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. 6, Issue. 4, April 2017, pg.142 – 150

Effective and Secure Method of Color Image Steganography

Omar M. Albarbarawi

Albalqa Applied University, Faculty of Engineering Technology, Jordan-Amman

Abstract: ***An efficient and secure method of hiding secret message-extracting embedded message into/from a color image will be proposed. The proposed method will be tested, implemented and analyzed. Different secrete messages with different length will be selected and embedded into color images with different sizes. Efficient, quality, and security issues will be done to prove the advantages of the proposed method.***

Keywords: Efficiency, quality, security, MSE, PSNR.

1- Introduction

RGB color image is a three dimensional matrix [1], [2]; the first dimension is for the red components, the second for the green components, while the third is for the blue component. RGB color image usually has a huge size, so it is convenient to use this image to hold a secrete message, and this process is called image steganography [3], [4], [5].

The data to be hided is called the secret message and the medium in which the data is hided is called the covering media. The covering media (which is in our paper is a color image) containing hidden message is called stego-image (holding 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.

The process of image steganography as shown in figure 1 can be implemented in 2 phases [6], [7], [8]:

- ✓ Phase 1:

Embedding the secret message based on the private key used to insert the message in the covering image.

- ✓ Phase 2:

Extracting secret message from the holding image based on the private key.

For comparative analysis of steganography techniques some parameters are used such as MSE, PSNR, embedding 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) (equation 1)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 (equation 2) 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 [3], [9].

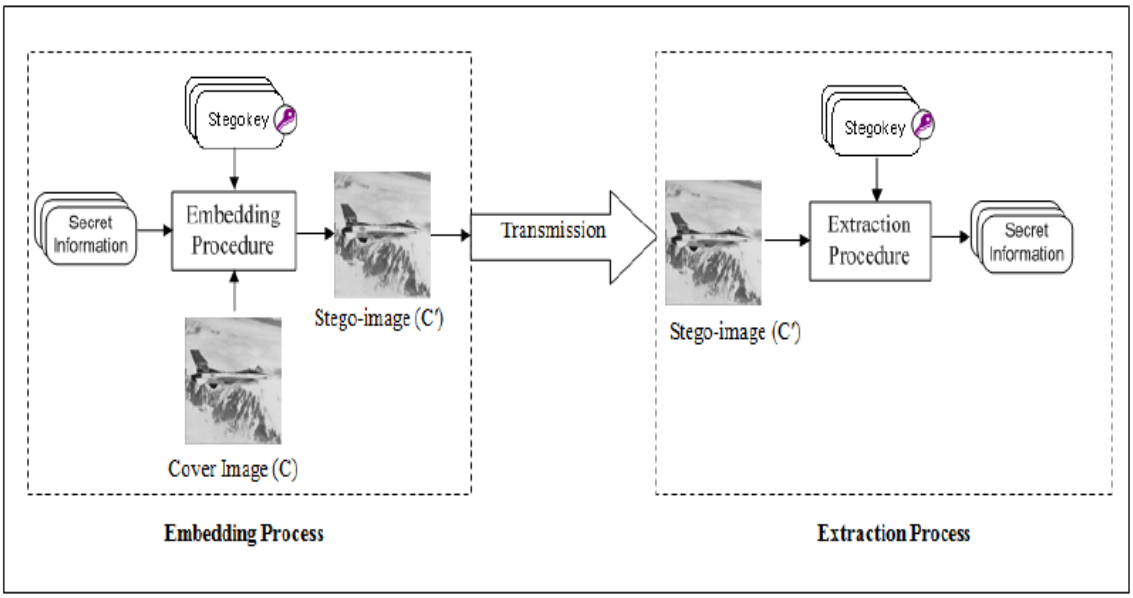

Figure 1: Steganography process

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

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

The PSNR value approaches infinity as the MSE approaches zero; this shows that a higher PSNR value provides a higher image quality. At the other end of the scale, a small value of the PSNR implies high numerical differences between images.
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.

2- The Proposed Method

Many methods [9],[10],[11] were proposed for secrete message hiding, mostly they are based on least significant bit (LSB) method , all these 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 proposed method here came to increase the security level, minimize the embedding and extracting time keeping the level of holding image quality closed to that one obtained by any other method.
The proposed method can be implemented applying the following steps:

- ✓ Phase 1: Embedding secrete message:

This phase can be implemented by executing the following sequence of operations:

1. Get the covering color image.
2. Get the size of each of the three color components (n1: number of rows; n2: number of columns).
3. Get the secrete message.
4. Get the length of the secrete message (n4).
5. Divide the message into three sub-messages.
6. Generate 3 random private keys: Red, green and blue keys, each key will contain the position in color component where to hide a character from the sub-message.
   These keys can be implemented applying the following formulas:

```
Kxred=floor (rand (1, ceil (n4/3))*n1);
Kyred=floor (rand (1, ceil (n4/3))*n2);
Kxgreen=floor (rand (1, ceil (n4/3))*n1);
Kygreen=floor (rand (1, ceil (n4/3))*n2);
Kxblue=floor (rand (1, ceil (n4/3))*n1);
Kyblue=floor (rand (1, ceil (n4/3))*n2);
```

7. Save the keys.
8. Use the positions in the keys to insert (hide) each sub-message in the corresponding color component.

- ✓ Phase 2: Extracting secrete message

This phase can be implemented applying the following sequence of operations:

1. Get the holding color image.
2. Separate the image into three components.
3. Get the private key.
4. Use the private keys to extract the sub-messages from each component.
5. Construct the secret messages from the three sub-messages.

3- Experimental Results and Analysis

3-1 Quality Analysis

The proposed method was implemented several times using various length messages and various size color images and the experimental results showed that it is very difficult to distinguish the difference between them using the human eye this is show in figures 2 to 5:

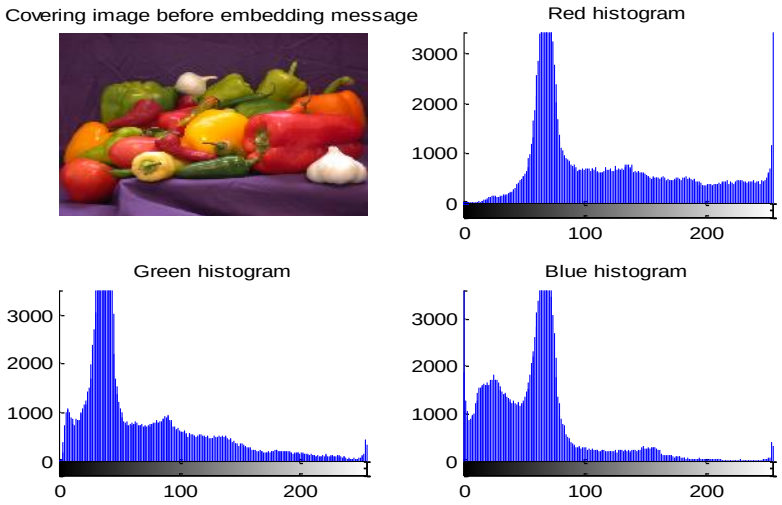

Figure 2: Original image (png with size 384x512x3)

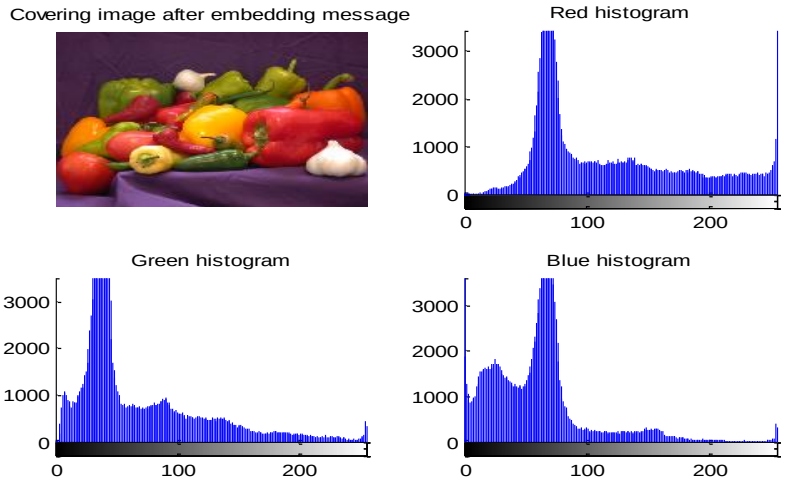

Figure 3: Holding image (message length=42)

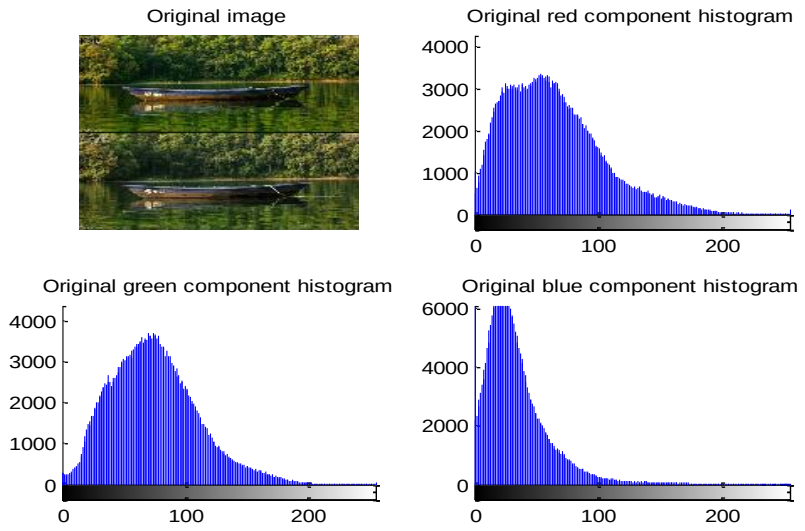

Figure 4: Original image (jpg with size 516x600x3)

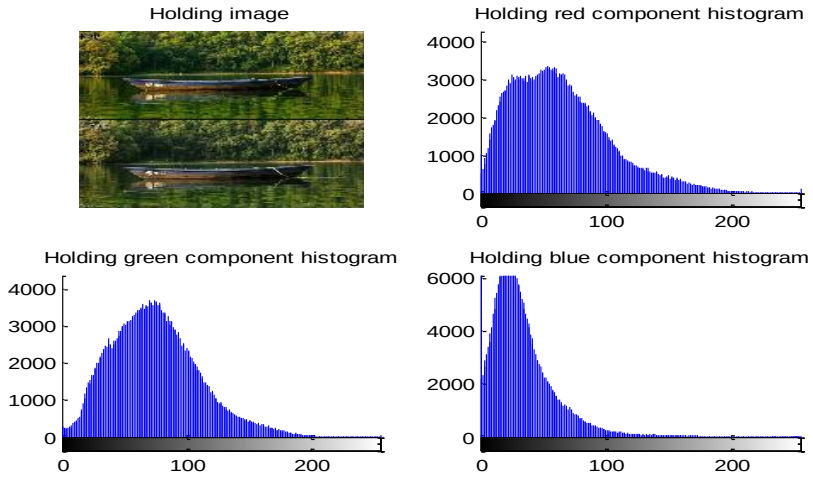

Figure 5: Holding image (message length=42)

The experimental results shown in tables 1 and 2 showed that the proposed method provides a high quality by giving a high value of PSNR and a low value of MSE.

Table 1: Calculated parameters using Png image with size=384x512x3

Message length	Embedding time(second)	Extraction time(second)	MSE	PSNR
10	0.000001	0.000001	0.0445	141.9392
20	0.000001	0.000001	0.1968	127.0797
30	0.000001	0.000001	0.2043	126.7078
40	0.000001	0.000001	0.2817	123.4927
50	0.000001	0.000001	0.4798	118.1682
60	0.000001	0.000001	0.5273	117.2244
70	0.000001	0.000001	0.5633	116.5651
80	0.000001	0.000001	0.6338	115.3851
90	0.000001	0.000001	0.6842	114.6209
100	0.000001	0.000001	0.8576	112.3610

Table 2: Calculated parameters using jpg image with size=516x600x3

Message length	Embedding time(second)	Extraction time(second)	MSE	PSNR
10	0.000023	0.000023	0.0435	142.1677
20	0.000023	0.000023	0.1131	132.6192
30	0.000023	0.000023	0.1488	129.8755
40	0.000023	0.000023	0.2104	126.4140
50	0.000023	0.000023	0.2320	125.4345
60	0.000023	0.000023	0.2452	124.8806
70	0.000023	0.000023	0.3500	121.3237
80	0.000023	0.000023	0.3535	121.2253
90	0.000023	0.000023	0.3848	120.3757
100	0.000023	0.000023	0.4858	118.0441

From tables 1 and 2 we can see that the proposed method gives a high quality by achieving a high value of PSNR and a low value of MSE. Here we have to notice that PSNR will grow with the holding image size, and will be decreased when increasing the secrete message length(but still acceptable because of the high value of PSNR) this is shown in figure 6 and 7.

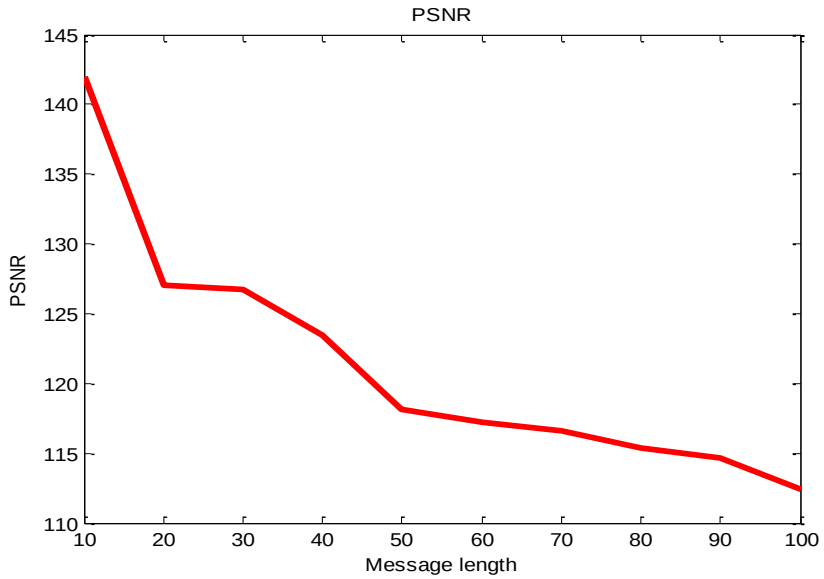

Figure 6: Relationship between PSNR and message length

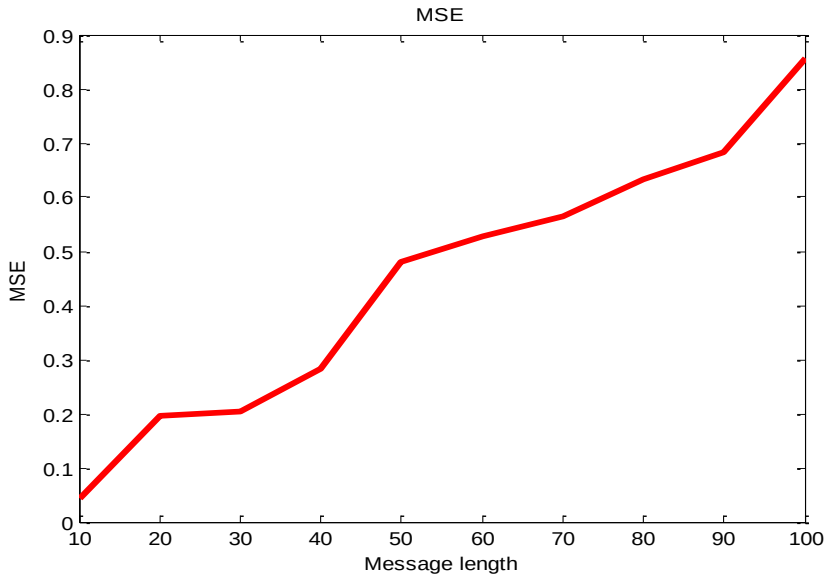

Figure 7: Relationship between MSE and message length

3-2 Security Analysis

The proposed method uses a private key to hide a secrete message and uses the same key to extract the secrete message from the holding image. This key is to be generated randomly and it will contain a set of pairs, each of them points to a coordinate in color image component where the character from the secrete message to be embedded, thus making the process of hacking (guessing) the key impossible, thus increasing the level of security. Table 3 shows the key used to hide a message of 12 character length in an image of 516x600x3 size.

Table 3: Private Key of message hiding

Color image component	First character	Second character	Third character	Fourth character
Red positions	(151, 259)	(115, 379)	(282, 357)	(445, 201)
Green positions	(367, 264)	(170, 161)	(214, 340)	(98, 74)
Blue positions	(448, 509)	(318, 589)	(59, 372)	(313, 332)

3-3 Performance Analysis

Table 1 and 2 show the times needed to hide and to extract secrete message these times are very small comparing with LSB method of data hiding, table 4 shows a comparisons between the proposed method results and LSB method results:

Table 4: Results comparisons

Parameter	LSB method	Proposed method
PSNR	170.8569	118.0441
MSE	0.0025	0.4858
Hiding time(second)	0.072000	0.000023
Extracting Time	0.042000	0.000023
Speed up(LSB time/Proposed time) embedding	3130.4	
Speed up(LSB time/Proposed time) extracting	1826.1	

Conclusions

A method of color image steganography was proposed, tested and implemented. The experimental results showed that the proposed method is very secure, provides a high quality and high performance. It was shown from the obtained results that the 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.

References

[1]. Jihad Nadir, Ziad Alqadi and Ashraf Abu Ein, Classification of Matrix Multiplication Methods Used to Encrypt-decrypt Color Image, International Journal of Computer and Information Technology (ISSN: 2279 – 0764) Volume 05 – Issue 05, September 2016.
[2]. Majed O. Al-Dwairi, Ziad A. Alqadi, Amjad A. AbuJazar and Rushdi Abu Zneit, Optimized True-Color Image Processing, World Applied Sciences Journal 8 (10): 1175-1182, 2010 ISSN 1818-4952.
[3]. Prof. Ziad A.A. Alqadi, Prof. Mohammed K. Abu Zalata, Ghazi M. Qaryouti, Comparative Analysis of Color Image Steganography, *IJCSMC, Vol. 5, Issue. 11, November 2016, pg.37 – 43.*
[4]. Bruice Schneier, Applied Cryptography Protocols, Algorithm and Source Code in C. Second edition. Wiley India edition 2007.
[5]. 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
[6]. 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.
[7]. 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.
[8]. 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
[9]. Mekha Jose, Hiding Image in Image Using LSB Insertion Method with Improved Security and Quality, International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064.
[10]. Reena M Patel,D J Shah , "Concealogram : Digital image in image using LSB insertion method", International journal of electronics and communication engineering & technology(IJECET), 2013.
[11]. Nadeem Akhtar, Pragati Johri, Shahbaaz Khan, "Enhancing the security and quality of LSB based image steganography", 2013 5th International Conference on Computational Intelligence and Communication Networks.

