A Proposed Method for Image Steganography using Edge Detection

Sneha Arora¹, Sanyam Anand²

¹Student, Lovely Professional University, jalandhar. ²Assistant Professor, Lovely Professional University, jalandhar. snehaarora.ptk@gmail.com, sanyam15736@lpu.co.in

Abstract: In this paper, we proposed a technique to 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. The proposed scheme achieved high embedding capacity and high quality of encoded image.

Keywords: Decoding, Edges, Encoding, Steganography.

Introduction

Steganography is the art of hiding information in ways that prevent the detection of hidden messages. Steganography, derived from Greek, literally means "covered writing." It includes a vast array of secret communications methods that conceal the message's very existence. These methods include invisible inks, microdots, character arrangement, digital signatures, covert channels, and spread spectrum communications. Steganography and cryptography are cousins in the spycraft family. Cryptography scrambles a message so it cannot be understood. Steganography hides the message so it cannot be seen. A message in ciphertext, for instance, might arouse suspicion on the part of the recipient while an "invisible" message created with steganographic methods will not [1].

Image Steganographic techniques can be divided in to two groups: the Spatial domain technique group and the Transform domain group. The Spatial domain technique embeds information in the intensity of the pixels directly, while the Transform domain technique embeds information in frequency domain of previously transformed image [2].

In this paper, most of the work is done to get better quality of encoded image and to enhance hiding capacity. This work is a kind of spatial domain technique.

Related Work

Simrat Pal Kaur and Sarbjeet Singh, "A New Image Steganography Based on 2k Correction Method and Canny Edge Detection", International Journal of Computing & Business Research ISSN: 2229-6166 [3].



This paper proposed the use of Steganography along with 2k correction method & edge detection method. This technique proves to be better than earlier techniques because of its capability of carrying large payload with better imperceptibility. This can be achieved by embedding more data in edge areas as compared to smooth areas of the image as human eye cannot detect the distortion at edges easily. The proposed algorithm yields better PSNR values as compared to previous algorithms [3].

> Saurabh Singh, Gaurav Agarwal, "Use of image to secure text message with the help of LSB replacement", International journal of applied engineering research, volume-1, 2010 [4].

This paper proposed a novel approach that can effectively hide a message inside a digital image file. In this paper author presented the technique which works by changing a few pixel color value; author used selected pixel value to represent characters instead of a color value and the resulting image still look mostly like the original except that a few points seem little out of place if we look very closely [4].

Nitin Jain, Sachin Meshram and Shikha Dubey, "Image Steganography Using LSB and Edge – Detection Technique", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 2012 [5].

This paper proposed a new scheme in which edges are used to embed data into gray scale images. Canny edge detector is used to detect the edges of the image and least significant bit insertion method is used to embed the data in to the image [5].

➤ Wen-Jan Chen, Chin-Chen Chang, T-Hoang Ngan Le, "High payload steganography mechanism using hybrid edge detector", Expert Systems with Applications 37 (2010) 3292–3301, ELSEVIER [6].

This paper proposed a steganography scheme which is based on the LSB (least significant bit) steganography mechanism and a hybrid edge detector which combines the fuzzy edge detector with canny edge detector. In this work the hybrid edge detector is applied first on the cover image and then the secret message is embedded in the edges of the image using LSB technique [6].

Proposed Scheme

In this section proposed method for text encoding and decoding is given.

A. System model

The system model of the proposed work is described in Figure.1.

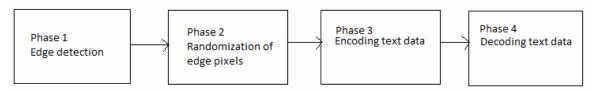


Figure.1 System Model



Phase 1: Edge detection:

Edges will be detected first by using 3x3 window scanning.

Phase 2: Randomization of edge pixels:

Sorting method will be used to randomize the edge pixels.

Phase 3: Encoding text data:

Text data will be encoded in to the blue component of sorted edge pixels.

Phase 4: Decoding text data:

Text data will be recovered from the encoded image.

B. Proposed algorithm for encoding text data

Step1: Input RGB image.

Step2: Detected the edges by 3x3 scanning window and store these edge pixels in an array (A1).

Step3: Input the text data and store in another array(A2).

Step4: Sort is applied on array (A1) to randomize the edge pixels.

Step5: The ASCII value of array A2[i] is replaced with blue component of array A1[i].

Step6: The output is the image containing text data.

C. Proposed algorithm for decoding text data

Step1: Input encoded image.

Step2: Input the array A1 as shared symmetric key.

Step3: Values of blue component at A1[i] are read.

Step4: The output is the text file.

Conclusion

In this paper, Edge based image steganography technique is proposed. In this technique, Advantage of edge detection technique is to be taken to increase capacity. Because editing in edge areas cannot be detected well by human eye, but editing in smooth areas can be detected easily.



References

- [1] Neil F. Johnson, Sushil Jajodia, "Exploring Steganography: Seeing and Unseen", 0018-9162/98/\$10.00 © 1998 IEEE.
- [2] Amanpreet Kaur, Renu Dhir and Geeta Sikka, "A New Image Steganography Based On First Component Alteration Technique", International journal of computer science and information security, vol.6, no.3, 2009.
- [3] Simrat Pal Kaur and Sarbjeet Singh, "A New Image Steganography Based on 2k Correction Method and Canny Edge Detection", International Journal of Computing & Business Research ISSN: 2229-6166, 2012.
- [4] Saurabh Singh, Gaurav Agarwal, "Use of image to secure text message with the help of LSB replacement", International journal of applied engineering research, volume-1, 2010.
- [5] Nitin Jain, Sachin Meshram and Shikha Dubey, "Image Steganography Using LSB and Edge Detection Technique", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 2012.
- [6] Wen-Jan Chen, Chin-Chen Chang, T-Hoang Ngan Le, "High payload steganography mechanism using hybrid edge detector", Expert Systems with Applications 37 (2010) 3292–3301, ELSEVIER.

* * * * *

