British Journal of Mathematics & Computer Science
10(1): 1-9, 2015, Article no.BJMCS.17628
ISSN: 2231-0851

SCIENCEDOMAIN *international*
www.sciencedomain.org

Stego-Scheme for Secret Communication in Grayscale and RGB Images

Aqsa Rashid[1*] and Muhammad Khurrum Rahim[2]

[1]Department of Computer Science and Information Technology, The Islamia University of Bahawalpur, Rahim Yar Khan, Pakistan.
[2]Department of Electrical Engineering, National University Computer and Emerging Sciences, Islamabad, Pakistan.

Article Information

DOI: 10.9734/BJMCS/2015/17628
Editor(s):
(1) Victor Carvalho, Polytechnic Institute of Cávado and Ave, Portuguese Catholic University and Lusiada University, Portugal.
Reviewers:
(1) Anonymous, Al-Zaytoonah University of Jordan, Jordan.
(2) Anonymous, Universiti Sains Malaysia, Malaysia.
Complete Peer review History: http://sciencedomain.org/review-history/9917

Original Research Article

Received: 20 March 2015
Accepted: 07 April 2015
Published: 27 June 2015

Abstract

This paper presents the new technique of the spatial domain image steganography for hidden electronic communication in grayscale and color images. The method hide one message bit per pixel and creates least changes in the statistical properties of the image. Experimental results, for the projected method, show the excellence of the method. The projected method is also implemented for two bits per pixel, three bits per pixel, four bits per pixel, five bits per pixel, six bit per pixel, seven bit per pixel and eight bits per pixel using the same concept. At the end the results shows that the method is good up to three bits per pixel.

Keywords: Communication; digital image; grayscale; electronic; mod function; RGB image; steganography; spatial domain.

1 Introduction

Steganography is the technique or execution of hiding a message, image, file or video inside a new message, image, file or video. The word "*steganography"* is mingling of two Greek words, *steganos* (στεγανός), means secret, hidden or private, and *graphein* (γράφειν) means text or writing. In current age of digital era, steganography is a gifted technique for secure transmission of data over the internet.

In this paper a method of image steganography is presented that uses the mod function and hide one message bit per pixel. This creates the least change in image statistics. In some other method the mod function is used

**Corresponding author: aqsarashid2@gmail.com;*

on the combination of specific bits but in this paper instead of specific bits, it uses the whole pixel value. Projected method is also implemented for hiding two, three, four, five, six, seven and eight bits and compares the results.

The rest of the paper is arranged as second section includes literature review, third gives the algorithm of the projected method, fourth section gives the analysis of the projected method for all the possible 256 shades, fifth section gives the experimental results and discussion, sixth section includes conclusion and references are listed in the last of the paper.

2 Literature Review

During the past year lots of methods of the steganography have been projected [1,2,3,4] Literature reviews of some spatial domain steganographic methods are mention below:

Least significant bit (LSB) substitution [5] is also known as flipping method. It directly applies the process of replacement if the message bit and least significant bit of the pixel are not identical. The process of replacement is also known as flipping.

Least significant bit (LSB) Matching [5,6] uses the adjustment process for embedding the message bit. Adjustment is performed in the form of increment and decrement.

Increased Capacity Stego-Scheme [7] simply increase the capacity of hiding data by using both the substitution and matching method. It applies the matching method on the second least significant bit and substitution on least significant bit.

Electronic Communication Scheme in Spatial Domain [8] uses the mod function on the specific bits to embed the secret message bits.

All above methods are simple, effective and good methods of steganography. But if they are to be implemented for two or three bits the result are not as good as the projected method gives.

3 Methodology

In this paper, instead of using specific bits, the defined mod function is implemented on the whole pixel.

Formal steps of embedding are following:

a. Take the pixel value.
b. Find the mod of pixel by 2^a as mod factor where a =1, 2, 3, 4, 5, 6, 7 and 8 depending on the number of bits to embed per pixel.
c. If the message bit and binary of mod value are equal then no adjustment is required otherwise adjustment will be performed to make message bit and binary of mod value equivalent.
d. End

Formal steps for extraction steps are:

a. Take the pixel value.
b. Find the mod of pixel by 2^a as mod factor where a =1, 2, 3, 4, 5, 6, 7 and 8 depending on the number of bits to embed per pixel.
c. The binary equivalents of the mod value are the message bit.
d. If the length of the message bits is completed then go to (e) else go to (a).
e. End

4 Analysis of Projected Method

The main logic behind the projected method is that only the binary equivalents of the mod value require no adjustment otherwise process of adjustment is to be performed in the form of increment or decrement in the pixel vale. For example if we want to embed one bit per pixel and the mod value is 0 then only 0 can be embed without adjustment. Similarly if we want to embed two bits per pixel and the mod value is 3 then only the binary of three, which is 11, can be embed without adjustment. Below is a detail analysis of all the possibilities for embedding 1, 2, 3, 4, 5, 6, 7, and 8 bits per pixel.

Table 1 show the analysis of projected method for hiding one bit per pixel. In this case the mod factor will be 2 as the hidden capacity is one bit per pixel.

Table 1. Embedding of 1 bit per pixel

Pixel value	Mod value	Message bit without adjustment	Message bit with adjustment
0	0	0	1
1	1	1	0
2	0	0	1
3	1	1	0
.	.	.	.
.	.	.	.
254	0	0	1
255	1	1	0

Table 2 shows the analysis of projected method for hiding two bits per pixel. In this case the mod factor will be 4 as the hidden capacity is two bits per pixel.

Table 2. Embedding of 2 bits per pixel

Pixel value	Mod value	Message bit without adjustment	Message bits with adjustment
0	0	00	01, 10, 11
1	1	01	00, 10,11
2	2	10	00, 01, 11
3	3	11	00, 10, 01
4	0	00	01, 10, 11
5	1	01	00, 10, 11
.	.	.	.
.	.	.	.
252	0	00	01, 10, 11
253	1	01	00, 10, 11
254	2	10	00, 01, 11
255	3	11	00, 01, 10

Table 3 shows the analysis of projected method for hiding three bits per pixel. In this case the mod factor will be 8 as the hidden capacity is three bits per pixel.

Table 3. Embedding of 3 bits per pixel

Pixel value	Mod value	Message bit without adjustment	Message bits with adjustment
0	0	000	001,010,011,100,101,110,111
1	1	001	000,010,011,100,101,110,111
2	2	010	000,001,011,100,101,110,111
3	3	011	000,001,010,100,101,110,111
4	4	100	000,001,010,011,101,110,111
5	5	101	000,001,010,011,100,110,111
6	6	110	000,001,010,011,100,101,111
7	7	111	000,001,010,011,100,101,110
8	0	000	001,010,011,100,101,110,111
9	1	001	000,010,011,100,101,110,111
.	.	.	.
.	.	.	.
254	6	110	000,001,010,011,100,101,111
255	7	111	000,001,010,011,100,101,110

Table 4 shows the analysis of projected method for hiding four bits per pixel. In this case the mod factor will be 16 as the hidden capacity is 4 bits per pixel.

Table 4. Embedding of 4 bits per pixel

Pixel value	Mod value	Message bit without adjustment	Message bits with adjustment
0	0	0000	0001,0010,0011,0100,0101,0110,0111 1000,1001,1010,1011,1100,1101,1110,1111
1	1	0001	0000,0010,0011,0100,0101,0110,0111 1000,1001,1010,1011,1100,1101,1110,1111
2	2	0010	0000,0001,0011,0100,0101,0110,0111 1000,1001,1010,1011,1100,1101,1110,1111
3	3	0011	0000,0001,0010,0100,0101,0110,0111 1000,1001,1010,1011,1100,1101,1110,1111
.	.	.	.
.	.	.	.
14	14	1110	0000,0001,0010,0011,0100,0101,0110,0111 1000,1001,1010,1011,1100,1101,1111
15	15	1111	0000,0001,0010,0011,0100,0101,0110,0111 1000,1001,1010,1011,1100,1101,1110
16	0	0000	0001,0010,0011,0100,0101,0110,0111 1000,1001,1010,1011,1100,1101,1110,1111
17	1	0001	0000,0010,0011,0100,0101,0110,0111 1000,1001,1010,1011,1100,1101,1110,1111
.	.	.	.
.	.	.	.
254	14	1110	0000,0001,0010,0011,0100,0101,0110,0111 1000,1001,1010,1011,1100,1101,1111
255	15	1111	0000,0001,0010,0011,0100,0101,0110,0111 1000,1001,1010,1011,1100,1101,1110

Table 5 shows the analysis of projected method for hiding five bits per pixel. In this case the mod factor will be 32 as the hidden capacity is five bits per pixel.

Table 5. Embedding of 5 bits per pixel

Pixel value	Mod value	Message bit without adjustment	Message bits with adjustment
0	0	00000	00001,00010,…., 11111
1	1	00001	00000,00010,…. ,11111
2	2	00010	00000,00001,00011,… ,11111
.	.	.	.
.	.	.	.
31	31	11111	00000,00001,00010,…,11110
32	0	00000	00001,00010,…., 11111
33	1	00001	00000,00010,…. ,11111
.			
.			
63	31		00000,00001,00010,…,11110
64	0		00001,00010,…., 11111
65	1		00000,00010,…. ,11111
.	.	.	.
.	.	.	.
255	31	11111	00000,00001,00010,…,11110

Table 6 shows the analysis of projected method for hiding six bits per pixel. In this case the mod factor will be 64 as the hidden capacity is six bits per pixel.

Table 6. Embedding of 6 bits per pixel

Pixel value	Mod value	Message bit without adjustment	Message bits with adjustment
0	0	000000	000001,000010,000011,…., 111111
1	1	000001	000000,000010,000011,…., 111111
2	2	000010	000000,000001,000011,…., 111111
.			
.			
62	62	111110	000000,000001,…,111100,111101,111111
63	63	111111	000000,000001,000010,….,111110
64	0	000000	000001,000010,000011,…., 111111
65	1	000001	000000,000010,000011,…., 111111
.	.	.	.
.	.	.	.
254	62	111110	000000,000001,…,111100,111101,111111
255	63	111111	000000,000001,000010,….,111110

Table 7 shows the analysis of projected method for hiding seven bits per pixel. In this case the mod factor will be 128 as the hidden capacity is seven bits per pixel.

Table 7. Embedding of 7 bits per pixel

Pixel value	Mod value	Message bit without adjustment	Message bits with adjustment
0	0	0000000	0000001,0000010,….,1111111
1	1	0000001	0000000,0000010,….,1111111
2	2	0000010	0000000,0000001,0000100,….,1111111
.	.	.	.
.	.	.	.
126	126	1111110	0000000,0000001,….,1111101,1111111
127	127	1111111	0000000,0000001,0000100,….,1111110
128	0	0000000	0000001,0000010,….,1111111
129	1	0000001	0000000,0000010,….,1111111
130	2	0000010	0000000,0000001,0000100,….,1111111
.	.	.	.
.	.	.	.
254	126	1111110	0000000,0000001,0000010,….,1111111
255	127	1111111	0000000,0000001,0000010,….,1111111

Table 8 shows the analysis of projected method for hiding eight bits per pixel. In this case the mod factor will be 256 as the hidden capacity is eight bits per pixel.

Table 8. Embedding of 8 bits per pixel

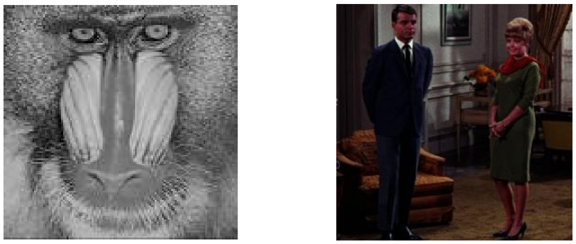
Pixel value	Mod value	Message bit without adjustment	Message bits with adjustment
0	0	00000000	00000001,00000010,…,11111111
1	1	00000001	00000000,00000010,….,11111111
2	2	00000010	00000000,00000001,0000011……, 11111110
.	.	.	.
.	.	.	.
254	254	11111110	00000000,00000001,……, 11111101,11111111
255	255	11111111	00000000,00000001, ……, 11111110

5 Results and Discussion

This section gives the experimental results of the projected method for grayscale and color images. It also include the results for two bits per pixel (2BPP), three bits per pixel (3BPP), four bits per pixel (4BPP), five bits per pixel (5BPP), six bits per pixel (6BPP), seven bits per pixel (7BPP) and eight bits per pixel (8BPP).

For the evaluation of the projected method, image are compared and tested by some well known parameters including visual appearance, mean square error (MSE), peak signal to noise ratio, universal image quality measure and structural similarity index measure (SSIM) [9,10,11,12,13,14].

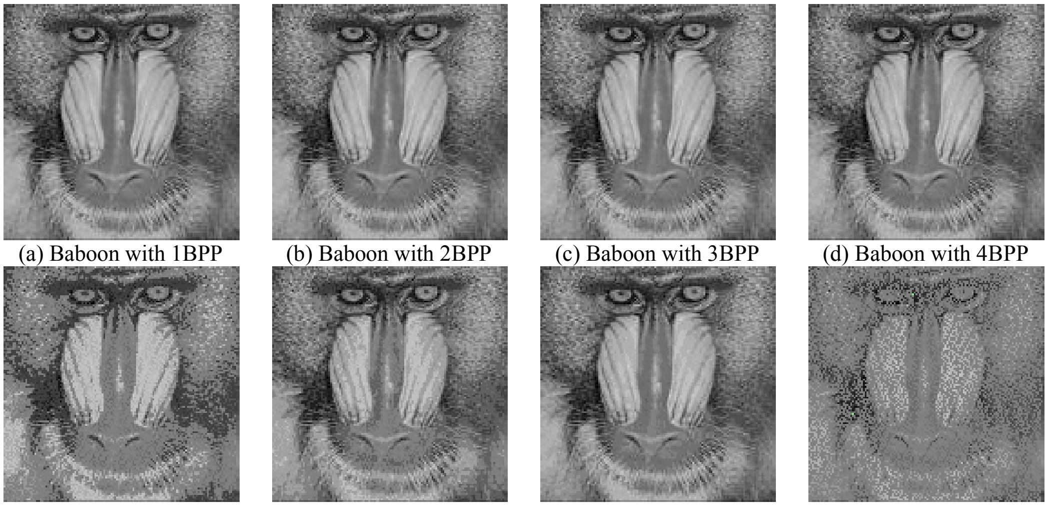
Fig. 1 shows the cover image used for experiments. (a) Shows the Baboon grayscale images and (b) is the Couple color image. Projected method is implemented and tested on many standard images but the result of two images are included in this paper.



(a) Baboon (b) Couple

Fig. 1. (a) is the Baboon images and (b) is the couple image

Fig. 2 shows the Baboon stego-images. (a-h) are the 1 to 8 bits per pixel stego-images.



(a) Baboon with 1BPP (b) Baboon with 2BPP (c) Baboon with 3BPP (d) Baboon with 4BPP

(e) Baboon with 5BPP (f) Baboon with 6BPP (g) Baboon with 7BPP (h) Baboon with 8BPP

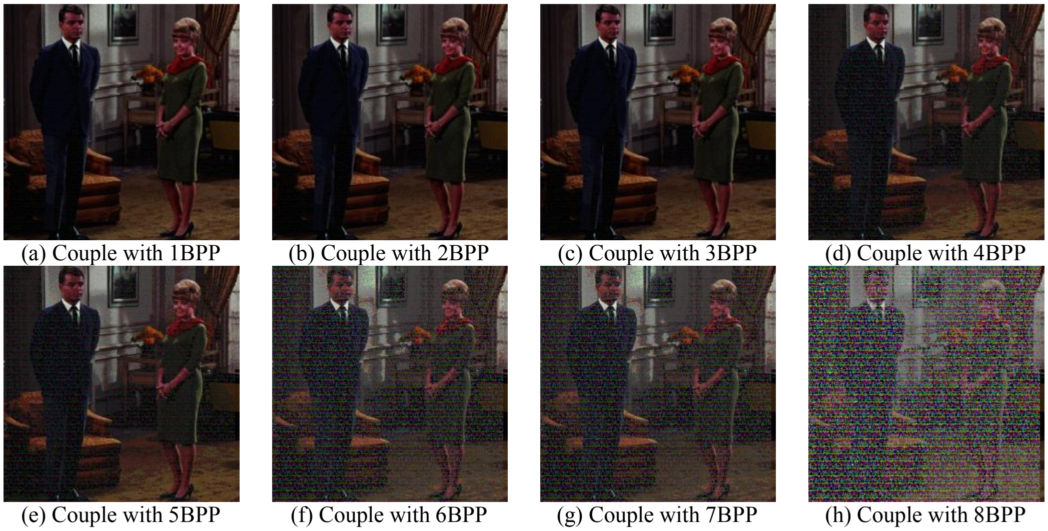
Fig. 2. Baboon stego-images

Fig. 3 shows the Couple stego-images. (a-h) are the 1 to 8 bits per pixel stego-images.

Table 9 shows the result of evaluation matrices used to check the effectiveness of the projected method for the Baboon image. The results are excellent for one and two bits per pixel and are good for three bits per pixel.

Table 9. Results of image quality measures for grayscale image

IQM	MSE	PSNR	UIQI	MSSIM
1BPP	0.4944	51.1534	0.9998	0.9998
2BPP	0.4985	51.1534	0.9998	0.9998
3BPP	1.2149	47.2851	0.9995	0.9995
4BPP	12.6359	37.1147	0.9952	0.9952
5 BPP	26.7133	34.0899	0.9862	0.9863
6BPP	50.7613	31.0754	0.9812	0.9812
7BPP	181.9650	25.5309	0.9364	0.9366
8BPP	676.3378	19.8388	0.6661	0.6673


(a) Couple with 1BPP (b) Couple with 2BPP (c) Couple with 3BPP (d) Couple with 4BPP

(e) Couple with 5BPP (f) Couple with 6BPP (g) Couple with 7BPP (h) Couple with 8BPP

Fig. 3. Couple stego-image

Table 10 shows the result of evaluation matrices used to check the effectiveness of the projected method for the Couple image. The results are excellent for one and two bits per pixel and are good for three bits per pixel.

Table 10. Results of image quality measures for color image

IQM	MSE	PSNR	UIQI	MSSIM
1BPP	0.0324	56.6589	0.9999	0.9999
2BPP	0.1425	54.3742	0.9998	0.9998
3BPP	2.0012	42.5126	0.9994	0.9995
4BPP	5.7685	40.7118	0.9970	0.9970
5 BPP	26.7133	34.0899	0.9862	0.9863
6BPP	140.86104	26.9757	0.9275	0.9278
7BPP	804.3863	19.4786	0.6664	0.6665
8BPP	4494.5318	11.1096	0.2185	0.2196

6 Conclusion

In this paper a new method of steganography is presented. Experimental results show that the projected method creates least changes in the image statistics which is invisible to human eye. Experimental results for two bits and three bits per pixel are also very good as compare to direct substitution of two or three message bits in pixel. The proposed method is implemented and tested on both the color and grayscale images. Almost 50 standard images are tested and results are compared. All these results and comparison shows that projected method is secure and can be used for secret transmission of data.

Competing Interests

Authors have declared that no competing interests exist.

References

[1] Poornima R, Iswarya RJ. An overview of digital image steganography. International Journal of Computer Science & Engineering Survey. 2013;4(1).

[2] Morkel T, Eloff THP, Olivier MS. An overview of image steganography. ICSA Research Group, Department of Computer Science; 2014.

[3] Jammi Ashok, Raju Y, Munishankaralak S, Srinivas K, Jammi Ashok. Steganography: An overview. et.01./ International Journal of Engineering Science and Technology. 2010;2(10):5985-5992.

[4] Shikha Sharda, Sumit Budhiraja. Image steganography: A review. International Journal of Emerging Technology and Advance Engineering. 2013;3(1).

[5] Aqsa Rashid. Experimental analysis and comparison of LSB substitution and LSB matching method of information security. IJCSI. 2015;12(1):1.

[6] Khurrum Rahim Rashid, Aqsa Rashid, Nadeem Salamat, Saad Missen. Experimental analysis of matching technique of steganography for Greyscale and colour image. International Journal of Computer Science & Information Technology (IJCSIT). 2014;6(6).

[7] Khurrum Rahim Rashid M, Nadeem Salamat, Saad Missen, Aqsa Rashid. Robust increased capacity image steganographic scheme. International Journal of Advanced Computer Science and Applications (IJACSA). 2014;5(11).

[8] Aqsa Rashid. Robust electronic communication scheme in spatial domain. BJMCS. 2015;7(3): 218-228.

[9] Rajkumar Yadav. Analysis of various image steganography techniques based upon PSNR metric. International Journal of P2P Network Trends and Technology. 2011;1(2). ISSN: 2249-2615.

[10] Pavani M, Naganjaneyulu S, Nagaraju C. A survey on LSB based steganography methods. International Journal of Engineering and Computer Science. 2013;2(8):2464-2467. ISSN: 2319-7242.

[11] Ismail Avcibas, Bulent Sankur, Khalid Sayood. Statistical evaluation of image quality measure. Journal of Electronic Imaging. 2002;11(2):206-223.

[12] Zhou Wang, Member, Hamid R. Sheikh. Image quality assessment: From error visibility to structural similarity. IEEE Transactions on Image Processing. 2004;13(4):1.

[13] Yousra A. Y. Al. Najjar, Dr. Soong DC. Comparison of image quality assessment. PSNR, HVS, UIQI, SSIM, IJSER. 2012;3(8). ISSN: 2229-5518.

[14] Amhamed Saffor, Abdul Rahman Ramli, Kwan-Hoong Ng. A comparative study of image compression between jpeg and wavelet. Malaysian Journal of Computer Science. 2001;14(1):39-45.

Peer-review history:
The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)
http://sciencedomain.org/review-history/9917