INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN: 2278 – 0211 (Online)

Variable Load Image Steganography using Multiple Edge Detection and Minimum Error Replacement Method

Vijay V
MISTE, Assistant Professor, Dept of T.C.E, K.S.I.T
Bhavya R
Assistant Professor, Dept of T.C.E, K.S.I.T

Abstract:

This paper proposes a steganography method using the digital images. Here, we are embedding the data which is to be secured into the digital image. Human Visual System proved that the changes in the image edges are insensitive to human eyes. Therefore we are using edge detection method in steganography to increase data hiding capacity by embedding more data in these edge pixels. So, if we can increase number of edge pixels, we can increase the amount of data that can be hidden in the image. To increase the number of edge pixels, multiple edge detection is employed. Edge detection is carried out using more sophisticated operator like Canny operator. To compensate for the resulting decrease in the PSNR because of increase in the amount of data hidden, Minimum Error Replacement [MER] method is used. Therefore, the main goal of image steganography i.e. security with highest embedding capacity and good visual qualities are achieved. To extract the data we need the original image and the embedding ratio. Extraction is done by taking multiple edges detecting the original image and the data is extracted corresponding to the embedding ratio.

***Keywords**: Security, Cryptography, Multiple Edge Detection, Minimum Error Replacement, Variable Embedding Ratio*

1.Introduction

Present communication system uses digital signals more than analog signals. Digital communication system uses digital signals, which are sent through the communication channel. Communication channels are susceptible for the intrusions. Internet is the major channel for communication and is very much necessary to secure the data transmitted through the internet. Many methods are developed to secure data. Data security is the major area where many developments are required. Cryptography is used extensively to secure the data. Steganography is another method which can be used to secure the data. Cryptography modifies the data with respect to some fixed model, so that the information is scrambled. But in Steganography a cover image is taken and the data is embedded into it in such a way that cover image is least altered. So in Steganography, not only the information is hidden also the existence of the information is hidden. It may be some time is required to hide the presence of secrete data rather than just making the data encrypted. Steganography is hence used to make the data more secure and then its existence is made secrete as well. It's better to use a digital image for Steganography. Digital images can store large amount of data. For example let us take an example of 512×512 grayscale image will have 262,144 pixels and each pixel is made up of 8-bits.So the total numbers of bits in the image is 2,097,152.The total number of LSB bits in the image is 262,144.If we embed only for LSB bits in the image we can still hide 262,144bits of data. This makes digital images suitable for Steganography. Also digital image is a common data which is shared in the internet and that makes image steganography better than any other.

The simplest way for image steganography is LSB substitution method. In LSB substitution method the information which is to be hidden is converted into bit stream. The LSB bits of each pixel of the image is then substituted or replaced by the information bits. Chan C.K and Chen L.M [1] proposed simple LSB substitution method. Simple LSB substitution method is simple but it is not secure. Simply by extracting the LSB bits we can get the information back. Wang R.Z, Lin C.F and Lin J.C [2] proposed moderately significant –bit replacement method. Marghny Mohamed, Fadwa Al-Afari, and Mohammed Bamatraf [3] proposed LSB substitution by genetical-optical key permutation.

Neighbor pixel information method is another way in which the number bits substituted for a given pixel is dependent on its neighbor pixel values. Moazzam Hossain, Sadia Al Haque, Farhana Sharmin [4] proposed steganography method using neighborhood pixel information. But the PSNR is obtained was about 43.144dB.The capacity is less. Edge detection is the method in which more number of bits is embedded into edge pixels and other pixels are normally loaded. LiLi, Bin Luo, Qiang Xiaojun Fang [5] proposed a method using edge detection using sobel operator. Single edge detection yields less number of edge pixels. Hence, Multiple Edge Detection is proposed in this paper.

Along with Multiple Edge Detection, Minimum Error Replacement method is used to increase the PSNR. So data hiding capacity and PSNR both are increased. Extraction is just the reverse of embedding procedure. By this the security is maintained along with achieving more capacity and good visual quality.

2.Proposed Methods

2.1.Multiple Edge Detection

Edge detection is a method used to detect the image edges. Image edge is the area in the image in which the gradient is steeply changing. The gradient in the image can be detected using operators like Sobel operator, Canny operator etc. But Canny operator is more sophisticated than Sobel operator. The gradient value obtained from Sobel operator is raw. Canny operator gives much more efficient gradient value. Reason for this is it uses a filter to reduce the noise level in the image first and finding the gradient value. Filter which is used to smooth the image is Gaussian filter. Gaussian filter is a 2-dimensional convolution filter, whose convolution matrix is as described below.

Gaussian filter,

$$\mathrm{A} = 1/159 \begin{pmatrix} 2 & 4 & 5 & 4 & 2 \\ 4 & 9 & 12 & 9 & 4 \\ 5 & 12 & 15 & 12 & 5 \\ 4 & 9 & 12 & 9 & 4 \\ 2 & 4 & 5 & 4 & 2 \end{pmatrix} * \mathrm{Image} \qquad (1)$$

'A' gives the smoothened image. It's done by 2-dimensional convolution of the image with the matrix. Then the gradient is calculated by 2-dimensional convoluting with the matrix shown below.

$$G_x = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} * A \qquad (2)$$

$$G_y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} * A \qquad (3)$$

'G_x' and 'G_y' are the horizontal and vertical components of the gradient values. The resultant gradient value is given by the vector sum of the two components, as given below,

$$G = G_x + G_y \qquad (4)$$

'G'is the resultant gradient value of the image. This gradient value can be used to find the edges of the image. Edge of the image is nothing but the pixels around which the gradient is varying rapidly. This gradient value is then compared with a threshold value. The threshold value is given by considering the average gradient value. Each pixel value is then compared with this threshold value. The pixels which are less than threshold value is non-edge pixel and the pixels whose value is greater than threshold value is considered as edge pixel.

Multiple edge detection is the method in which the above mentioned steps are repeated more than once. That is the edge detected image is again subjected to edge detection process. Its optimum to use 2-3 times. Multiple edge detection doubles the number of edge pixels in an image. This intern increases the data capacity.

2.2.Variable Embedding

Variable embedding is employed as there are two types of pixels, edge pixels and non-edge pixels. Edge pixels are heavily loaded and non- edge pixels are normal loaded. So this increases the data hiding capacity. Here we come across a factor known as the Variable Embedding Ratio[VER]. This ratio specifies the number of bits embedded in edge and non-edge pixels. It's specified as the ratio like 4:2, 4:1 etc. Variable embedding can also be used to increase the security as well. The receiver should know the Variable Embedding Ratio without which extraction is not possible.

Variable Embedding Ratio has to be used sensibly. According to the information, Variable Embedding Ratio is chosen so as to increase the PSNR. At the same time it can be used to improve security. Only the authorized person who knows the VER can extract the data.

2.3.Minimum Error Replacement Method

Multiple Edge Detection and Multiple Embedding increase the data hiding capacity of the image. For that it compensates the PSNR. As data hiding capacity is important, the

PSNR also important for good Steganography. Hence this paper employs Minimum Error Replacement method to increase the PSNR of the image. In this method the Stego-image is compared with the original image and the difference in the pixel value is calculated. Accordingly in the pixels in which the error vale is high the immediate higher bit of the pixel is changed. This brings down the error range. Hence the overall error reduces which in turn increases the PSNR.

Let for example, the original pixel value of pixel in an image be: 1011 1000

Let the last 3 bits of the pixels are changed. After the embedding of data the pixel value changed to, say:1011 1111

Now the error between these two is ‘7’.This is a large error and this reduces the PSNR significantly.

So, in Minimum Error Replacement Method the next higher bit that is 5^{th} bit is changed.

Thus the new pixel value is: 1011 0111

this reduces the error range to ‘1’, which is negligible. If after changing the next bit, the error rate is more than the previous then retain the previous value which is its least error range.

3.Embedding Procedure

The embedding procedure is very simple. The embedding procedure proposed is for the grayscale images of any size. The embedding procedure is as follows,

- Using (1) the image is smoothened and using (2),(3) and (4) The gradient of the image is determined.
- A threshold value is taken and it is compared with the pixel gradients. If the gradient value is lesser than threshold value, it is not considered as the edge pixel. Other pixels are edge pixels.
- Step 1 and 2 are repeated for 2-3 times. Edge detection carried out 2-3 times, so that the edge pixels are increased.
- Let the number of edge pixels available be ‘x’
- The information to be hidden is converted into bit-stream. First, each character is converted into its ASCII equivalent and then into bits.
- Let the number of bits in this bit-stream be ‘y’.
- The appropriate Variable Embedding Ratio [VER] is selected according to the information bits ‘y’.

- According to the VER, the bits from information bit-stream are embedded to image.

- After embedding each bit the Error is calculated as,
- Error= Original pixel value-New pixel value.
- If this Error is more than 2, Minimum Error Replacement method is applied
- Minimum Error Replacement method is as follows,
  - If the Error is more than 2, the next higher bit in the pixel is complemented.
  - Again the Error is calculated with respect to the original pixel value.
  - If this Error is more than the previous Error, then the complemented bit in the pixel is changed to original bit value.
  - If the Error is less than the new bit value is retained.

- The resulting image is the Stego-image.

4.Extraction Procedure

Extraction of the information from the Stego-image is simple. Extraction process requires the original image and the VER. The original image is subjected to Multiple Edge Detection, as described in the embedding procedure. Then, according to the VER, the bits are retrieved from the Stego-image.

Minimum Error Replacement method will not cause any distortion in retrieval of data. Because the Minimum Error Replacement method deals with the next higher bit. So the information bits are not altered.

5.Experimental Analysis

Experiments are carried out to support our theory and the following results are found. Experiments are done in MATLAB 6.5 version. Experiment is carried out on different grayscale images and a comparative study is presented.

Figure 1: Lena (512×512)

ER	Maximum bits that can be hidden	PSNR in dB
4:0	126616	38.21
4:1	525612	37.11
4:2	600256	36.47

Table 1: Comparison between different VER without MER

5.1.Experiment ON 'Lena'-IMAGE

5.1.1.Without Minimum Error Replacement Method

From Table 1 it can be seen that with the introduction of VER method the PSNR decreases drastically. For just hiding 126616 bits in the image the PSNR reduces to 38.12.

Method	Maximum Hiding Capacity(In Bits)	PSNR(In dB)
Four Neighbors	392208	41.1468
Diagonal Neighbors	395680	40.6505

Table 2: Methods proposed by Moazzom Hosain, Sadia Al Haque and Farhana Sharmin

5.1.2.<u>With Minimum Error Replacement Method</u>

With the addition of Minimum Error Replacement method the PSNR increases drastically. For a data hiding capacity of 126616 the PSNR has increased from 38.21 to 42.1485, and for maximum of 600256 bits PSNR increases from 36.47 to 40.0034 which is a significant increase. Even though the PSNR is high in the Neighbor methods their data hiding capacity is less comparatively.

VER	Maximum bits that can be hidden.	PSNR in dB
4:0	126616	42.1485
4:1	525612	41.5566
4:2	600256	40.0034

Table 3: Comparison between different VER with MER

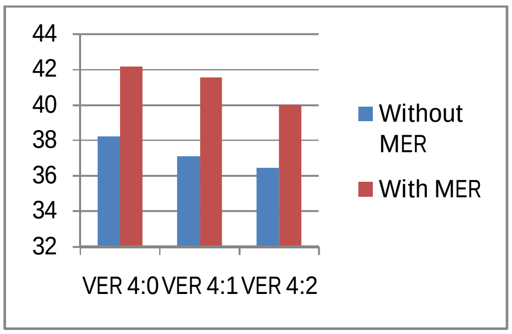

Figure 3

6.Conclusion

In this paper we propose using the method of Minimum Error Replacement method to the method of Multiple Edge Detection and Variable Embedding. Multiple Edge Detection and Variable Embedding increases the maximum data hiding capacity and the minimum error Replacement method compensates for the PSNR reduction caused by them.

7.Reference

1. Chan K. and Cheng M. "Hiding Data in Images using Simple LSB Substitution" Computer Journal of Pattern Recognition Letters, volume 37,No.3, PP . 469-474,2004.
2. Wang R. Z , Lin C. F and Lin J. C "Hiding Data in Images Optimal Moderately Significant –bit replacement", IEE Electron Letter, vol. 36, no. 25, PP. 2069-2070, 2000.
3. Marghny Mohamed, Fadwa Al-Afari, and Mohammed Bamatrf "Data Hiding by LSB substitution using Genetic Optimal Key Permutation", International Arab Journal of e-technology, vol 2, No.1 January 2011.
4. Moazzam Hossain, Sadia Al Haque, Farhana Sharmin. "Variable Rate Steganography in Gray Scale Digital images Using Neighborhood pixel information", The International Arab Journal of information technology, vol. 7, No. 1, January 2010.
5. Li Li, Bin Luo, and Qiang Li Xiaojun Fang., "A color Images steganography method by multiple embedding strategy based on Sobel operator," International conference on multimedia information networking and security, IEEE 2009, 978-0-7695-3843-3/09.
6. Masoud Afrakhteh, Subariah Ibrahim," Steganography Using More Surrounding Pixels", Proceedings of the World Congress on Engineering 2010, Vol I , June 30 - July 2, 2010, London, U.K.
7. H. Yang, Xingming SUN and Guang SUN, "A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution", Radio Engineering, vol. 18, no. 4, Dec. 2009.
8. W. Luo, F. Huang and J. Huang, "Edge Adaptive Image Steganography Based on LSB Matching Revisited", IEEE Transactions on Information Forensics and Security, vol. 5, no. 2, June2010.
9. C.K. Chan and L.M. Cheng, "Hiding data in images by simple LSB substitution ", Pattern Recognition Society, Published by Elsevier Ltd, vol. 37, pp 469 – 474, Aug. 2003.
10. C.F. Lee and H.L Chen, "A novel data hiding scheme based on modulus function," Journal of Systems and Software, vol. 83, no. 1pp.832–843,Dec.2009.

11. J.C. Joo, H.Y. Lee, C. N. Bui, W.Y. Yoo, and H.K. Lee, "Steganalytic measures for the steganography using pixel-value di□erencing and modulus function," in Proceeding s of the 9th Pacific Rim Conference on Multimedia, vol. 5353 of Lecture Notes in Computer Science , pp. 476–485, 2008.
12. F. Huang, B. Li, and J. Huang, "Attack LSB matchingsteganography by counting alteration rate of the numberof neighbourhood gray levels," in Proc. IEEE Int. Conf.Image Processing, Oct. 16–19, 2007, vol. 1, pp.401–404.