International Journal of Hybrid Information Technology
Vol.6, No.5 (2013), pp.59-66
http://dx.doi.org/10.14257/ijhit.2013.6.5.06

Image Steganography using Hybrid Edge Detection and First Component Alteration Technique

Sarabjeet Kaur and Sonika Jindal

Shaheed Bhagat Singh State Technical Campus, Ferozepur

Kaursarabjeet095@gmail.com, sonikamanoj@gmail.com

Abstract

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. Experimental results show that we have achieved not only high embedding capacity but also enhanced the quality of the stego image.

Keyword: *Cover object, Decoding, Encoding, Stego object*

1. Introduction

Steganography is the method for secret communication. The word "Steganography" derives from Greek and it means "cover writing" [1]. Secret information can be hiding in one of two ways, cryptography and steganography. The methods of cryptography attract the attention of attacker, whereas the methods of steganography hide the existence of information. From the methods of steganography, the most common method is to use images to hide the data. That is called image steganography. In this method, the pixels of the images are altered to hide the secret data so as invisible to the others and the changes applied in the image are not tangible. The image used to encode the secret data is called the cover image while the cover image with the secret data encoded in it is called the stego image. Images are the most popular cover files used for steganography. In image steganography, many different image file formats exist. For different image file formats, different steganographic algorithms are there. There are two types of compression: lossy and lossless [2]. Both methods save storage space, but the procedures are different. Lossy compression creates smaller files by discarding excess image data from the original image. It deletes details that are too small for the human eye to differentiate. As a result, close approximations of the original image are made, but not an exact duplicate. An example of an image format that uses this compression technique is JPEG, whereas lossless method hides messages in more significant areas of the cover image, making it more robust. So the lossless image formats are most suitable for image steganography [3]. Image files fulfill this requirement of redundancy so they are very commonly used as a medium for steganography. Audio files contain redundant information but not used as widely as image files. There are two techniques proposed to use images as cover objects. These techniques can be categorized in the following two ways: Spatial domain techniques and Transform domain techniques.

ISSN: 1738-9968 IJHIT

Spatial domain techniques embed secret information in the intensity of the pixels directly, while in transform domain, images are first transformed and then the message is embedded in the image [7]. In spatial domain methods a steganographer modifies the secret data and the cover medium in the spatial domain. It involves encoding at the level of the LSB [6]. Transform domain techniques firstly transform the cover images using discrete cosine transformation or discrete fourier transformation and then hide the data inside them. Transform domain techniques [8] hide data in mathematical functions.

2. Related Works

Rubata Riasat *et al.*, (2011) proposed a hash based approach for image steganography. The most important part of the proposed algorithm is the used hashing technique that is perfect hashing. Perfect hashing is faster than the other techniques and it reduces hash collision. The proposed approach hides the text to red, green and blue channel of the pixels of the color image by replacing the ASCII value of the first, second and third character with the value of red, green and blue channel respectively. The strong point of the given approach is that it is fast and secure and the weak point of this approach is that picture quality of the output image is not very good [5]. Joyshree Nath *et al.*, (2011) proposed a randomization method for generating the randomized key to encrypt and decrypt the text file. In this work author have used two methods first, in which they encrypt the secret message using a method MSA proposed by Nath and second, in which they insert encrypted secret message inside the cover file by changing the least significant bit(LSB). The strong point of the given approach is that we can embed almost any type of file inside some cover file like image file (.jpeg or .bmp) or any image file inside another image file. Another strong point of the given approach is that if we change the key little bit then the whole encryption and decryption process will change [7]. Subba Rao *et al.*, (2011) proposed the randomization of cipher bits for secured image steganography. In this work author generate the random sequences of cipher bits by the use of an L.F.S.R (Linear Feedback Shift Register) and select the random sequence closest to the image and then embed these random sequences of cipher bits in the image. The strong point of the given approach is that there is no one to one mapping between a cipher text and an image. The weak point of the given approach is that this cannot hide large data in single image [8]. K. Pramitha *et al.*, (2011) proposed a new image steganography method based on image contrast for gray scale images. In this work a group of 2x2 blocks of spatially adjacent pixels is selected as the valid block for embedding the secret message and then modulo 4 operation is applied on each valid block to embed the binary bits. Each secret message is also encrypted by RSA encryption algorithm for more security. The strong point of the given approach is that it increases capacity of the secret data to be hide and provide imperceptible stego image quality [9]. Rajkumar Yadav, (2011) Proposed a technique in which Peak signal to noise ratio metric was used to compare different images. The image which has higher value of PSNR is better as compare to other image. So the author analyses that 6^{th}, 7^{th} and 8^{th} bit method is better as compare to LSB because 6^{th}, 7^{th} and 8^{th} bit method has high PSNR ratio than LSB. The advantage of this method is that this method has high robustness [10]. Pan et al, (2011) proposed a pixel value differencing based technique was in which the cover image is divided into 2x2 non overlapping blocks, then the modulus function method is used in horizontal direction and simple PVD method is used in vertical direction for steganography [13]. Elham Ghasemi *et al.*, (2011) proposed the application of Wavelet Transform and Genetic Algorithm in a novel steganography scheme. In this work, a genetic algorithm based mapping function to embed data in Discrete Wavelet Transform coefficients in 4x4 blocks on the cover image. The optimal pixel adjustment process is applied after embedding the

message. the frequency domain is utilized to improve the robustness of steganography and implementation of Genetic Algorithm and Optimal Pixel Adjustment Process to obtain an optimal mapping function to reduce the difference error between the cover and the stego-image, therefore improving the hiding capacity with low distortions [14]. Sevedi *et al.*, (2011) Proposed a new robust adaptive data hiding method in wavelet transform domain of image in which secret data is embedded in blocks of image that seems to be noisy based on the bit plane complexity of each block and does not destroy the co-occurrence matrix of wavelet coefficient [15]. Vikas Tyagi *et al.*, (2012) proposed a method in which a combination of least significant bit and symmetric encryption algorithm was used. In this the author first encrypt the data which he wants to embed. After encryption data is stored in image. The advantage of this method is that the data which is hide in image can transmit with more secrecy [11]. J. K. Mandal *et al.*, (2012) proposed a technique for secret data storing in each component of a pixel in an image using original pixel value differencing. The disadvantage of PVD is that the value of pixel increased from 0~255. So this overflow is eliminated in this paper. The advantage of original PVD method is that the quality of stego image is better as compare to image generated by PVD [12].

3. Proposed Work

3.1 Proposed Algorithm for Encoding data in Image

Step 1: Input the 24 bit RGB image I of size rxc.

Step 2: Detected the edges of the input image by using hybrid edge detector which is the combination of 3x3 scanning method using different orientations and sobel operator and then use these edge pixels as the key (K).

Step 3: Input the Text file (.txt) and store the secret message in an array list (S).

Step 4: Convert the characters, symbols etc. of secret message in to ASCII codes.

Step 4: The ASCII value of S[i] is replaced with blue component of K[i].

Step 7: The output will be the image containing secret message (I_1).

3.2 Proposed Algorithm for Decoding data from Image

Step 1: Input the encoded image (I_1).

Step 2: Input shared key (K), the pattern where data has been stored.

Step 3: Values of blue-byte at K[i] are read. As each byte contains the ASCII value of the character, the each ASCII value is converted to the character and each character is written to Text file.

Step 4: The output is the Text file (.txt) that contains the secret data decoded from the image.

4. Experimental Results

The results were evaluated both qualitatively and quantitatively. Two metrics are: PSNR (peak signal to noise ratio) and MSE (mean square error) are calculated for all the standard images. PSNR is most easily defined via the mean squared error (MSE). Given a noise-free m×n monochrome image I and its noisy approximation K, MSE and PSNR are defined as:

MSE – The MSE is the cumulative squared error between the compressed and the original image.

$$\text{MSE} = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\|I(i,j) - K(i,j)\|^2 \quad \ldots\ldots\ldots\ldots\ldots \quad [16]$$

PSNR – Peak signal-to-noise ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale.

$$\text{PSNR} = 10.\log_{10}\left(\frac{MAX_I^2}{MSE}\right) = 20.\log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots [16]$$

Here, MAXI is the maximum pixel value of the image. When the pixels are represented using 8 bits per sample, value of MAXI is 255. More generally, when samples are represented using linear PCM with B bits per sample, maximum possible value of MAXI is 2B-1. For color images with three RGB values per pixel, the definition of PSNR is the same except the MSE is the sum over all squared value differences divided by image size and by three. Typical values for the PSNR in image compression are between 30 and 40 dB [16].

Figure 1 shows original image of size 512x512 pixels and Figure 2 shows the edge detected of the original images and Figure 3 shows the encoded images with text data.

Peppers.tif Lena.tif Baboon.tif

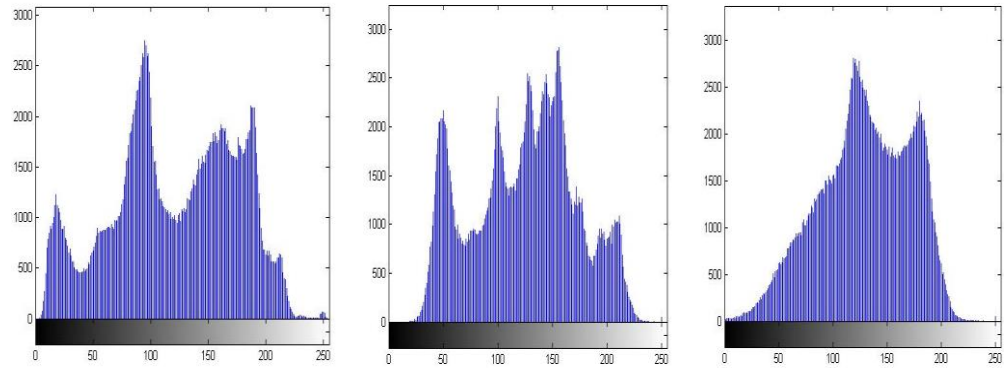
Figure 1. Original Images of Size 512x512

Peppers.tif Lena.tif Baboon.tif

Figure 2. After Applying Edge Detection Algorithm

Peppers.tif Lena.tif Baboon.tif

Figure 3. Encoded images with text data



Histogram of Peppers Histogram of Lena Histogram of baboon

Figure 4. Histograms of Original Images

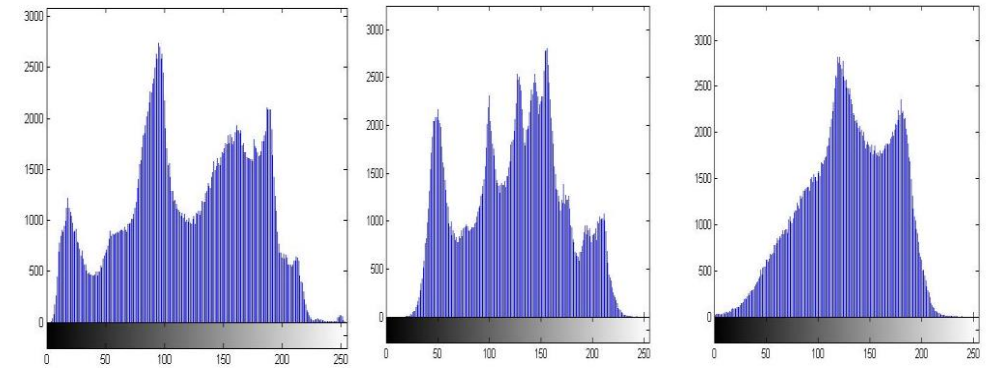


Figure 5. Histograms of encoded images with text data

We evaluated both qualitatively and quantitatively results of the proposed algorithm and its evaluated results are shown in Table 1 and Table 2.

Table 1. MSE Outputs

Text Data to be Hide (Bytes)	Lena	Peppers	Baboon
792	1.9044	3.7463	3.3397
1702	4.4395	8.0184	6.7508
2547	6.4501	12.4848	9.4621
4110	10.4937	20.1557	13.9992
6075	18.3308	31.9407	20.2122
11346	35.9050	53.8168	36.1801

Table 2. PSNR Outputs

Text Data to be Hide (Bytes)	Lena	Peppers	Baboon
792	45.3672	42.4288	42.9277
1702	41.6915	39.1239	39.8712
2547	40.0692	37.2010	38.4049
4110	37.9555	35.1208	36.7038
6075	35.5330	33.1214	35.1087
11346	32.6133	30.8556	32.5801

By analyzing visual and quantitative results, we can see that the proposed algorithm has good capacity and imperceptibility. Because typical values for the PSNR are between 30 and 50 dB, where higher is better. As we can see from the table 2 that our PSNR results are in between 30 and 50 dB, so we can say that our results are good.

5. Conclusion

In this paper, we have proposed a color image steganography scheme in which we use hybrid edge detection which is the combination of 3*3 matrix scanning and sobel edge detection and first component alteration technique. As compared with other steganography schemes proposed scheme increases the capacity of stego image due to the use of hybrid edge detection. Experimental results confirm that the proposed scheme is not only achieving the high capacity but also obtaining a stego image of good quality.

References

[1] T. Morkel *et al.*, "An overview of image steganography", Proceedings of the fifth annual information security South Africa conference (ISSA2005), **(2005)**.
[2] T. Moerland, "Steganography and steganalysis", Leiden institute of advanced computing science.
[3] M. Lal and J. Singh, "A novel approach for message security using steganography", 3rd International conference of advance computing & communication technologies, APIIT, Panipat, India, **(2008)** November 8-9.
[4] S. M. Seyedzade, R. E. Atani and S. Mirzakuchaki, "A novel image encryption algorithm based on hash function", IEEE, 978-1-4244-9708-vol-9, **(2010)**.
[5] R. Riasat, *et al.*, "A hash based approach for color image steganography", IEEE, 978-1-61284-941-vol-6, **(2011)**.
[6] S. C. Tai and S. M. Yang, "A Fast method for image noise estimation using laplacian operator and adaptive edge detection", IEEE, 978-1-4244-1688-vol-2, **(2008)**.
[7] J. Nath and A. Nath, "Advanced Steganography Algorithm using Encrypted secret message", International journal of advanced computer science and applications, vol. 2, no. 3, **(2011)**.
[8] S. Rao Y. V., B. Rao S. S. and R. Rekha N., "Secure image steganography based on randomized sequence of cipher bits", IEEE transactions, 978-0-7695-4367-vol-3, **(2011)**.
[9] K. Pramitha, L. P. Suresh and K. L. Shunmuganathan, "Image steganography using mod-4 embedding algorithm based on image contrast", IEEE, 978-1-61284-653-vol-8, **(2011)**.
[10] R. Yadav, "Analysis Of Various Image Steganography Techniques Based Upon Psnr Metric", International journal of P2P network trends and technology, vol. 1, Issue 2, **(2011)**.
[11] V. Tyagi, A. Kumar, R. Patel, S. Tyagi and S. S. Gangwar, "Image Steganography Using Least Significant Bit With Cryptography", Journal of global research in computer science, vol. 3, no. 3, **(2012)**.
[12] J. K. Mandal and D. Das, "Colour Image Steganography Based On Pixel Value Differencing In Spatial Domain", International journal of information sciences and techniques, vol. 2, no. 4, **(2012)**.
[13] F. Pan, "Image Steganography Method Based On Pvd And Modulus Function", IEEE Transactions, International conference on electronics, communications and control, **(2011)**.
[14] E. Ghasemi, J. Shanbehzadeh and N. Fassihi, "High Capacity Image Steganography Usingwavelet Transform And Genetic Algorithm", Proceedings of international multiconference of engineers and computer scientists, vol. 1, **(2011)** March 16-18.
[15] S. H. Seyedi, H. Aghaeinia and A. Sayadian, "A New Robust Image Adaptive Steganography Method In Wavelet Domain", IEEE Transactions, Iranian conference of electrical engineering, **(2011)**.
[16] http://en.wikipedia.org/wiki/Peak_signal-to-noise_ratio.

Authors

Sarabjeet Kaur is a Post graduate student . She is doing part time Mtech in Computer Science and Engg from Shaheed Bhagat Singh State Technical Campus, Ferozepur. She is a pro-term lecturer in Shaheed Bhagat Singh State Technical Campus, Ferozepur.

Sonika Jindal received the Masters in Computer Sc. & Engineering from Punjabi University, Patiala (Punjab) and is pursuing her Ph.D. She is currently working as Assistant Professor in Computer Sc. Deptt at Shaheed Bahgat Singh State Technical Campus, Ferozepur since October 2001.She has more than 14 years of teaching experience. Her areas of interest include Digital Image Processing, Image Retrieval based on content, Artificial Intelligence, Nature Inspired Computing, evolutionary computing with particular attention to pattern recognition, computer vision applications and machine learning. She has authored various papers in National/International Conferences and Journals.