based on Block Mapping”, Journal of Theoretical and Applied Information Technology, Vol. 95, No. 7, April 2017.

[5] Yusra A. Y. al-Najjar, Dr. Der Chen Soong, ”Comparison of Image Quality Assessment: PSNR, HVS, SSIM, UIQI”, International Journal of Scientific and engineering Research, Volume 3, Issue 8, August-2012.

[6] Adel Almohammad, Robert M. Hierons, Gheorghita Ghinea, ”High Capac- ity Steganographic Method Based Upon JPEG”. The Third International Conference on Availablity, Reliability and Security, 2008. ARES08, pp: 544-
549.

[7] A. Soria-Lorente and S. Berres,” A Secure Steganographic Algorithm Based on Frequency Domain for the Transmission of Hidden Information”, Hin- dawi, Security and Communication Networks, Volume 2017, Article ID

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

5397082.

[8] Nicholas Sia Pik Kong, Haidi Ibrahim, and Seng Chun Hoo, ”A Litera- ture Review on Histogram Equalization and its Variations for Digital Image Enhancement”, International Journal of Innovation, Management and Tech- nology, Vo. 4, No. 4 August 2013.

[9] P. C. Cosman, R. M. Gray, and E. A. Riskin, ”Combining vector quantiza- tion and histogram equalization”, in Data Compression Conference, 1991. DCC 91, Snowbird, UT, USA, pp. 113118, 1991

[10] A. Iranli, H. Fatemi, and M. Pedram, ”HEBS: histogram equalization for backlight scaling”, Design, Automation and Test in Europe, 2005, pp. 346351, vol. 1, 2005