Image Steganography Based on Edge Detection and the Average Values between Edge Points

Samraa Adnan Al-Asadi

Department of Information Networks / College of Information Technology, University of Babylon

samraa.alasadi@uobabylon.edu.iq

ARTICLE INFO
Submission date: 5/7/2018
Acceptance date: 12/9/2018
Publication date: 10/3/2019

Abstract

Steganography aims to hide a message or generally a file in some cover medium with hiding the existence of the secret message. Many medium can be used as carriers or covers, but images still the most popular due to its heavy use in the internet and its higher amount of data that can be used to hide more secret data. In this paper, a new approach for concealing secret text message within color image is introduced. It depends mainly on using the three red, green and blue bands of the color cover image as three independent grayscale images, then using different edge detector for each one. After finding these edges, the secret text message bits are divided into three segments, each concealed within different grayscale image by utilizing the strongest edges first. The embedding of the secret message bits is implemented by calculating the average value between each two adjacent edge pixels for concealing one bit.

Key words: Image Steganography, Edge Detection, Color images

.

تضمين وإخفاء البيانات داخل الصور بالاعتماد على اكتشاف حواف الصورة ومتوسط القيم بين نقاط الحواف

سمراء عدنان الاسدي

قسم شبكات المعلومات/ كلية تكنولوجيا المعلومات/ جامعة بابل

الخلاصة

إن الهدف الرئيسي من تقنية إخفاء المعلومات هو تضمين رسالة سريه أو أي ملف ضمن احدى الوسائط (نص اخر او صورة على سبيل المثال) مع إخفاء وجود هذه الرسالة السرية. يمكن استخدام العديد من الوسائط كناقلات أو أغلفة ، لكن الصور لا تزال الأكثر شيوعا نظرا لاستخدامها الكثيف في الإنترنت وكمية البيانات العالية التي يمكن استخدامها لإخفاء المزيد من البيانات السرية. في هذا البحث، يتم تقديم نهج لإخفاء الرسائل النصية السرية داخل الصورة الملونة والذي يعتمد بشكل أساسي على استخدام الحزم الثلاثة الحمراء والخضراء والزرقاء لصورة الغلاف الملون كثلاث صور مستقلة بالتدرج الرمادي ، ثم استخدام كاشف حواف مختلف لكل صوره على حده. بعد العثور على هذه الحواف ، يتم تقسيم بتات الرسائل النصية السرية إلى ثلاثة أجزاء ، كل منها مخفي داخل صورة مختلفة بالتدرج الرمادي باستخدام أقوى الحواف أولا. يتم تنفيذ تضمين بتات الرسالة السرية عن طريق حساب متوسط القيمة بين كل بكسلين متجاورين لإخفاء بت واحد من الرساله النصيه السريه.

الكلمات الدالة: إخفاء المعلومات, كشف حواف الصوره, الصورة الملونة.

Introduction

Steganography, cryptography and watermarking are data-hiding techniques that eliminate the security issue occurred as the internet is heavily grown and used. When transmitting a file between the sender and the transmitter, the third party should be prevented from reaching or just knowing about this message or file [1]. Steganography is the art and science of hiding the secret message within some kind of carrier files such as text, image, audio and video. Steganography conceals the secret message so that no one can predict the existence of that secret message [2, 3].

Between these carriers, images are preferred for transmitting the secret message over the internet, due to its small size, its adaptable content, and its visual resilience [4]. Selection of pixels for embedding the secret message is very important to secure the steganography technique, where using the pixels that are randomly changing is better because changing the value of some of these pixels is difficult to be noticed by human eyes [4]. Depending on the relationship of the pixel with its neighbors, edge detector decides whether that pixel is an edge point or not. If the pixel's gray level changes rapidly than its neighbors it will be an edge, otherwise it is not [5]. Due to the sudden change (higher or lower) in the gray level between an edge point and its neighbors, edge point is perfect to be used for embedding the secret message [4]. Number of masks used as edge detectors, like Sobel, Prewitt which both are 3*3 gradient edge detectors [5, 6]. Laplacian operator that is zero crossing detector with mask coefficients sum to zero is also used as edge detector [5]. Collection of edge points results in lines and curves that indicate the objects boundaries of the image [5, 7].

Related Works

Following, some of the related works that are using edges to conceal the secret message:

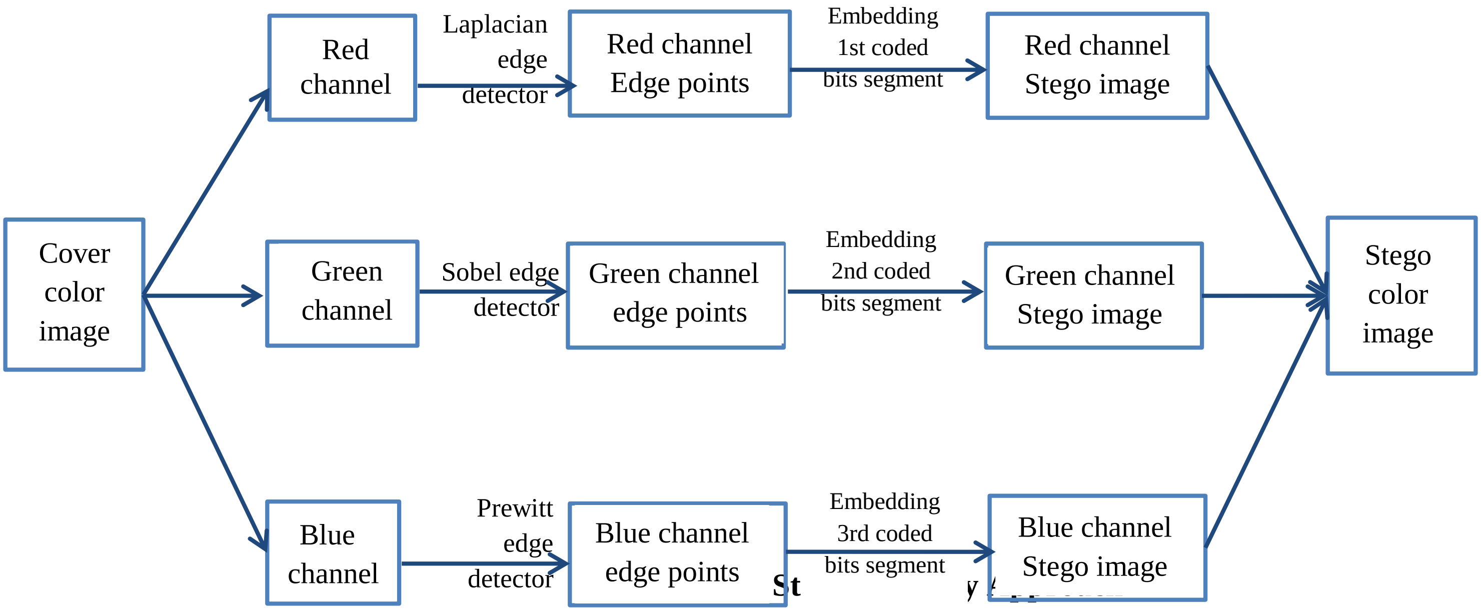
- Nitin Jain et. al, (2012) presented a technique by converting the grayscale image to binary image in order to find dark (black) areas, then converting these binary images to RGB image, and using every eight pixels of the dark places as a byte to embed one bit from the secret message by utilizing the least significant bit for each byte [6].
- Youssef Bassil, (2012) propose a method for hiding the secret message in the three LSBs of every pixel detected as an edge by using Canny edge detector. The proposed method is parameterized by the size of the Gaussian filter, and both low and high threshold values. These parameters make the method has different output for the same cover image and secret data [7].
- Arup Kumar Pal, et.al, (2013) proposed a method that first divides the cover image into edge and non-edge regions, then the bit of the secret message are embedded at some LSBs of each pixel. Exactly, the proposed method uses x LSBs from the edge region pixels and y LSBs form non-edge region pixels, where x>y [8].
- Sneha Arora et. al, (2013) proposed a method depends on finding edge point for embedding the secret data since it is more difficult to notice the change by human eyes in the noisy areas (edges), the method embeds the secret message in the first (blue) component of the sorted edge pixels [9].
- Saiful Islam et. al, (2014) proposed a steganography technique that depends mainly on the amount of data to be embed, where the more amount of data implies the use of

weaker edges. For embedding the secret data, two least significant bits of the edge pixels are modified to the corresponding two consecutive secret message bits [4].

- Shahzad Alam et. al, (2014) presented a steganography technique that get advantage of finding edge points in order to increase the capacity. For imbedding, the proposed method uses secret key based random LSB substitution [10].
- Krupali V. Deshmukh et. al, (2014) presented a steganography method for binary images by using edge based grid, this method has main parts. First, is finding the start location of valid contour, then tracing the contour segment and checking its embeddability, L shape pattern is used to achieve good perceptional quality[11].
- S. Uma Maheswari et. al, (2015) proposed a frequency domain steganography method and utilizing the advantage of Ridgelet transform, by representing the image with straight edges. They used hybrid edge detector in the embedding phase to get the edges from the cover image, the edge image is then partitioned into several blocks to operate with straight edges. Then the Ridgelet transform is applied to each block. The more significant edges are selected to hiding the secret data [1]
- Smitha GL et. al, (2018) presented a steganography technique that uses Sobel edge detector on the cover image to get edges, then utilizing sharper edges for embedding the secret message bits. The proposed method applies compression and encryption on the secret message in order to reduce the amount of embedded data and to raise the security [12].

The Proposed Steganography Approach

The proposed approach uses 7-bits ASCII codes for coding the secret text message, these codes starts from “0000000” to “0111111” while the last ASCII code ”1111111” is used as a sign for the end of the input secret bits stream. The coded stream of bits is divided into three segments; each segment will be embedded separately into red, green, or blue channel of the color cover image. Each segment of the coded bit stream is concatenated with the special 7-bits code “1111111” in order to denote the end of each bits segment in the extraction process. So, the color cover image is converted to three grayscale images of red, green, and blue channels, then the edges will be collected from each channel using different edge detector. For the red channel, *Laplacian edge detector* is used and for green channel *Sobel edge detector* is used, while *Prewitt edge detector* is used for the blue channel. For each grayscale image, sharper edge points are utilized first for concealing the secret message bits. After concealing the secret bits, the stego color image is obtained by combining the three stego grayscale images. Figure 1 shows the block diagram for the proposed steganography approach.



The benefit of splitting the cover color image to three grayscale images is to find different edge points for each channel. So for the Stego color image, there is no clear cut for which pixel is changed, and for each pixel also there is no clear cut for which component (red, green or blue) are used for the concealing process. The embedding of each secret bit is determined by examining the average value between each two successive edge points. Following are the steps of the proposed steganography embedding method:

- Get three gray scale images for Red, Green and Blue channels from the color cover image.
- For each Red, Green, and Blue channel, use a different edge detector to find edge points sets.
- For each edge set determine the more significant (sharper) edge points.
- Coded the secret text message using the ASCII codes.
- Divide the coded bits stream to three segments.
- Conceals each segment in a different gray scale image.

-For each bit:

- If the secret bit is “0”:
- If the average between two successive edge points has no reminder: do nothing
- Else subtract or add 1 to one of these two edge points.
- If the secret bit is “1”:
- If the average between two successive edge points has reminder: do nothing
- Else subtract or add 1 to one of these two edge points.
- Get the color Stego image by combining the three Stego gray scale images.

As example of the embedding of a secret bit, suppose the two edge points are 150 and 156, so the average between them is 153 with no remainder. In this case if secret bit is “0”, no process will be done, while if the secret bit is “1”, the first edge point will become either 151 or 149, in order to make the remainder equal to 1.

At the extraction of the secret message bits, the process will be reversed as the following steps:

- Separate the Stego color image into three red, green and blue channels to get three Stego grayscale images.
- Use the same edge detectors used in the embedding part to get the edge point sets for each Stego grayscale image.
- For each Stego grayscale image, and from each two successive edge points, one secret bit is extracted depending on the reminder of the average between them.
  - If there is no reminder, the secret bit is "0";
  - Else the secret bit is "1".
- Combine the three extracted bit streams.
- Depending on the ASCII codes, get the secret message from the secret bits.

As example for the extraction of a secret bit from two successive edge points, suppose the two edge points are 100 and 150, so the average between them is 125 with no remainder. In this case, the secret bit is "0", while if the two edge points have the values of 100 and 101, the average between them is 100 with a reminder, so the extracted bit is "1".

Experimental Results

Each secret embedded bit either causes a change on the edge point or not, that depends on the bit value "0" or "1" and depends also on the remainder of the average value between the two edge points. Approximately, the number of pixels changed due to the embedding process is half the total number of the embedded secret bits. Many experiments are done with different length of the secret message with the same cover image, and all show that result.

The proposed steganography method can embed half the number of the detected edge points because each embedded bit needs two edge points. So, each two edge pixels of the cover color image can conceal 3 secret bits. For concealing one secret byte, 6 edge pixels from the color cover image are needed. Image with more edges can conceal more secret data than image of few edges. Table 1 shows the number of significant edges for three different cover images, while Figure 2 shows these cover image samples.

Table 1: Number of Edge Points for Different Color Cover Images

Cover image	Number of Edge points		
	Red Channel	Green Channel	Blue Channel
Lena	572	1955	1027
Balloons	123	203	58
Fruits	260	1390	880

(a) Lena Cover Image

(b) Fruits Cover Image

(c) Balloons Cover Image

Fig. (2): Samples of Color Cover Images

Peak Signal to Noise Ratio (PSNR) is a measurement used to check the quality of the proposed steganography method by checking the similarity between both cover and stego images.

The higher the PSNR value, the better the steganography approach. Eq. (1) is the PSNR equation.

$$\text{PSNR}= 10 \log_{10} \frac{(MAX)^2}{MSE} \quad \ldots\ldots\ldots\ldots\ldots\ldots.. (1)$$

Where MAX is the highest gray level value can be found in the image, while MSE is the Mean Square Error that is computed as shown in Eq. (2)

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

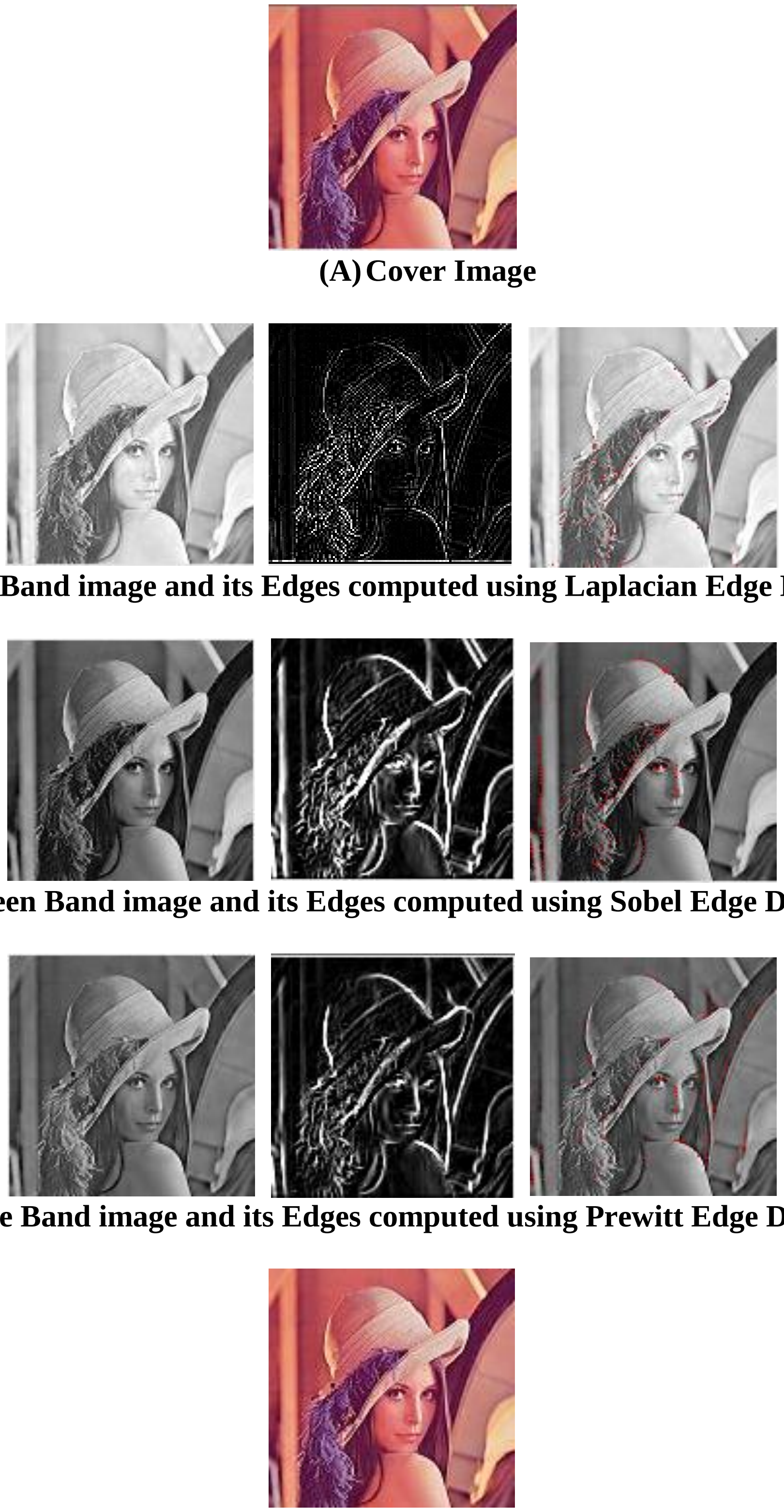
Where m and n are the height and width of both cover and stego images, *I (i, j)* is the pixel value of the cover image and *K (i, j)* is the pixel value of the stego image.

The proposed method has a high PSNR value since it uses edge points with moderate capacity of the embedding secret data. Since that not all the embedded secret bits causes change in the cover image, the yielded PSNR is high. As a result, when embedding secret messages with different length and for different cover images, the PSNR is in the range 57 to 66 as shown in Table 2.

Table 2: PSNR Values for different Cover Images

Cover Images	PSNR
Lena	66.30
Balloons	62.07
Fruits	57.19

Figure 3 shows a case of embedding bits stream with length equal to one quarter of the total number of edge pixels of the cover image. Red points are edge pixels that are used for the embedding of the secret bits.



(A) Cover Image

(B) Red Band image and its Edges computed using Laplacian Edge Detector

<

(C) Green Band image and its Edges computed using Sobel Edge Detector

(D) Blue Band image and its Edges computed using Prewitt Edge Detector

(E) Stego Image

Fig. (3): Case Study of the Proposed Steganography Approach

Conclusion

The proposed steganography approach has the advantage of concealing the secret data in areas with different and frequently changing gray level values than using each pixel of the cover image. Using the edge points will achieve this goal since the edge pixels are either significantly higher or lower than their adjacent pixels. Using different edge detector for each red, green and blue bands of the color cover image makes the concealing of secret bits randomized throughout the stego image. This makes the proposed approach more robust and secure.

References

[1] S. Uma Maheswari and D. Jude Hemanth, "Image Steganography using Hybrid Edge Detector and Ridgelet Transform", Defence Science Journal, Vol. 65, No. 3, May 2015, pp. 214-219, DOI : 10.14429/dsj.65.7871

[2] Samraa A. Al-Asadi and Wesam Bhaya, "Text Steganography in Excel Documents Using Color and Type of Fonts", Research Journal of Applied Sciences, 11: 1054-1059, 2016, DOI: 10.3923/rjasci.2016.1054.1059 URL: http://medwelljournals.com/abstract/?doi=rjasci.2016.1054.1059

[3] Samraa Adnan Al-Asadi, "Image Steganography Based on Variable Sized Segments", Journal of Engineering and Applied Sciences, 13: 2282-2287, 2018, DOI: 10.3923/jeasci.2018.2282.2287
URL: http://medwelljournals.com/abstract/?doi=jeasci.2018.2282.2287

[4] Saiful Islam, Mangat R Modi and Phalguni Gupta, "Edge-based image steganography", EURASIP Journal on Information Security, 2014, doi:10.1186/1687-417X-2014-8

[5] SCOTT E UMBAUGH, "DIGITAL IMAGE PROCESSING AND ANALYSIS, Human and Computer Vision Applications with CVIPtools", Taylor & Francis Group, LLC, 2011

[6] Nitin Jain, Sachin Meshram, 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

[7] Youssef Bassil, "Image Steganography based on a Parameterized Canny Edge Detection Algorithm", International Journal of Computer Applications (0975 – 8887) Volume 60– No.4, December 2012

[8] Arup Kumar Pal and Tarok Pramanik, "Design of an Edge Detection Based Image Steganography with High Embedding Capacity", institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2013, pp: 794-800

[9] Sneha Arora, and Sanyam Anand, "A Proposed Method for Image Steganography using Edge Detection", An International Journal of Engineering Sciences, Issue June 2013, Vol. 8, 2013

[10] Shahzad Alam, Vipin Kumar, Waseem A Siddiqui and Musheer Ahmad, "Key Dependent Image Steganography Using Edge Detection", IEEE, DOI 10.1109/ACCT.2014.72, 2014

[11] Krupali V. Deshmukh, Prof. Gyankamal J. Chhajed, "A Stenographic Method for Data Hiding in Binary Image using Edge based Grids", Int. J. Computer Technology & Applications, Vol 5 (4),1369-1374, 2014

[12] Smitha GL, Baburaj E, "Sobel edge detection technique implementation for image steganography Analysis", Biomedical Research 2018; Special Issue, pp: S48