International Journal of Electronics and
Communication Engineering (IJECE)
ISSN(P): 2278-9901; ISSN(E): 2278-991X
Vol. 4, Issue 1, Jan 2015, 29-36
© IASET

International Academy of Science,
Engineering and Technology
Connecting Researchers; Nurturing Innovations

BLOCK-LEVEL SECURE STEGANOGRAPHY SCHEME USING HIGH FREQUENCY COORDINATES

POONAM, KIRAN JOT SINGH & DIVNEET SINGH KAPOOR

Department of Electronics & Communication Engineering, Chandigarh University, Punjab, India

ABSTRACT

A technique for information security has been proposed in this paper. Steganography is a technique which hides data in digital mediaso as not to stimulate an eavesdropper doubt. Digital media includes image, audio, video etc. An important thing to notice about this technique is that, it does not let any third party to know that any data is hidden. Only the sender and intended recipient could view the information. In this paper, Bit Insertion Technique is used to hide data that is to be sent. Data is being hidden in high frequency areas as well as in non-edge areas. Reason of hiding data in edges is that any alterations made in edge areas of an image are invisible to naked human eye. Presented algorithm preserves the quality of image after hiding data in terms of PSNR. Experimental results show that proposed methodcaters both high embedding capacity and preserves the visual quality of the stego image.

KEYWORDS: Steganography, Least Significant Bit (LSB), Bit Level Block (BLB), Embedding, Peak Signal-to-Noise Ratio (PSNR), Human Visual System (HVS), Edges

1. INTRODUCTION

Security of information is the factor which is needed so badly today. Which is why, various techniques of data security have been employed so far. Steganography is one of them. It is used to transmit a secret message under the cover of digital media such as images. Main objective of the technique is to avoid being detected that any conversation is even taking place. Steganography is derived from two Greekwords [1] i.e. 'Steganos' and 'Graphie' where Steganos means covered and Graphie means writing. On the whole, Greek translation of the term is concealed writing.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 [2]. Steganography Algorithm presented in this paper fulfils all important requirements. These are: Imperceptibility, Irrecoverability, Data payload and good Visual quality. These could be explained as follows:

- **Imperceptibility**: It refers to the ability of Steganography algorithm to hide data in an undetectable way so that no one can see any visible distortions in carrier file.
- **Irrecoverability:** It refers to how hard it is for someone apart from sender and intended recipient to detect and recover secret data out of cover file.

- **Data or capacity:** Determines the number of bytes that can be covered within the carrier file without distorting it.

Terminologies Used In Steganography

- **Cover Message:** It is the carrier of message, image audio or video
- **Secret Message**: It is the information needed to be hidden. It could be anything that can be decoded in binary.
- **Secret key**: It is used as a password and is optional.
- **Embedding Algorithm**: It is an idea to embed secret information in cover image.
- **Extraction Algorithm**: An idea to retrieve secret detail from Stego image is referred to as extraction algorithm.

The general model of steganography is shown in Figure 1. In this process, secret message is embedded into cover file using steganography 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 steganography algorithm. Secret key is optional. If it is used during embedding, it is necessary to provide secret key during extraction [3].

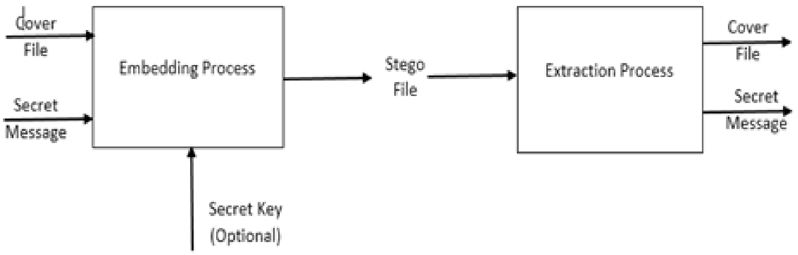

Figure 1: General Model of Steganography

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 [4]. There are many extensions introduced for this approach that focus on improving the quality and increasing the steganographycapacity. Few of these techniques are discussed in the following section. Steganography is not a new field. It is been used through centuries. Invisible inks, wax covered tablets were used for the purpose of hiding secret information in history. But now the world has turned digital, so the signals used today are video, audio and images. There are various methods for hiding data digitally in images. But least significant Insertion method is the simplest one. It would be more advantageous if edge detection method and LSB substitution are used together. Same is done by author in [5]. Reason behind finding edges is that, any alteration made in edges of an image is almost invisible to naked human eye. Author has used hybrid edge detector so as to find maximum number of edges. This detector is a combination of canny edge detector and fuzzy edge detector. Visual quality is maintained and data capacity is also increased as a result. Authors in [6] have proposed a technique for color images which utilised edge detection using Sobel operator. Multiple Time Embedding scheme is utilised which helped obtaining higher embedding capability. PSNR of about 45db is obtained. Weiqi Luo, Fang Jun Huang, Jiwk Huang in [7] have discussed a technique utilising multiple edge detection and variable implanting. This scheme chooses embedding areas on the bases of hidden text size and also on difference between two pixels which are consecutive. Comparison is done between proposed scheme and previous schemes, which shows that proposed scheme gives much better security. Coloured images are three layer images and could hide more amount of data in comparison with grey scale images. Taking this into account, a color image Steganography scheme with hybrid edge detector is used by author in [8]. Results obtained are better when compared with other Steganography schemes. Organisation of rest of the paper is as follows: Section II presents proposed algorithm with embedding and extraction procedure. Section III contains the results obtained after applying the steganography algorithm with different sizes of data. Section IV in the end concludes the paper along with future scope.

2. PROPOSED WORK

In proposed work, a Block based Steganography Technique is proposed which hides the message bits at the edges as well as at edges of cover image. The presented algorithm can be applied to the RGB images and does not hide the data to the greyscale 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 analysed 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 1st 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 its status is stored as 1 into the 1st pixel and if the pixel is non- edge then 0 is stored into the 1st pixel as status. Stego image is obtained after hiding whole data. 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 1st pixel of every block the status of the rest 3 pixels in the group is retrieved as edge or non-edge. Out of 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. Hidden message is retrieved after retrieving whole data. The block diagram for retrieval of message from Stego image is shown in figure 3.

Message Hiding Algorithm

Steps:

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

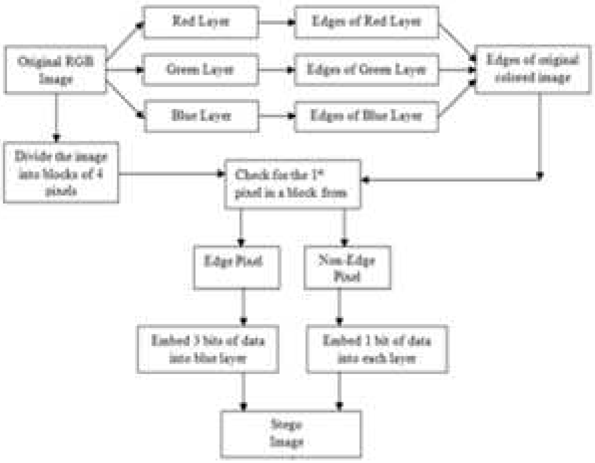
Original RGB Image
Red Layer
Green Layer
Blue Layer
Edges of Red Layer
Edges of Green Layer
Edges of Blue Layer
Edges of original colored image
Divide the image into blocks of 4 pixels
Check for the 1st pixel in a block from
Edge Pixel
Non-Edge Pixel
Embed 3 bits of data into blue layer
Embed 1 bit of data into each layer
Stego Image

Figure 2: Message Hiding Process

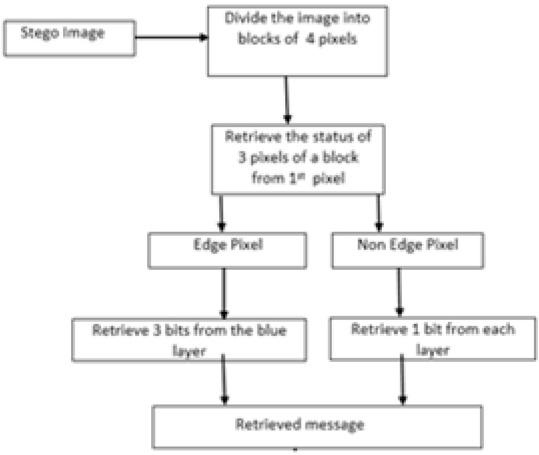
Stego Image
Divide the image into blocks of 4 pixels
Retrieve the status of 3 pixels of a block from 1st pixel
Edge Pixel
Non Edge Pixel
Retrieve 3 bits from the blue layer
Retrieve 1 bit from each layer
Retrieved message

Figure 3: Message Retrieval Process

Comparison with Previous Work

Comparison with First Component Alteration Technique

Message Retrieval Algorithm

Steps

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

3. RESULTS

Experimental results using the proposed method are presented in this section. To test the system, images of different sizes to calculate the steganography capacity and performance are given. Moreover, to check the steganography quality, MSE and PSNR are calculated. For this purpose different messages of different length of characters is embedded.

Steganography capacity is calculated using the following formula

Max msg length= (No. of rows * No. of columns)/4

For example, we have an image of size 512 X 512 then the msg length can be calculated as:

Max msg length = (512*512)/4 =65536Capacity= Max msg length* no of bits hide in a block

Capacity=65536*9= 589824bits or 72 kb

Presented steganography algorithm embeds 3 bits in one pixel i.e. one character can be stored per 3 pixels because each character consists of 8 bits. Two important performance metrics are Peak Signal to Noise Ratio and Mean squared Error [9].

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

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

Table 1: Comparisons between Proposed Method and Previous Work

Image	Data Length (in Bytes)	S. Kaur et al [8]		Proposed Method	
		MSE	PSNR	MSE	PSNR
Owl (512 X 512 X 3)	792	1.9044	45.3672	0.0006	79.753
	1702	4.4395	41.6915	0.0012	77.255
	2547	6.4501	40.0692	0.0028	73.602
Plane (512 X 512 X 3)	792	3.7463	42.4288	0.0015	83.704
	1702	8.0184	39.1239	0.0034	80.799
	2547	12.4848	37.2010	0.0021	74.816
Giraffe (331 X 345 X 3)	792	3.3397	42.9277	0.0053	84.094
	1702	6.7508	39.8712	0.0135	78.061
	2547	9.4621	38.4049	0.0023	74.581

Comparison between Proposed Technique and Previous Technique (Multiple Embedding Strategy)

Table 2: Comparison between Proposed Method and Previous Work Using Multiple Embedding Strategy

Image	L. Li et al [6]		Proposed Method	
	BPP	PSNR	BPP	PSNR
Owl (512 X 512 X 3)	2	53.166	3	73.164
Plane (512 X 512 X 3)	2	53.905	3	65.196
Giraffe (512 X 512 X 3)	2	52.842	3	71.567

Results Using Proposed Algorithm

Data of Length 792, 1792, 2547 Bytes for owl Plane and Giraffe Images:

Original Image Edges of Image Image after hiding 792 Image after hiding 1792 Image after hiding 2547

Bytes **Bytes** **Bytes**

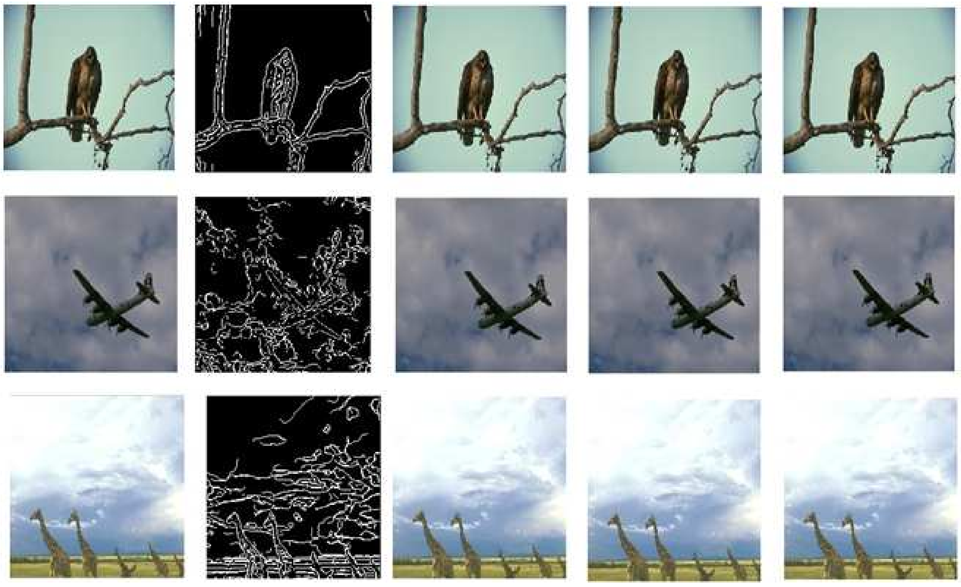

Figure 4: Message Hiding With 792, 1792, 2547 bytes of Data

Between Proposed Technique and Previous Technique (Edge Adaptive)

Table 4: Between Proposed Method and Previous Work Using Edge Adaptive

Embedding Rate (%)	W. Luo et al [7]	Proposed Method
	PSNR (in dB) Size (384 X 512 X 3)	PSNR (in dB) Size (384 X 512 X 3)
10	61.9	76.8021
30	56.8	72.4140
50	54.1	69.4584

4. CONCLUSIONS

A Block based Steganography Techniquehas been implemented and analysed for colour images in this paper. To make the algorithm well suited for high data capacity embedding system, the edge pixels from every layer are found out 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. Results have been compared with other previous Techniques and are found far better than previous. Future work should include improving embedding capacity by increasing the block size.

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. Tayana Morkel, "Image Steganography Applications for Secure Communication", Universities van Pretoria, May 2012

3. Shashikala Channalli, Ajay Jadhav, "Steganography*:* An Art of Hiding Data", International Journal on Computer Science and Engineering, Vol.1 (3), pp. 137-141, 2009.

4. S.F. Mare, M. Vladutiu, L. Prodan, “Decreasing change impact using smart LSB pixel mapping and data rearrangement ”, IEEE, 2011

5. 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.

6. L. Li, B. Luo, Q. Li et al, “A Color Images Steganography Method by Multiple Embedding Strategy Based Sobel Operator”, IEEE International Conference on Multimedia Information Networking and Security, pp. 118-121, 2009.

7. W. Luo, Member, IEEE, F. Huang, Member, IEEE et al, “Edge Adaptive Image Steganography Based on LSB Matching Revisited”, IEEE transactions on information forensics and security, Vol. 5, No. 2, June 2010.

8. 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.

9. 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.

10. V. Sharma, S. Kumar, “A New Approach to Hide Text in Images Using Steganography”, IJARCSSE, Volume 3, Issue 4, ISSN: 2277 128X, April 2013.