International Journal of Engineering Research and Development
e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 10, Issue 4 (April 2014), PP.68-73

A Robust Image Steganography using Multiple Edge Detection and Advanced Error Replacement Method

Geetha C.R.[1], Dr.Puttamadappa C.[2]
[1]*Research Scholar, Jain University, Bangalore, Karnataka, INDIA*
[2]*Professor and Principal Sapthagiri College of Engineering Bangalore, Karnataka, INDIA*

Abstract:- This paper proposes a Steganography method using the digital images. The art of embedding the data which is to be secured into the digital image is called as Image Steganography. 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, Advanced Error Replacement [AER] method is proposed here. Because we are changing bits other than the one in which the data is hidden, by employing AER Technique, the proposed encryption algorithm is immune to many of the standard Stego Analysis Procedure. Therefore, the proposed image Steganography method improves the PSNR and ensures high security without comprising the Data hiding capacity and visual qualities of the Cover image. 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, this ratio again forms a secret which will be known only to the receiver.

Keywords:- Security, Cryptography, Multiple edge detection, Minimum error replacement, Variable embedding ratio.

I. 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 gray scale 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 method for secure communication.

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.

II. PROPOSED METHODS

A. 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 smoothen the image is Gaussian filter. Gaussian filter is a 2-dimensional convolution filter, whose convolution matrix is as described below.

Gaussian filter,

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

A gives the smoothened image. It is 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. It is optimum to use 2-3 times. Multiple edge detection doubles the number of edge pixels in an image. This intern increases the data capacity.

B. 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.

C. Advanced 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 Advanced Error Replacement method to increase the PSNR of the image. This error replacement method can be used in all the cases to reduce the error if the error exceeds the Threshold value. The range of error after embedding k bits using LSB substitution method is

$-(2^k-1) <= \text{Error} <= (2^k-1)$ this error range is brought down to

$-(2^{k-1}) <= \text{newError} <= (2^{k-1})$ using AER method.

Where, Error is the difference between the cover pixel(X_cov) and the stego pixel(X_stg) and newError is the difference between the cover pixel(X_cov) and the new stego pixel(Y) formed after applying AER

The error exceeds the threshold, then in order to limit the error the original pixel value is added or subtracted suitably with modifing factor „x" , which is generated as follows,

$M = (2^k \% \text{Error})$, where % is the modulus operator. New stego pixel value,

New stego pixel value,

$$Y = \begin{cases} X\_cov + M, & \text{for, } X\_cov > X\_stg \\ X\_cov - M, & \text{otherwise} \end{cases}$$

The error between the New stego pixel (Y) and the original cover pixel (X_cov) now will be within the limits of newError as shown above.

Let us take this example to understand the proposed AER technique. The cover image pixel value that is the original pixel value is 10000000 and the data to be embedded is 1111. So we are supposed to replace the 4(k) LSB of the original image with the data,

Cover pixel value X_cov : 10000000
Data to hide : 1111
Stego pixel value X_stg :10001111 Here the difference in the cover and the stego pixel value is (10001111 – 10000000 = 1111) 15.

Application of AER method for the example,

1. Threshold T for 4 LSB substitution is $T = 2^{k-1} = 2^3 = 8$.
2. Error generated in the example is more than T (15 > 8).
3. Then $x = (2^k \% \text{Error}) = (2^4 \% 15) = 1$.
4. Since (X_cov < X_steg) = (10000000 < 10001111) we have

New Stego pixel Y = X_cov – M = 10000000 – 1 = 01111111.
It can be seen that the data to be hidden that is 1111 is still in the 4 LSB of the New Stego pixel Y and the error now is X_cov – Y = 10000000 - 01111111 = 1.

Therefore the error is brought down to 1 from 15 using AER technique.

III. 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:

1) Using (1) the image is smoothened and using (2), (3) and (4) the gradient of the image is determined.
2) 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.
3) 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"
4) 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".
5) The appropriate Variable Embedding Ratio [VER] is selected according to the information bits „y".
6) According to the VER, the bits from information bit-stream are embedded to image.
7) After embedding each bit the Error is calculated as, Error= Original pixel value-New pixel value.
8) If this Error is more than Threshold, Advanced Error Replacement method is applied.
9) The resulting image is the Stego-image.

Here the difference in the cover and the stego pixel value is (10001111 – 10000000 = 1111) 15.
Application of AER method for the example,

1. Threshold T for 4 LSB substitution is $T = 2^{k-1} = 2^3 = 8$.
2. Error generated in the example is more than T (15 > 8).

3. Then $x = (2^k \% \text{ Error}) = (2^4 \% 15) = 1$.
4. Since (X_cov < X_steg) = (10000000 < 10001111) we have

New Stego pixel Y = X_cov – M = 10000000 – 1 = 01111111.

It can be seen that the data to be hidden that is 1111 is still in the 4 LSB of the New Stego pixel Y and the error now is X_cov – Y = 10000000 - 01111111 = 1.

Therefore the error is brought down to 1 from 15 using AER technique.

III. 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,

1) Using (1) the image is smoothened and using (2),(3) and (4) The gradient of the image is determined.
2) 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.
3) 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"
4) 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".
5) The appropriate Variable Embedding Ratio [VER] is selected according to the information bits „y".
6) According to the VER, the bits from information bit-stream are embedded to image.
7) After embedding each bit the Error is calculated as, Error= Original pixel value-New pixel value.
8) If this Error is more than Threshold, Advanced Error Replacement method is applied.
9) The resulting image is the Stego-image.

IV. EXTRACTION PROCEDURE

Extraction of the information from the Stego-image is the inverse operation of the Embedding Algorithm. Extraction process requires the original image and the VER key. 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.

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

V. EXPERIMENTAL ANALYSIS

Experiments are carried out to support our theory and the following results are found. Experiments are done in MATLAB R2011a version. Experiment is carried out on different grayscale images and a comparative study is presented.

Figure 2. Edge detected image operator

Figure 1.Cover Image using canny

Figure 3. Stego image for 1bpp of data

Figure 4.Stego image for 2bpp of data

The cover image taken is the Standard 512*512 Lena image , which is the figure 1. The image is subjected to multiple edge detection to determine the edges and data is hidden by choosing a required VER ratio. Figure3 and figure 4 are the resulting Stego images for data capacity of 1bpp and 2bpp respectively for an embedding ratio of 4:2. It can be visually analyzed that the visual quality of the image is retained due to the application of the proposed method.

The table below shows the results obtained by various authors of the same image Lena.

From the above table it is clear that the results obtained is much more than that in the standard methods. Further the same method is extended for various images the result obtained are again more as proposed by the paper.

Method	Data hidden in bits	PSNR
4- Neighbor	**392208**	**41.14**
Diagonal Neighbor	**395680**	**40.65**
PVD	**407680**	**41.79**
Proposed	**262144**	**46.34**
	524288	**43.56**

VI. CONCLUSIONS

This paper proposed a Robust Image Steganography method using advanced method of Error replacement and Multiple Embedding, which improves the PSNR and the data hiding capacity without comprising the visual quality of the image. Further the security of the proposed method is very high as the majority of the Stego analysis method fails in retrieving the hidden message as variable embedding is made use, since the application of AER changes the higher order MSB bits the position of data that is hidden cannot be known which further increases the robustness of the method along with reduction in error.

REFERENCES

[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] Andrew D Ker., "Steganalysis of LSB Matching in Gray scale Images", IEEE signal Processing letters, volume 12, NO 6, June 2005.

[7] PRSS Venkatapathi Raju, Y Vamsidhar, Ravi Chandra Sriram, "Edge Adaptive Image Steganography on LSB using Godel numbering," IJCST volume 2,SP1, December 2011,ISSN 0976-8491.

[8] R. Amirtharanjan, R Akila, P Deepikachowdavarapu, "A Comparative Analysis of Image Steganography, " International Journal of Computer Application, 0975-8887 volume-2-no 3, May 2010.

[9] Chen, W. Y., "Color image steganography scheme using set partitioning in hierarchical trees coding, digital Fouriertransform and adaptive phase modulation," Applied Mathematics and computation, 2007, vol.185, pp.432-44.