Design of an Edge Detection Based Image Steganography with High Embedding Capacity

Arup Kumar Pal[1] and Tarok Pramanik[2]

[1] Department of C.S.E, ISM Dhanbad,Jharkhand, India
[2] Department of C.S.E, R.V.S College of Engineering and Technology, Jamshedpur, India
{arupkrpal,tarok.kgec}@gmail.com

Abstract. In this paper, the authors have proposed an image steganography method for improving the embedding capacity of the gray-scale cover image. In general, the embedding of the secret message into the sharp areas i.e. edge region rather than in the smooth areas i.e. non edge region of the cover image attains relatively better quality stego-image. So in the proposed work, we have also exploited the presence of edges in the cover image to embed a large amount of secret message into the cover image. The proposed method carried out into two phases: in the first phase the cover image is classified into edge region and non-edge region. Subsequently in the second phase, the binary secret message bits are embedded by replacing some least significant bits (LSBs) of each pixel. In the proposed work, x LSBs replacement are preferred for the pixels belongs to edge region and y LSBs replacement are considered for non-edge region pixels where x>y. The proposed method increases the embedding capacity of the cover image compare to some existing standard steganographic methods. The scheme has been tested on several standard gray-scale test images and the obtained simulation results depict the feasibility of the proposed scheme.

Keywords: Edge Detection, Image Steganography, Information Security, LSB Substitute method.

1 Introduction

The widespread popularity and usage of Internet make the information interchange or communication easier and faster. In such type of communication, the data or information travel through the public channel. So sometime, it becomes essential to prevent the unauthorized accessibility of these data from the illegitimate users. To keep the data secure, various types of cryptography [1] and steganography [2] techniques have been devised. In cryptography, the encryption technique [1] transferred the secret data into corresponding cipher text using a secret key. This cipher text is unintelligible to the illegitimate user. Only the decryption technique [1], reverse process of the encryption, extracts the original data from the cipher text using the secret key. Although after encryption process, the produced cipher text is remained secure but still it flags the importance of the cipher text and attracts

K. Singh, A.K. Awasthi, and R. Mishra (Eds.): QSHINE 2013, LNICST 115, pp. 794–800, 2013.

illegitimate users or opponent's attention to employ different possible cryptography attacks on the cipher text to extract its original content. To sidestep this kind of drawback of the cryptography, steganography [2] is another widely accepted approach for secure communication of the secret message. In this method, the actual data or secret message are embedded into a digital cover media like digital image, audio or video in such a way that the secret message will be visually imperceptible after embedding into the cover media. In steganography, after embedding secret message into the cover media, the modified cover media, which is known as a stego-media should look visually almost similar to the cover media. So in this approach, the secret message becomes imperceptible and also such approach is capable to divert opponents' attention so that the chance of attacks will be reduced. Therefore to protect the secret message from being illegally accessed, steganography is a better choice than the cryptograpy.

In general, steganography is classified as video steganography [3], audio steganography [4], image steganography [5] and text steganography [6] based on the used carrier or cover media like video, audio, image and text respectively to embed the secret data into them. In image steganography, the used cover media is a digital image which is termed as cover image or host image. The cover image with the embedded secret data forms the stego-image. During designing of an image steganography, it is found a trade-off between the hiding capacity of the cover-image and the visual quality of the stego-image. So the aim of an effective image steganography is to preserve high quality of stego-image with high embedded secret message . To achieve this goal, in literature several well accepted image stegnography[5,7-10] have been proposed. Among them simple least significant bit (LSB) substitution [2] is one of the widely used methods due to its low computational complexity and high hiding capacity. In this approach, the secret data are initially converted into binary data and the corresponding binary bits sequence are concealed into cover image pixels by replacing a number of the least significant bits (LSB) of each pixel. In digital image most of the significant information is carried out by the most significant bits (MSB) of each pixel so changing the MSBs of the cover image pixel will cause serious degradation of the visual quality of the stego-image [5]. Thus, the LSB substitution method fixes on to embed secret data into the parts of LSB of the cover image pixel. In general up to first *3* LSB bits of the cover image pixels are used to conceal the secret message bits otherwise the quality of the stego-image is found to degrade extremely [5]. In literature, some modified schemes based on LSB substitution [5, 7] were proposed but all those schemes were only capable to improve the visual quality of the stego-image where no improvement of the hiding capacity is found. So in this paper, our aim is to improve the embedding capacity without compromising the visual quality of the stego-image. It has been found in many experiments that the insertion of the secret data into the sharp or edge region of a cover image is more effective than embedding into the smooth region [9], as it causes less distortion on the cover-image. So in the proposed work, we have taken advantage of sharp/edge region of the cover image pixels to hide large amount of secret data by replacing 4 LSB bits where in non-edge or smooth region pixels are replaced up to maximum 3 LSB bits. In the proposed method, hiding capacity has been increased as well as the quality of the stego-image is well preserved. The rest of the paper is organized as follows. The details of the proposed image steganography method are presented in section 2. The experimental results are described in sections 3 to show the effectiveness of the proposed method and finally, section 4 provides some conclusions.

2 Proposed Image Steganography

The intention of the proposed image steganography method is to improve/increase the hiding capacity of the cover image. The proposed method takes advantage of the presence of edge region in the cover image to embed more secret information than embedding into non-edge region. The embedding process of the proposed work is implemented broadly in two phases. In the first phase, we have used edge detection mask like sobel [11] with a suitable threshold value on the cover image to find the edge detected image. In the subsequent stage, this edge detected image helps to locate the edge and non-edge region of a cover image. In the last phase, the embedding process has been carried out where we have used simple LSB substitution methods for embedding binary bit sequence of the secret message into the cover image using varying LSB substitute values. In the embedding process, the pixels belongs to edge region are replaced by higher LSB substitute values than the pixels belongs to non-edge region. However in edge detection based steganography method, the main challenge is to identify the same edge and non-edge region from the resulted stego-image during extraction process. So in this work, we have embedded some additional information during embedding process so that the receiver can easily found out the edge and non-edge region from the stego-image. The embedded information may consider as indicator. The algorithmic steps of the proposed embedding procedure are presented as follows.

Algorithm 2.1: Embedding Procedure
Input: A secret image and a cover image
Output: A stego-image.
Step 1: Employ any edge detection mask/operator with a suitable threshold value, *Th* on the cover image to obtain the edge detected cover image. Convert the secret image into secret binary data *(SB).*
Step 2: Decompose both the edge detected image and the cover image into non-overlapping blocks of size $n \times n$. Find the presence of the prominent edge line in each block from the cover image based on the occurrence of the edge line in corresponding block of the edge detected image.
Step 3: Use first pixel of every block as an indicator pixel. Replace *3* LSBs of indicator pixel for each block by one of the following *3* bits information *000, 001, 010, 011* and *100* for indicating the presence of smooth region, horizontal edge, vertical edge, 45^0 diagonal edge and 135^0 diagonal edge respectively.
Step 4: Process each block as raster scan order (i.e. from left to right followed by top to down) and embed secret message bits from *SB* into each block where during embedding process for each block if the pixels belong to the edge line then choose 'x' bits secret message from *SB* for embedding into each pixel LSBs position.

Otherwise if the pixels belong to the non- edge region then consider ‘y’ bits secret message from *SB* for insertion into the corresponding pixels LSBs position. Here x>y. Now after completion of embedding all binary bits sequence of *SB* into cover image, the stego-image is formed.

The schematic diagram of the proposed embedding procedure is shown in Fig.1. The secret message can be extracted from the stego-image in comparatively less number of steps than embedding procedure. The algorithmic steps are presented as follows.

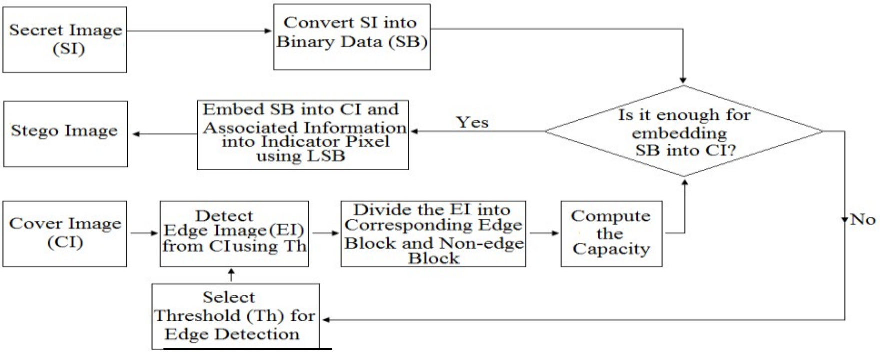
Secret Image (SI)
Convert SI into Binary Data (SB)
Stego Image
Embed SB into CI and Associated Information into Indicator Pixel using LSB
Yes
Is it enough for embedding SB into CI?
No
Cover Image (CI)
Detect Edge Image(EI) from CIusing Th
Divide the EI into Corresponding Edge Block and Non-edge Block
Compute the Capacity
Select Threshold (Th) for Edge Detection

Fig. 1. The Proposed Embedding Procedure

Algorithm 2.2: *Extraction Procedure*
Input: The stego-image
Output: The secret image (SI)
Step 1: Decompose the stego-image into non-overlapping blocks of size $n\times n$.
Step 2: Process each block as raster scan order and extract 3 bits information from first pixel 3LSBs position of every block. Extracted 3 bits information is the indicator value to locate the presence of prominent edge direction in the corresponding block.
Step 3: Based on indicator value find the edge pixels and non-edge pixels from each block. Extract from each pixel (except indicator pixel) LSB position either ‘x’ bits data for edge pixel or ‘y’ bits data for non-edge pixel to form secret binary data (SB). Convert the secret binary data (SB) into corresponding image i.e. the secret image.

3 Experimental Results and Discussion

In he proposed scheme has been tested on number of standard gray-scale images but in this paper, we have presented the simulation results for two different types of cover images. For making comparisons convenience, we have chosen same secret message i.e. a standard gray-scale image for embedding into different cover images. The used cover images, each of size *510*×*510* and the secret image of size *289*×*324* are shown in Fig. 2.

In our experiment, the detection of an edge image (EI) from the cover image (CI), using an appropriate threshold value (Th), has been carried out by a MATLAB command *EI=edge (CI,‘sobel’,Th).* Here, we have considered *Th=0.1* and *0.01* for comparative study. Fig. 3 shows the presence of edge pixels in the corresponding cover image. In our experiment, the cover image are decomposed into non-overlapping blocks of size *5×5* and afterwards the secret message bits and the corresponding indicator value are embedded into each blocks using LSB substitute method. The pixels those belongs to edge line, contains 4-bits secret message in LSB position whereas the non-edge pixels contain 3-bit secret message in their corresponding LSB position. The stego-images thus formed are shown in Fig.4. Based on the human visual perception, it can be observed that the stego-images shown in Fig.4 are quite good and almost similar as their corresponding original cover image. We also compared our proposed work with LSB substitute method and OPAP method [5] in terms of the peak signal-to-noise ratio (PSNR) value and by computing embedding capacity respectively. Table 1 shows the obtained PSNR values from different stego-images, resulting after embedding the secret pappers image, using different method like LSB substitute method, OPAP [5] and the proposed method with threshold value 0.01 and 0.1 respectively. According to the results shown in Table 1, it is evident that the PSNR values of the stego-images are slightly inferior than the other compared methods. However in our proposed method, the obtained PSNR values are reasonably good since it has been observed that an image with a PSNR value greater than 30 dB is acceptable by human visual perception [10] . The LSB substitute and OPAP methods provide same embedding capacity and it always fixed for any cover image. The embedding capacity for a cover image of size 510×510 is 95.25 KB when 3 bits LSB replacement is considered. But in the proposed scheme, the embedding capacity varies for image to image since every image has different edge patterns. Table 2 shows the embedding capacity of the proposed method for various cover images. According to the results shown in Table 2, it is clear that the embedding capacity of the proposed method with Th=0.1 is not better than LSB substitute and OPAP methods. However embedding capacity of the proposed method with Th=0.01 is superior to the other mentioned methods. So the prposed method with Th=0.01 is capable of providing high embedding capacities while retaining image quality higher than 30dB.

(a) (b) (c)

Fig. 2. The original Cover image (a) Lena Image and (b) Goldhill; the secret message (c) Peppers image

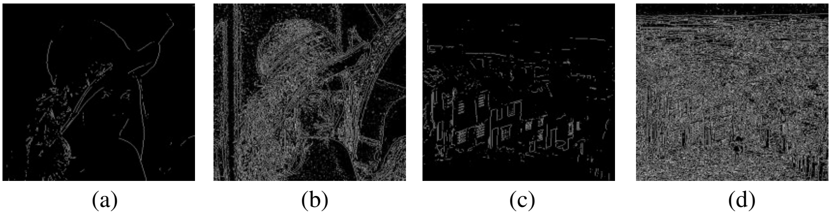

Fig. 3. Edge detected image of (a) Lena using threshold value 0.1;(b) Lena using threshold value 0.01;(c) Goldhill using threshold value 0.1;(d) Goldhill using threshold value 0.01

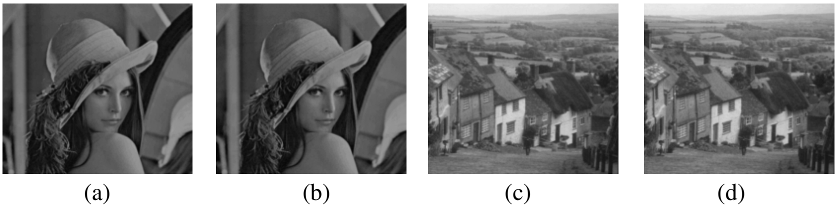

Fig. 4. Stego-image of (a) Lena using threshold value 0.1; (b) Lena using threshold value 0.01; (c) Goldhill using threshold value 0.1;(d) Goldhill using threshold value 0.01

Table 1. Comparative Study in Terms of PSNR (in dB) of the Stego-images Created by Various Embedding Algorithms

Cover Image	**Embedding Method**			
	LSB Substitute	**OPAP [5]**	**Proposed (Th=0.1)**	**Proposed (Th=0.01)**
Lena	38.1826	39.0843	**37.6974**	**36.6174**
Goldhill	38.1741	39.0747	**37.5753**	**36.3499**

Table 2. The Embedding Capacity of the Proposed Method

Embedding Method	**Cover Image**	**Number of Non-Edges Blocks**	**Number of Edges Blocks**	**Embedding Capacity (KB)**
Proposed Method (Th=0.1)	Lena	9526	878	**91.98**
	Goldhill	8811	1593	**92.41**
Proposed Method (Th=0.01)	Lena	2860	7544	**96.05**
	Goldhill	698	9706	**97.37**

4 Conclusion

In image steganography, a trade off always exists between hiding capacity of the cover image and the visual quality of the stego-image. In this paper, the proposed method is proficient to enlarge the hiding capacity with retaining high quality stego- image. In steganography, it has been found that up to 3 bits secret message is possible to embed in the pixels LSB position where in contrast more than 3 bits secret message can be embedded into the pixels belong to edge region. Therefore in this paper for improving the hiding capacity, we have considered 4 LSBs replacement for embedding secret message bits into the pixels belongs to edge region whereas 3 LSBs replacement are preferred for pixel belong to non-edge region. The experimental results shows that the proposed method has attain better hiding capacity than the LSB substitute and OPAP methods with maintaining acceptable PSNR value for the stego- image.

References

[1] Stalling, W.: Cryptography and Network Security: Principles and Practices, 4th edn. Pearson Education, India (2007)

[2] Lu, C.-S.: Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property. Idea Group Publishing (2005)

[3] Hanafy, A.A., Salama, G.I., Mohasseb, Y.Z.: A secure covert communication model based on video steganography. In: Military Communications Conference, MILCOM 2008, vol. 1-6, pp. 16–19. IEEE (November 2008)

[4] Cvejic, N., Seppanen, T.: Increasing the capacity of LSB-based audio steganography. In: 2002 IEEE Workshop on Multimedia Signal Processing, December 9-11, pp. 336–338 (2002)

[5] Chan, C.K., Cheng, L.M.: Hiding data in images by simple LSB substitution. Pattern Recognition 37(3), 469–474 (2004)

[6] Satira, E., Isikb, H.: A compression-based text steganography method. The Journal of Systems and Software 85, 2385–2394 (2012)

[7] Wang, R.Z., Lin, C.P., Lin, J.C.: Hididng data in images by optimal moderately-significant-bit replacement. IEE Electronics Letters 36(2), 2069–2070 (2000)

[8] Wang, R.Z., Lin, C.F., Lin, J.C.: Image hiding by optimal LSB substitution and genetic algorithm. Pattern Recognition 34(3), 671–683 (2001)

[9] Chen, W.J., Chang, C.C., Le, T.H.: High payload steganography mechanism using hybrid edge detector. Expert Systems with Applications 37, 3292–3301 (2010)

[10] Yu, Y.H., Chang, C.C., Lin, I.C.: A new steganographic method for color and grayscale image hiding. Computer Vision and Image Understanding 107, 183–194 (2007)

[11] Gonzalez, R.C., Woods, R.E.: Digital Image Processing, 3rd edn. Pearson Education, India (2008)