International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 4 Issue 5, May-2015, pp: (18-23), Impact Factor: 1.252, Available online at: www.erpublications.com

A High Capacity Data Hiding Approach for Color Images

Silky Arora
Dept. of Electronics & Communication Engg.
SBIET, Pundri, Haryana, India

Abstract: Steganography is the art and science of hiding secret data information in other media like digital images. The secret message is hidden in such a way that no one can apart from the sender or the intended recipient view the information. Therefore, different techniques have been proposed so far for. This paper introduces a hybrid approach of data hiding for color images based on 3 LSB technique and edge detection. In the presented algorithm, to preserve the quality of the stego image it is preferred to hide the data at the edges because by doing so the visual quality of the image is affected less as compared to the other areas in the image. The present algorithm offers high steganographic quality in terms of PSNR and provides high embedding capacity without compromising with the quality. The experimental results show that the proposed scheme not only achieves high embedding capacity but also enhances the quality of the stego image. Also steganalysis cannot be done easily as visual quality is good and hence the algorithm is more secure for secure data transmission.

Keywords: Steganography, Least Significant Bit (LSB), Embedding, Peak Signal-to-Noise Ratio (PSNR), Edge detection.

1. Introduction

Today is the age of science and technology where nothing is considered impossible and everything is vulnerable to attacks. So a numbers of secret communication techniques are used to communicate confidential information. Steganography is one of technique which is used to transmit a secret message under the cover of digital media such as images. Steganography derived from two Greek words [13] i.e. 'Steganos' and 'Graphie' where Steganos means covered and Graphie means writing. On the whole Greek translation of the term is concealed writing [9]. Steganography aims to hide the existence of message by embedding secret message to be communicated in any cover message which can be text, audio, video or image. For image steganography, cover message can be any randomly chosen image.

Out of the five pillars of information assurance, namely confidentiality, authentication, identification, integrity and non-repudiation, steganography offers confidentiality by ensuring the privacy of sensitive information. Authentication and identification is only offered if keys are used. However, integrity of information can never be offered by standalone steganography. Non-repudiation is also not possible, because the person can later deny embedding the message as there is no proof of ownership is provided during steganography [8]. The general model of steganography is shown in Fig.1.In this process secret message is embedded into cover file using steganographic algorithm to form stego-file. Then stego-file is communicated over any channel and then receiver extracts message from stego-file using extraction algorithm which is reverse of the steganographic algorithm. Secret key is optional. If it is used during embedding, it is necessary to provide secret key during extraction [11].

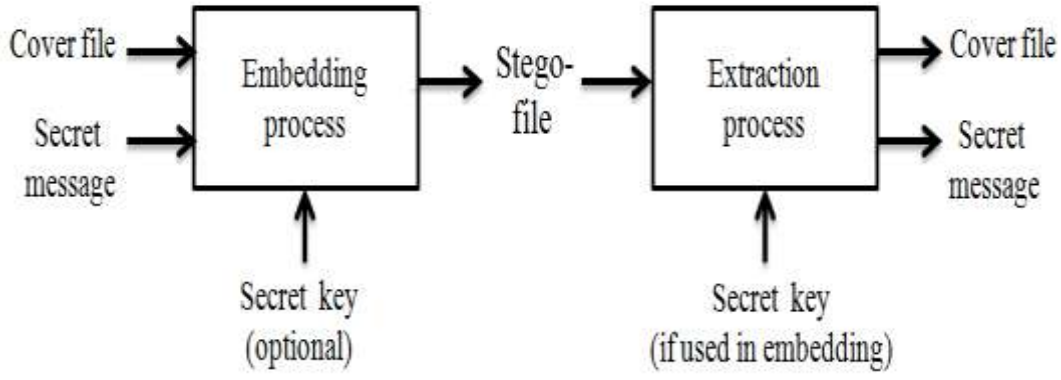

Fig. 1: General model of steganography

LSB (Least Significant Bit) is the traditional approach of steganography which acts as the base for many other techniques. In this technique, message bits are directly hidden into the LSB's of every pixel. It does not affect the visual quality of image, because human eyes are insensitive to gradual changes in shade [7]. There are many extensions introduced for this approach that focus on improving the quality and increasing the steganographic capacity. Few of these techniques are discussed in the following section.

The rest of the paper is organized as follows: In Section II related work is presented. The implementation of the system and proposed algorithm is discussed in section III. Discussion of various results obtained from testing the system based on the proposed algorithm, with various sizes of data is explained in section IV and section V we conclude the paper along with future scope.

2. Related Work

S. Arora et al [1] in this paper, author proposed a technique that hide the text data into the color images using edge detection method. The alteration in edges cannot be distinguished well so edges can hide more data without losing quality of an image. In this technique, Edges of an image are detected by scanning using 3x3 window and then text message is concealed in edges using first component alteration technique.

In 2014 **K.N. Chaturvedi et al [14]** presented a two layer architecture for data hiding for more security of data. The first layer is called cryptography, which secured against cryptanalysis and second layer is steganography that prevents, as much as possible, against any suspicion of the hidden text. In this approach, firstly, it is required to extract all the three-color components of a digital image then to find the edges of each component. Since intensity values of edge pixels differ abruptly in comparison to nearest neighbor pixels, it will not arouse suspicion if the intensity values of these pixels are changed. Thus, embedding of the higher-order bits in the edge pixels is possible as compared to the lower-order bits in the non-edge pixels. Thus finally this work is more contributive towards the goal of increasing the embedding rate and strength against steganalysis attack in the edge based steganography.

S. Kaur et al [3] in this paper, image steganography technique based on first component alteration technique using hybrid edge detector is proposed. There are lots of algorithms to hide data but they are also decreasing the quality of the image. In this work, edges of an RGB image has been detected by hybrid edge detector which is the combination of 3x3 matrix scanning and sobel edge detector, and then text will be embedded in to the first component of edges of the color image.

W.J. Chenet al [4] in this paper, author used least significant bit (LSB) substitution mechanism, based steganographic technique for embedding a secret message in an image with high capacity, while the human visual system (HVS) would be unable to notice the hidden message in the cover image. In this paper, besides employing the LSB substitution technique as a fundamental stage, advantage of edge detection technique is utilized.

V.S. Jain et al [5] in this paper, author proposed a new steganographic algorithm that is used to hide text file inside an image. In order to increase/ maximize the storage capacity a compression algorithm that compresses the data to be embedded. The compression algorithm we have used works in a range of 1bit to 8 bits per pixel ratio.

3. Present Work

In present work, a Block based Steganography Technique is proposed which hides the message bits at the edges of the cover image. The presented algorithm can be applied to the RGB images and does not hide the data to the gray scale images. In the proposed algorithm, to preserve the quality of the stego image it is preferred to hide the data at the edges because by doing so the visual quality of the image is affected less as compared to the other areas in the image. And to make the algorithm high data capacity embedding system, the edge pixels from every layer are calculated using canny edge detector. Then the whole image is divided into the blocks of 4 pixels. The last 3 pixels of each block are used to hide the secret data. All these 3 pixels are analyzed for its status as edge or non edge pixel and if pixel is found edge pixel then 3 bits of data is replaced with the 3 LSBs of the blue layer of that pixel. But if the pixel is found non edge then 3 bits of data is scattered into 3 layers of that pixel by replacing the one bit of data with the 1 LSB of each layer. And also 1^{st} pixel of every block is used to hide the status of the rest 3 pixels in the group. If the pixel is edge pixel then store its status as 1 into the 1^{st} pixel and if the pixel is non edge then store its status as 0 into the 1^{st} pixel. After hiding the whole data into the image blocks stego blocks are re arranged and stego image is obtained. The block diagram showing the basic layout of present approach of message hiding is shown in figure 2.

To retrieve the hidden message from the stego image the stego image is divided into blocks of 4 pixels and from the 1^{st} pixel of every block the status of the rest 3 pixels in the group is retrieved as edge or non edge. out the rest 3 pixels in the group, if the pixel is found edge pixel then retrieve the 3 bits from the blue layer of this pixel otherwise retrieve one bit from every layer of the pixel. After retrieving these data bits from whole blocks arrange them in a proper manner to retrieve the hidden message. The block diagram for retrieval of message from stego image is shown in figure 3.

Message Hiding Algorithm

1. Read RGB image.
2. Divide the image into blocks of four pixels.
3. Read the status of last three pixels of the group as edge and non edge pixel.
4. Hide their status in first pixel of the group.Hide 1 for edge pixel and 0 for non edge pixel.
5. If pixel is edge pixel then hide 3 bits of secret message into three bits of blue component.
6. Hide one bit at LSB of each layer if pixel is non edge.

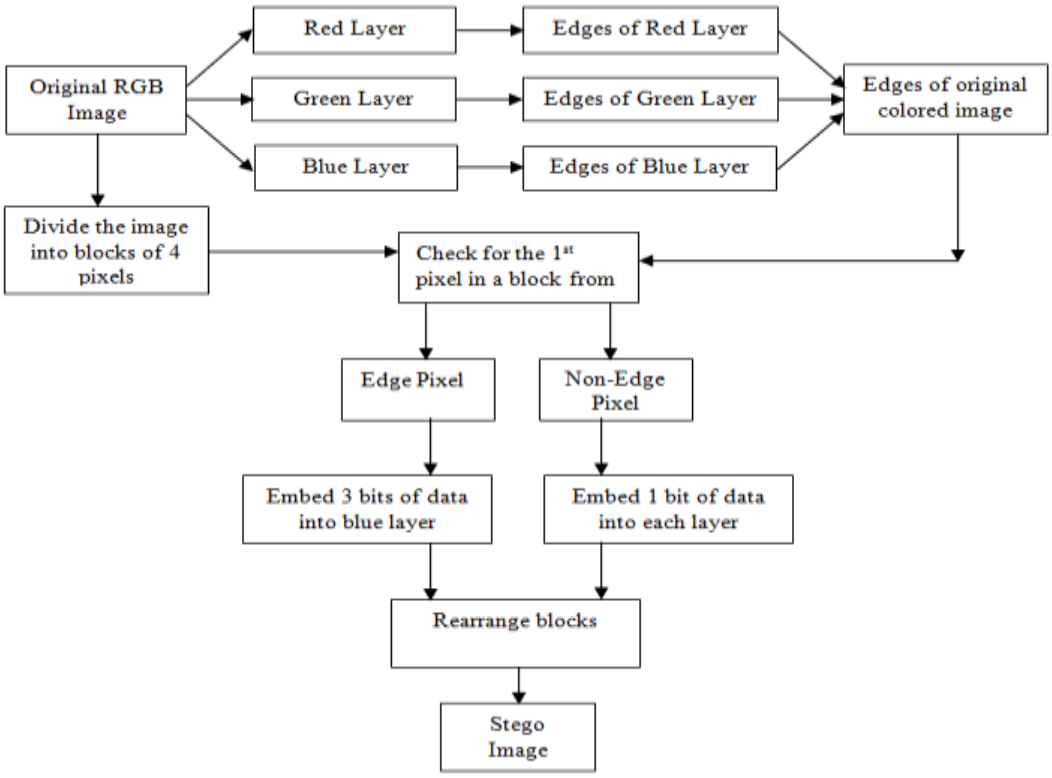

Fig: - 2 Message hiding process

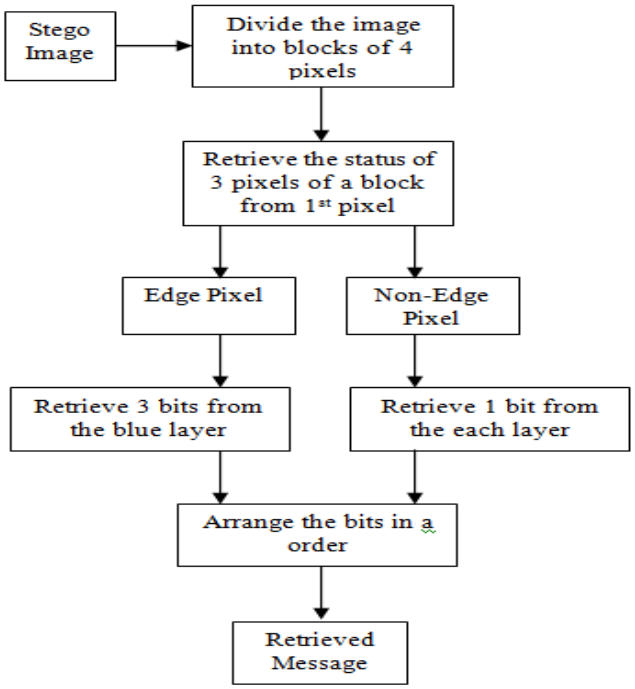

Fig: - 3 Message retrieval process

Message Retrieval Algorithm

1. Read the Image
2. Divide the Image into blocks of four pixels.
3. Read the first pixel of the group and check the status of each pixel.
4. Retrieve three bits from blue component of pixel if it is found edge pixel.
5. Otherwise retrieve one bit from each component of the pixel if it is found non edge pixel.

4. Experimental Results

Experimental results using the proposed method are presented in this section. The whole work is executed in MATLAB tool. To test the algorithm, images of different sizes are used to check the performance. Moreover, to check the steganographic quality, MSE and PSNR are calculated using equation1 and 2. For this purpose different message of different length of characters is embedded in each image as follows:

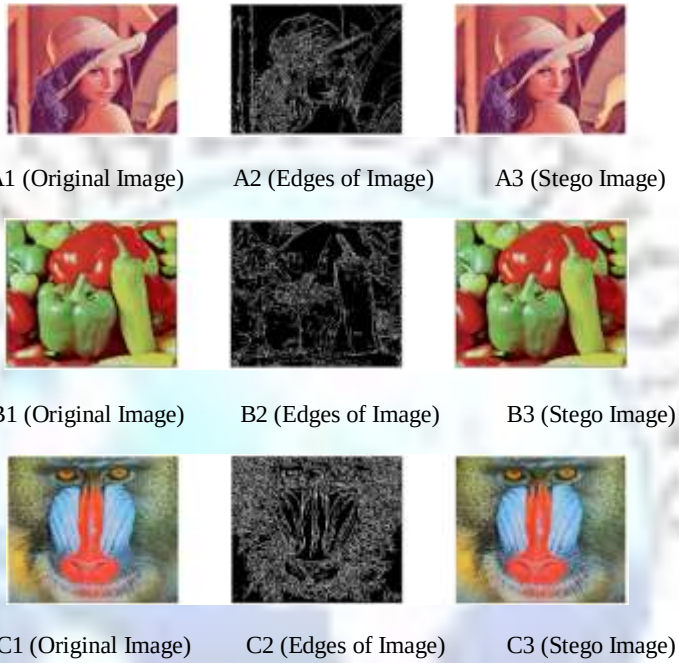

Fig. 3: Message hiding process (Data Length: 792 Bytes)

Results for proposed method are shown in table 1.

Table:-1 Proposed method results

Image	Data Length (in bytes)	MSE	PSNR
Lena (512 X 512 X 3)	792	0.0006	79.812
	1702	0.0016	76.181
	2547	0.0031	73.164
Pepper (512 X 512 X 3)	792	0.0015	76.388
	1702	0.0034	72.806
	2547	0.0045	71.567
Baboon (331 X 345 X 3)	792	0.0053	70.870
	1702	0.0135	66.838
	2547	0.0197	65.196

Data Payload for proposed Algorithm:

Data capacity of the presented technique for an image of size 512 X 512 can be 72KB as 65,536 blocks can be made from this whole image. And this much capacity can be achieved by hiding 9 bits per block.

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left[I(i,j) - K(i,j)\right]^2 \quad (1)$$

$$PSNR = 10.Log_{10}\left(\frac{MAX^2}{MSE}\right) \quad (2)$$

Table 2: Comparisons between proposed method and previous work

Image	Data Length (in bytes)	Previous Work [3]		Proposed method	
		MSE	PSNR	MSE	PSNR
Lena (512 X 512 X 3)	792	1.9044	45.3672	0.0006	79.812
	1702	4.4395	41.6915	0.0016	76.181
	2547	6.4501	40.0692	0.0031	73.164
Pepper (512 X 512 X 3)	792	3.7463	42.4288	0.0015	76.388
	1702	8.0184	39.1239	0.0034	72.806
	2547	12.4848	37.2010	0.0045	71.567
Baboon (331 X 345 X 3)	792	3.3397	42.9277	0.0053	70.870
	1702	6.7508	39.8712	0.0135	66.838
	2547	9.4621	38.4049	0.0197	65.196

5. Conclusion

This paper introduced a Block based Steganography Technique which hides the message bits at the edges of the cover image is implemented and analyzed for color images. We have performed test on standard images with different sizes of message data to be hidden. To make the algorithm high data capacity embedding system, the edge pixels from every layer are calculated using canny edge detector. In this technique the image is divided into a block of four pixels, the 1st pixel store the status of the other three pixels and remaining three pixels store the information bits. In the proposed algorithm, to preserve the quality of the stego image it is preferred to hide the data at the edges because by doing so the visual quality of the image is affected less as compared to the other areas in the image. Along with this high steganographic capacity, it offers very good quality in terms of PSNR. The results of proposed method and First Component Alteration Technique are compared in the Table 2.The proposed method results show that the proposed scheme not only achieves high embedding capacity but also enhances the quality of the stego-image from the HVS by an edge detection technique.

References

[1]. S. Arora, S. Anand, "A Proposed Method for Image Steganography Using Edge Detection," International Journal of Emerging Technology and Advanced Engineering, Vol. 3, Issue 2, pp. 296-297, Feb. 2013.
[2]. N. Jain, S. Meshram, S. Dubey, "Image Steganography Using LSB and Edge-Detection Technique," International Journal of Soft Computing and Engineering (IJSCE), Vol. 2, Issue-3, pp. 217-222, Jul. 2012.
[3]. S. Kaur, S. Jindal, " Image Steganography using Hybrid Edge Detection and First Component Alteration Technique," International Journal of Hybrid Information Technology, vol. 6, No. 5, pp. 59-66, 2013.
[4]. W.J. Chen, C.C. Chang, T.H.N. Le, "High payload steganography mechanism using hybrid edge detector," Expert Systems with Applications 37, pp.3292–3301, 2010.
[5]. V. Sharma, S. Kumar, "A New Approach to Hide Text in Images Using Steganography", IJARCSSE, Volume3, Issue 4, ISSN: 2277 128X, April 2013.
[6]. Ross J. Anderson, Fabien A.P. Petitcolas, "On the Limits of Steganography", IEEE Journal of Selected Areas in Communications, 16(4):474-481, ISSN 0733-8716, May 1998.
[7]. S.F. Mare, M. Vladutiu, L. Prodan, "Decreasing change impact using smart LSB pixel mapping and data rearrangement", IEEE, 2011.

[8]. Tayana Morkel, "Image Steganography Applications for Secure Communication", Universities van Pretoria, May 2012.
[9]. N. Provos, P. Honeyman, “Hide and seek: an introduction to steganography”, IEEE Security and Privacy Magazine 1 (2003).
[10]. Ronak Doshi, Pratik Jain, Lalit Gupta," Steganography and Its Applications in Security ", International Journal of Modern Engineering Research (IJMER) Vol.2, ISSN: 2249-6645, Issue.6, Nov-Dec. 2012.
[11]. Shashikala Channalli, Ajay Jadhav,"Steganography: An Art of Hiding Data", International Journal on Computer Science and Engineering, Vol.1 (3), pp. 137-141, 2009.
[12]. Atallah M. Al-Shatnawi, "A New Method in Image Steganography with Improved Image Quality", Applied Mathematical Sciences, Vol. 6, 2012.
[13]. Krishna Nand Chaturvedi, Amit Deogar, “A Noval Approach for Data Hiding using LSB on Edges of a Gray Scale Cover Images”, International Journal of Computer Applications, Vol. 86, pp. 36-40, 2014.