Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 5, Issue. 11, November 2016, pg.37 – 43

Comparative Analysis of Color Image Steganography

Prof. Ziad A.A. Alqadi, Prof. Mohammed K. Abu Zalata, Ghazi M. Qaryouti

Albalqa Applied University

Jordan_Amman

Abstract: Image steganography is the art of hiding secret message or text into a digital image. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret text message in images, there exists a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. This paper will produce a simple and effective method to be used to hide short messages into RGB color image. The proposed method will be implemented, tested and compared with other existing method of image steganography. A comparative analysis will be made to demonstrate the effectiveness of the proposed method. The effectiveness of the proposed method will be estimated by computing Mean square error (MSE), Peak Signal to Noise Ratio (PSNR), time to hide the text message, and time to extract the message from the cover image.

Keywords: Cover image, MSE, PSNR, Hiding time, extracting time, speed up.

I- Introduction

Internet in now a days is the most popular, effective and faster media for data transmission, thus the data senders and data receivers via the internet need a highly secure method of data protection in order to avoid a variety of problems such as hacking, eavesdropping. Cryptography [1] and Steganography [2] are the available two fields for data security and **protection.**

Cryptography is a technique of converting the messages that are intended to be secret into some other form, such that it is not understandable to anyone other than the intended sender and recipients. Steganography is a technique for securing information by hiding it in some other medium, such that the existence of information is concealed to everyone except for the intended sender and receiver [3].

Steganography [4] refers to the art and science of hiding secret information in some other media. The information to be hided is called the secret message and the medium in which the information is hided is called the cover media. The cover media (which is in our paper is a color image) containing hidden message is called stego-image. The algorithms employed for hiding the message in the cover medium at the sender end and extracting the hidden message from the stego-image at the receiver end is called stego system.

For comparative analysis of steganography techniques some parameters are used such as MSE, PSNR, inserting time needed to hide a massage in color image, and extracting time needed to extract the message from the covering color image.

PSNR- Peak signal to noise ratio is calculated usually in logarithmic (dB) scale is a metric use to measure the quality of any image reconstructed, restored or corrupted image with respect to its reference or ground truth image. It is a full reference image quality measure defined as the maximum value of maximum signal power with respect to MSE (Mean square error) assumed as noise power. Similarly MSE can be calculated as the square difference between reference image and reconstructed image. Thus a higher value of PSNR indicates that the image is of higher quality and vice-versa. A 20 dB or higher PSNR indicates that the image is of good quality.

$$MSE = \frac{1}{mn}\sum_{0}^{m-1}\sum_{0}^{n-1}\|f(i,j) - g(i,j)\|^2 \quad (1)$$

$$PSNR = 20\log_{10}\left(\frac{MAX_f}{\sqrt{MSE}}\right) \quad (2)$$

Formula 1 is used to calculate PSNR, while formula 2 is used to calculate MSE

Where:

f represents the matrix data of our original image, **g** represents the matrix data of our degraded image in question' **m** represents the numbers of rows of pixels of the images and i represents the index of that row **n** represents the number of columns of pixels of the image and j represents the index of that column $\mathbf{MAX_f}$ is the maximum signal value that exists in our original "known to be good" image.

2- Related works

Shikha and Vidhu Kiran Dutt in [5] proposed a technique (let us call it P1) which encodes a text message using a key. This works by using the ascii number representation of the characters in the key (and certain permutations) to create coordinate pairs that represent the places in matrix (which is a sub matrix of the matrix representing the cover image) where the unit alterations to the image matrix will be made. R.Amirtharajan and others in[6] proposed another technique for image steganography which was called **MOD10** method which hides the data in the remainder obtained by dividing the gray value of the pixel by 10. This method has a key which determines whether the data is same as the remainder or 10-remainder. The key improves the quality of the stego-image.

Deferent various method of image steganography are based on least-significant-bits (LSBs) or on its substitution [7] and here we will review some of these methods:

1. **Optimum Pixel Adjustment Procedure** [8], reduces the distortion caused by the LSB substitution method. The pixel value is adjusted after the hiding of the secret data is done to improve the quality of the stego image without disturbing the data hidden.
2. **Inverted Pattern Approach**[9] Is LSB substitution approach uses the idea of processing secret messages prior to embedding. In this method each section of secret images is determined to be inverted or not inverted before it is embedded. In addition, the bits which are used to record the transformation are treated as secret keys or extra data to be re-embedded.
3. **IP Method Using Relative Entropy [9],** this method used Relative entropy to measures the information discrepancy between two different sources with an optimal threshold obtained by minimizing relative entropy. In this method instead of finding the mean square error for inverted pattern approach, the relative entropy is calculated to decide whether S or S‘ suites the pixel.
4. **Pixel Value Differencing (PVD) [10]**, in this method Pixel Value differencing is able to provide a high quality stego-image in spite of the high capacity of the concealed information. That is, the number of

insertion bits is dependent on whether the pixel is an edge area or smooth area. In edge area the difference between the adjacent pixels is more, whereas in smooth area it is less. While human perception is less sensitive to subtle changes in edge areas of a pixel, it is more sensitive to changes in the smooth areas.

3- The proposed method

All LSB methods of hiding message in color image are simple but they are not highly secure and they need an extra work to add an encryption tool to increase the security of hidden information, thus the proposed method can be used to hide short messages within a color image taking in consideration achieving best performance by providing a high secure of message hiding and extracting within a minimum time of processing.

The following sequence op operations can be used to implement the proposed method:

a- Inserting the message into the cover image:

1. Get the cover color image.
2. Retrieve the cover image size.
3. Calculate the max index size(MIS=row*columns*3).
4. Get the message length(L).
5. Reshape the cover image to 1 column matrix.
6. Generate a private random key of indexes within the range 1 to MIS and length=L.
7. Save the private key.
8. Use the indexes of the private key to insert the message into the cover matrix.
9. Reshape the cover matrix again to 3 dimensional matrix.

b- Retrieving the message from the image:

1. Get the cover image
2. Reshape the cover image to 1 column matrix.
3. Use the private key to get the indexes of the message within the image.
4. Retrieve the message.

4- Implementation and results discussion

The following matlab code was written to implement the proposed method:

```
close all, clear all, clc
a=imread('peppers.png');
subplot(2,2,1)
imshow(a), title 'Original image'
subplot(2,2,2)
imhist(a(:,:,1)), title 'Red histogram'
subplot(2,2,3)
imhist(a(:,:,2)), title 'Green histogram'
subplot(2,2,4)
imhist(a(:,:,3)), title 'Bkue histogram'
tic
[n1 n2 n3]=size(a);
b=reshape(a,n1*n2*n3,1);
%get the massage
st='Text hiding';
n4=length(st);
ss=n1*n2*n3;
pos=rand(1,n4);
pos=fix(pos*ss);
for i=1:n4
  cc=pos(1,i);
  b(cc,1)=st(i);
end
bb=reshape(b,n1,n2,n3);
toc
figure,
subplot(2,2,1)
imshow(bb), title 'Covering image'
subplot(2,2,2)
imhist(bb(:,:,1)), title 'Red histogram'
subplot(2,2,3)
imhist(bb(:,:,2)), title 'Green histogram'
subplot(2,2,4)
imhist(bb(:,:,3)), title 'Bkue histogram'
tic
for i=1:n4
  cs=pos(1,i);
```



```
   st1(i)=b(cs,1);
end
toc
char(st1)
```

The proposed method was implemented using the color image 'peppers.png' as a covering image. Table 1 shows the indexes of a message length=11.

Table 1: Indexes for the message 'Text hiding'

Message character	Location(index)
T	409672
e	366463
x	468804
t	564369
	308236
h	519128
I	102013
D	577878
i	160106
n	148829
g	516533

The same covering image was used to hide messages with deferent length and the results of implementation are shown in table 2.
A matlab programs also were written to implement the other methods of image Stegsnography and the results of implementation are shown in tables 3m 3, and 4.

Table 2: Comparison parameters for the proposed method

Text length	MSE	PSNR	Time to insert text(TIT) Sec.	Time to extract text(TET) Sec.	Total time(TT) Sec.
10	0.0484	218.7246	0.000096	0.001888	0.0020
20	0.0496	216.1664	0.000097	0.002132	0.0022
30	0.0665	186.6899	0.000133	0.003421	0.0036
40	0.1835	112.3540	0.000930	0.003920	0.0049
50	1.0581	46.7905	0.000940	0.004070	0.0050

Table 3: Comparison parameters LSB method

Text length	MSE	PSNR	Time to insert text(TIT) Sec.	Time to extract text(TET) Sec.	Total time(TT) Sec.
10	0	Inf	0.062000	0.000112	0.0621
20	0	Inf	0.06200	0.016000	0.0780
30	0	Inf	0.062000	0.016000	0.0780

40	0	Inf	0.063000	0.016000	0.0790
50	0	Inf	0.063000	0.016000	0.0790

Table 4: Comparison parameters for the P1 method

Text length	**MSE**	**PSNR**	**Time to insert text(TIT) Sec.**	**Time to extract text(TET) Sec.**	**Total time(TT) Sec.**
10	1.6954e-004	3.6964e+003	0.109000	0.140000	0.2490
20	1.6954e-004	3.6964e+003	0.109000	0.125000	0.2340
30	1.6954e-004	3.6964e+003	0.140000	0.141000	0.2810
40	1.6954e-004	3.6964e+003	0.141000	0.141000	0.2810
50	1.6954e	3.6964e+003	0.141000	0.141000	0.2810

From these tables we can see that PSNR is greater than 20, which means that the covering image is in good quality as illustrated in figure 1 and 2.

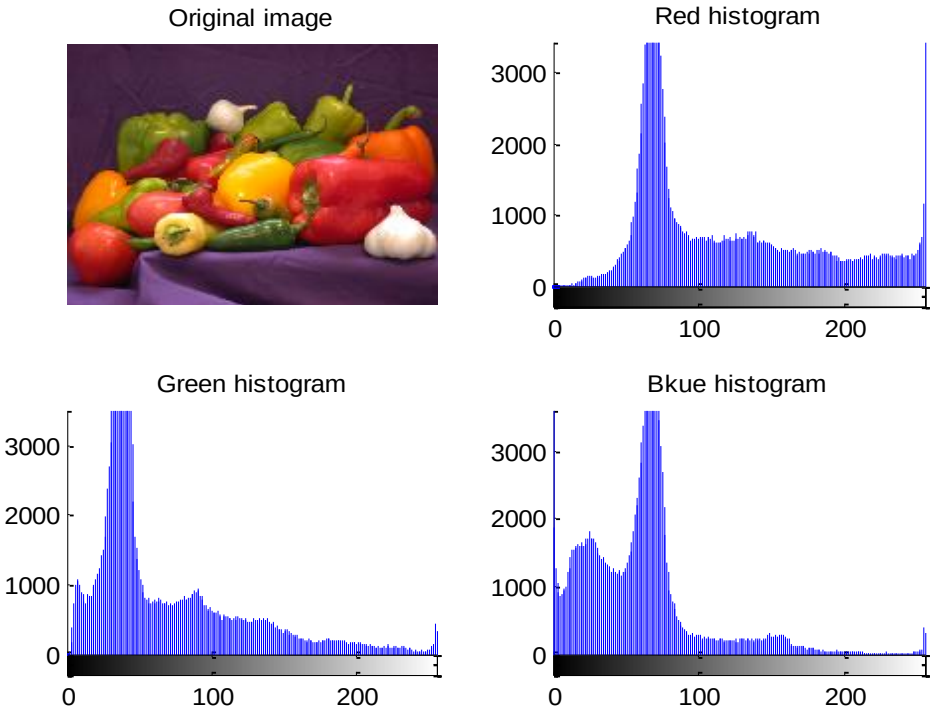

Figure 1:Original image and its histograms

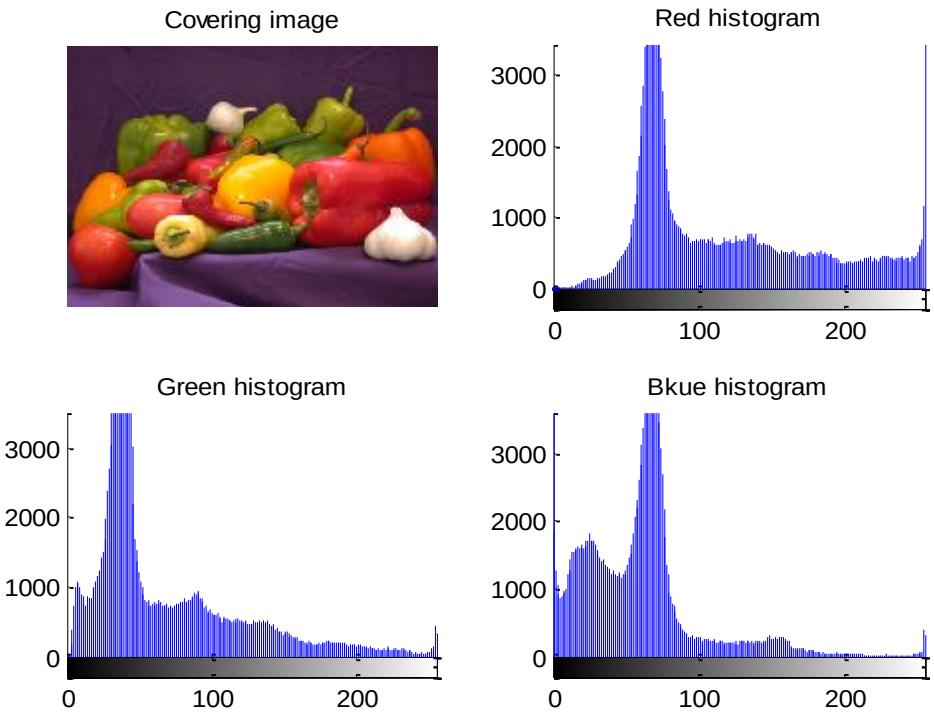

Figure 2:Covering image and its histograms

From table 2, 3 and 4 we can see that proposed method has an advantages over the other two methods by reducing the time needed to hide and extract the message, figure 3 show the time enhancement using the proposed method.

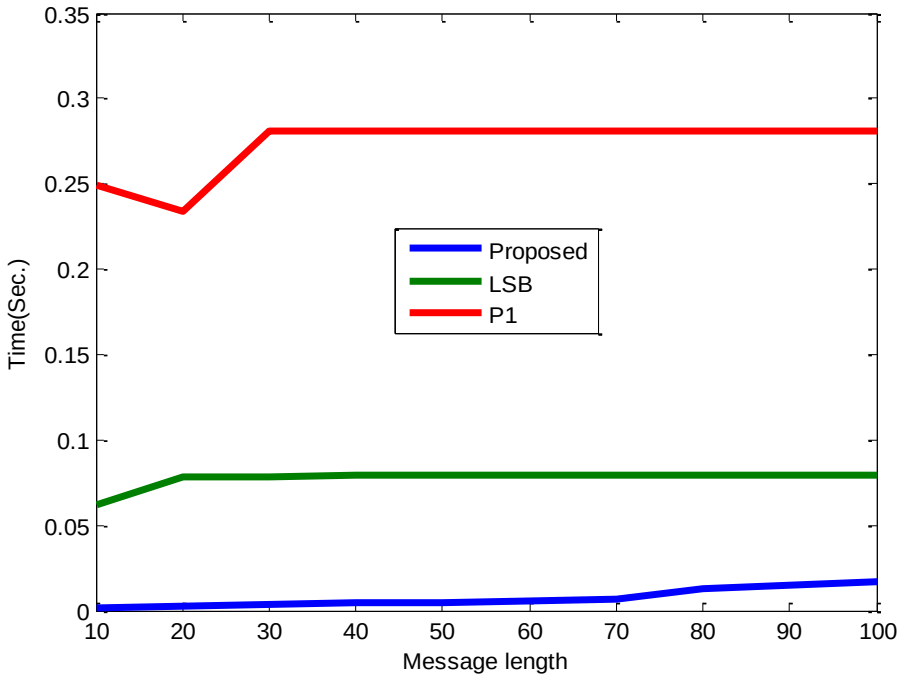

Figure 3: Proposing time.

Other matlab codes were written for other available methods to show the performance of the proposed method. Table 5 shows the implementation results using a short message with length:=50 characters.

Table 5 : Implementation results

Method	**Total time for hiding text and extracting**	**Speed up**
Proposed	0.0050	1
OPAR	0.0151	3.0200
IPA	0.0153	3.0600
IAPIPURE	0.0178	3.5600
MOD10	0.0241	4.8200
PVD	0.0408	8.1600
LSBV	0.0790	15.8000
P1	0.2810	56.2000

Conclusions

A method for image Steganography was proposed implemented and tested, It was shown from the obtained results that covering image always has a good quality And has a high value of PSNR, thus it is difficult to guess whether the covering image is differ from the original one.

It was also shown that the proposed method has a good performance comparing with other methods of image Steganography, and it was shown that the proposed method has a good speed up.

References

[1]. Bruice Schneier, Applied Cryptography Protocols, Algorithm and Source Code in C. Second edition. Wiley India edition 2007.
[2]. Yuan-Hui Yu , Chin-Chen Chang, Iuon-Chang Lin, A new steganographic method for color and grayscale image hiding Computer Vision and Image Understanding 107 (2007) 183–194
[3]. W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "*Techniques for data hiding*", IBM Systems , vol. 35, Issues 3&4 1996 Journal, pp. 313-336.
[4]. Souvik Bhattacharyya and Gautam Sanyal. *An image based Steganography model for promoting global cyber security*. In, 2009 Proceedings of International Conference on Systemic, Cybernetics and Informatics, Hyderabad, India.
[5]. Shikha and Vidhu Kiran Dutt, Steganography: The Art of Hiding Text in Image using Matlab, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 9, September 2014
[6]. R.Amirtharajan, R. Akila, P.Deepikachowdavarapu, A Comparative Analysis of Image Steganography, *International Journal of Computer Applications (0975 – 8887)*
Volume 2 – No.3, May 2010.
[7]. R.Z. Wang, C.F. Lin, J.C. Lin, Image hiding by optimal LSB substitution and genetic algorithm, Pattern Recognition 34 (3) (2000) 671–683.
[8]. C.K. Chan, L.M. Chen, Hiding data in images by simple LSB substitution, Pattern Recognition 37 (3) (2004) 469–474.
[9]. C.H. Yang, Inverted pattern approach to improve image quality of information hiding by LSB substitution Pattern Recognition 41 (2008) 2674–2683.
[10]. C.C. Thien, J.C. Lin, A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function, Pattern Recognition 36 (11) (2003) 2875–2881.

