Experimental Review of Steganography Method that uses 5th, 6th and 7th Bit of a Pixel

Aqsa Rashid
Department of Computer Science & IT
The Islamia University of Bahawalpur, Pakistan

Muhammad Khurrum Rahim
Department of Electrical Engineering
NUCES, FAST, Pakistan

ABSTRACT
This paper is the detailed experimental analysis and review of the steganography method "A New Image Steganograpgy Approach for Information Secrity Using Gray Level Images in Spatial Domain" that uses 5th, 6th and 7th bit of the pixel for hiding message bit. In this paper it is implemented and analyzed for both, color and grayscale, images. For analysis and critical review, well known image quality measures, security analysis and some steganalysis method are used. The focal motivation of this paper is to provide in depth analysis of the selected method and test it with important measures for evaluating the distortion, performance, robustness and security.

General Terms
Security

Keywords
Bit Plane Analysis, IQM, LSB, Steganography, Security Analysis

1. INTRODUCTION
With the quick progress and extensive use of internet, information transmission faces confronts of security and unauthorized access of secret data [1]. In this situation steganography is considered as gifted approach. Its core use is to put out of sight the happening of communication in excess of a civic control. In disparity to cryptography, steganography have a tendency to conceal the presence of the message or communication appearance, while cryptography tries to hide the content of the clandestine message. Hiding the presence of message or communication can be made by inserting a clandestine message into the clear cover medium which no one besides the correspondent and the receiver can imagine.

1.1 Cover Medium used for Steganography
Different digital medium are used as cover medium for hiding the secret data. On the basis of medium, steganography is named accordingly. These include the following:

- **Image Steganography**: Steganography that uses image as cover medium is named as Image steganography. Secret data is embedded or concealed in the pixel data of the image.
- **Video Steganography:** In video steganography, secret data is concealed in video file format. A video file is defined as series or combination of images. Mp4, AVI, MPEG and other video format are used as cover object in video steganography.
- **Audio Steganography:** Audio file act as a cover medium in audio steganograogy. This medium has turn into very considerable medium due to VOIP (voice over IP) reputation.
- **Text Steganography:** In text steganography, white spaces, tabs, capital letters etc are used to complete the process of steganography.

This paper present the in depth analysis and review of the "A New Image Steganography Approach for Information Security Using Gray Level Images in Spatial Domain [2]". The rest of the paper is arranged as section 2 gives the methodology, section 3 gives experimental analysis, section 4 compares the selected method with the LSB substitution and LSB matching method of steganography, section 5 gives conclusion and references are in the last section.

2. METHODOLOGY
If 1 to 8 denotes the eight bits of the pixel of grayscale image then this method uses 5th, 6th and 7th bit in embedding and extraction process. For the decimal value of these bits, concept of even and odd is applied.

2.1 Embedding Algorithm
Formal embedding steps of the selected method are:

a. Take the pixel and check that if it is other than 0 or 255, as these are boundary pixel values (BPV) and will not take part in processing, then proceed to next step otherwise select next pixel by step (a).

b. Extract the 5th, 6th and 7th bit of the pixel.

c. Compute the decimal value of these bits.

d. If the decimal equivalent of the bit is 0, 2, 4 or 6 then only 0 can be embed without adjustment. Embedding of 1 in such case requires increment or decrement of 1 in pixel value.

e. If the decimal equivalent of the bit is 1, 3, 5 or 7 then only 1 can be embed without adjustment. Embedding of 0 in such case requires increment or decrement of 1 in pixel value.

2.2 Extraction Algorithm
Formal embedding steps of the selected method are:

a) Take the pixel and check that if it is other than 0 or 255, as these are boundary pixel values (BPV) and will not take part in processing, then proceed to next step otherwise select next pixel.

b) Extract the 5th, 6th and 7th bit of the pixel.

c) Compute the decimal value of these bits.

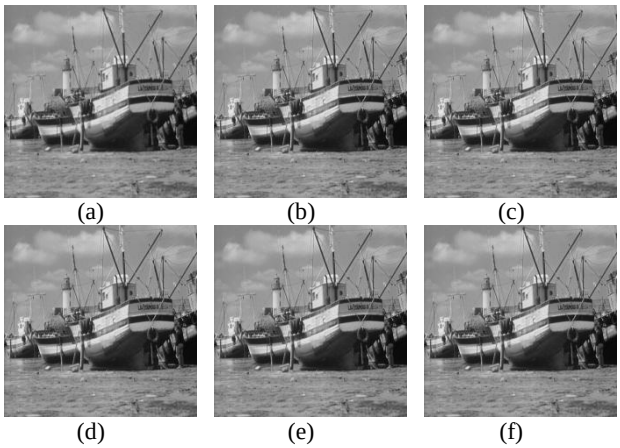
d) If the decimal equivalent of the bit is 0, 2, 4 or 6 then 0 is the message bit.

e) If the decimal equivalent of the bit is 1, 3, 5 or 7 then the message bit is1.

3. EXPERIMENTAL RESULTS AND DISCUSSION

This section presents the experimental result for the grayscale and color image.

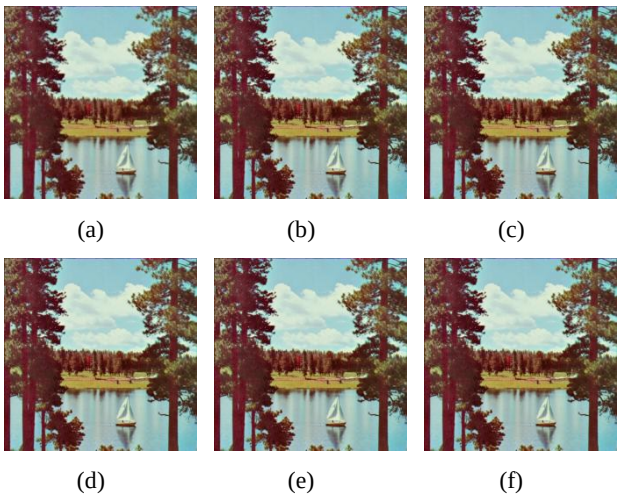
Fig. 1 show visual appearance of the grayscale Boat Cover and stego images used for experimentation. Stego images of Fig. 1 are produced by embedding different payload of secret message bits in the cover image. Figure 2 shows the visual appearance of cover and stego Sailboat on Lake Color image. From Fig. 1 and Fig. 2 it is clear that the visual appearance of stego images is undistinguishable by human perception as compare to cover image.



(a) (b) (c)

(d) (e) (f)

Fig 1: (a) Original Boat Image (b) Boat Stego image with 95832 bits (c) Boat Stego image with 80176 bits (d) Boat Stego image with 63688 bits (e) Boat Stego image with 54904 bits (f) Boat Stego image with 30280 bits

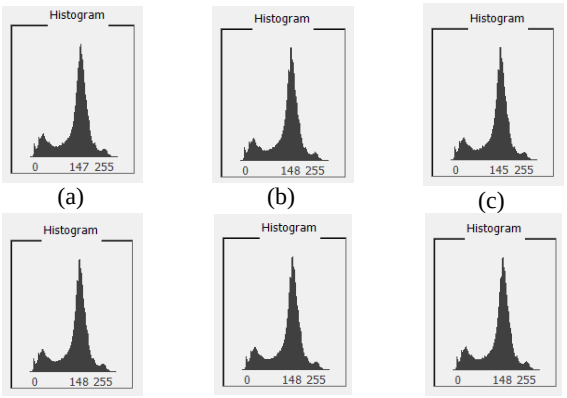


(a) (b) (c)

(d) (e) (f)

Fig 2: (a) Original Sailboat on Lake Image (b) Sailboat on Lake Stego image with 95832 bits (c) Sailboat on Lake Stego image with 80176 bits (d) Sailboat on Lake Stego image with 63688 bits (e) Sailboat on Lake Stego image with 54904 bits (f) Sailboat on Lake Stego image with 30280 bits

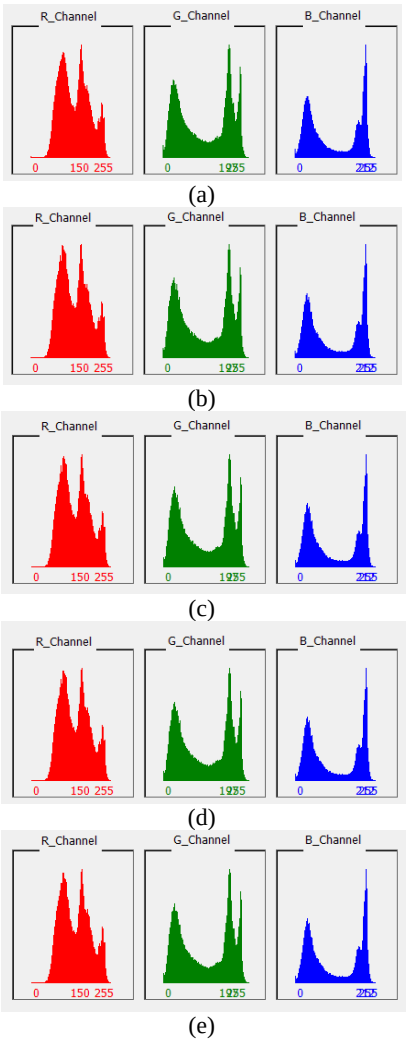
Fig.3 and Fig.4 shoes the histograms of the cover and stego images used in experimentation. Fig. 3 shows the histograms of images of Fig.1. Fig.4 shows the channel based histograms of the images of Fig.2. Perceptually there is no difference between the histograms of cover and stego images which shows the robustness of the stego scheme.



(a) (b) (c)

(d) (e) (f)

Fig 3: (a) Histogram of Original Boat Image (b) Histogram of Boat Stego image with 95832 bits (c) Histogram of Boat Stego image with 80176 bits (d) Histogram of Boat Stego image with 63688 bits (e) Histogram of Boat Stego image with 54904 bits (f) Histogram of Boat Stego image with 30280 bits



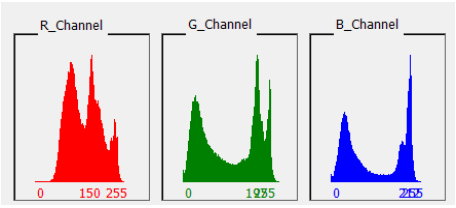
(a)

(b)

(c)

(d)

(e)



(f)

Fig 4 : (a) Channel Based Histogram of Original Sailboat on Lake Image (b) Channel Based Histogram of Sailboat on Lake Stego image with 95832 bits (c) Channel Based Histogram of Sailboat on Lake Stego image with 80176 bits (d) Channel Based Histogram of Sailboat on Lake Stego image with 63688 bits (e) Channel Based Histogram of Sailboat on Lake Stego image with 54904 bits (f) Channel Based Histogram of Sailboat on Lake Stego image with 30280 bits

Table 1 includes the result of important image quality measures [3] , including mean square error (MSE) [4], peak signal to noise ratio (PSNR) [5, 6], universal image quality index measure (UIQI) and structural similarity index measure (SSIM) [7, 8], computed between the cover and stego images of Figure 1. A low MSE, high PSNR, UIQI and SSIM closer to 1 indicate that the distortion in the steo image is not at significant level.

Table 2 shows the result of security analysis (SA) [3, 9] measures, including Jaccard Measure (J), Intersection (I), Correlation (C), Chi-Square (CS) and Bhattacharya (B), computed between the cover and stego images of Figure 1.

Similarly Table 3 and 4 show the result of image quality measure (IQM) and security analysis (SA) for the color image of Figure 2.

Experimental results of IQMs and SA, from Table 1, Table 2, Table 3 and Table 4, shows that this method is robust and creates least distortion while embedding. The results of computations are very close to ideal value.

Table 1. Result of IQM for Images of Fig.1

Image	Bits	MSE	PSNR	UIQI	SSIM
Boat 512x512	95832	0.1827	55.5133	0.9999	0.9999
	80176	0.1529	56.2867	0.9999	0.9999
	63688	0.1218	57.2753	0.9999	0.9999
	54904	0.1051	57.9142	0.9999	0.9999
	30280	0.0578	60.5129	0.9999	0.9999

Table 2. Result of SA for images of Fig. 1

	Bits	J	I	C	CS	B
Boat 512x512	95832	0.9999	0.9993	0.9999	0.0007	0.0012
	80176	0.9999	0.9994	0.9999	0.0006	0.0011
	63688	0.9999	0.9995	0.9999	0.0005	0.0010
	54904	0.9999	0.9996	0.9999	0.0004	0.0009
	30280	0.9999	0.9998	0.9999	0.0002	0.0006

Table 3. Result of IQM for images of Fig. 2

Image	Bits	MSE	PSNR	UIQI	SSIM
Sailboat on Lake 512x512	191664	0.1218	57.2680	0.9999	0.9999
	177520	0.1129	57.0004	0.9999	0.9999
	157616	0.1005	58.1155	0.9999	0.9999
	107760	0.0688	59.7739	0.9999	0.9999
	69552	0.0450	61.6409	0.9999	0.9999

Table 4. Result of SA for images of Fig. 2

	Bits	J	I	C	CS	B
Sailboat on Lake 512x512	191664	0.9999	0.9995	0.9997	0.0005	0.0020
	177520	0.9999	0.9995	0.9999	0.0005	0.0019
	157616	0.9999	0.9996	0.9999	0.0004	0.0018
	107760	0.9999	0.9997	0.9999	0.0002	0.0016
	69552	0.9999	0.9998	0.9999	0.0002	0.0014

3.1 Worst Case Analysis

Table 5 shows the possibility of change (-1 or +1) , no change (NC) and boundary pixel value (BPV).From Table 5 it is clear that there are 99.21 % chances of embedding at first attempt.

Table 5. Analysis of all the 256 Gray Levels

Gray Level	5^{th} 6^{th} 7^{th} Bit	Decimal of 567^{th} Bit	Inert ion of 0	Insertion of 1
0	000	0	BPV	BPV
1	000	0	NC	+1
2	001	1	-1	NC
3	001	1	+1	NC
4	010	2	NC	-1
5	010	2	NC	+1
6	011	3	-1	NC
7	011	3	+1	NC
. . .				
252	110	6	NC	-1
253	110	6	NC	+1
254	111	7	-1	NC
255	111	7	BPV	BPV

From Table 5 following situations are the worst cases possibilities:

- Image has more BPV in the image.
- Always increment is required in the pixel value for insertion of the message bit.
- Always decrement is required in the pixel value for insertion of the message bit.

4. COMPARISON WITH LSB MATHING/SUBSTITUTION

Table 6 shows the similarities and difference between the selected method and LSB matching and LSB substitution method of steganograpgy [10].

Table 6.Comparison of Selected Method with LSB Method

LSB Matching[11] /substitution [12]	Selected Method
Spatial domain simple methods.	Spatial domain simple, effective and good approach.
Creates least changes in image statics.	Creates least changes in image statics.
LSB of the pixel is involved in process of embedding and extraction.	LSB is used while embedding process. Extraction process does not require LSB.
As the LSB is involves in processing, so message can be lost due noise produced due to hardware imperfection.	Message is not in the LSB so remain safe.
Bit plane analysis shows a clear change in LSB bit plane.	Bit plane analysis shows a clear change in LSB bit plane. But as the message is not in the LSB, so it does not matter a lot.
As the message bits are in LSB of the pixel, so any unauthorized person can easily collect all the message bits.	Message bits are not in the LSB.

5. CONCLUSION

Steganography is an art and science of hidden writing. In the current era of digital communication, it is a gifted approach. This paper presents the in depth analysis for the steganography method that uses 5^{th}, 6^{th} and 7^{th} bit of a pixel in processing. Experimental results are the proof of the fact that this method could be the good selection of steganograpgy method for secure transmission of important and secret data over the internet. Image quality measures shows that distortion created by this method is very less and undetectable by the human perception. Result of security analysis proves the robustness and security level of the selected method. Moreover, not to hide the message in the LSB of the pixel gives this scheme an additional feature that message will remain safe even if the intruder change all the LSBs of the pixel or even if the LSBs have been changed due to hardware imperfection or noise. This review provides the detail and easy understating of the steganographic method to the people who want to work in the field of Information security by steganography and present new methods.

6. ACKNOWLEDGMENTS

Special thanks belong to **Sir Dr. Malik Muhammad Saad Missen**, Director Weekend Program at the Department of CS&IT, The Islamia University of Bahawalpur, Pakistan, and **Sir Dr. Nadeem Salamat**, Assistant Professor at the Department of Mathematics and Statistics, Karakoram International University, Gilgit, Pakistan for help and guideline.

Thanks to "The USC-SIPI Image Database" and "Photo database provided by Fabien a. P. Petitcolas" for providing the images (Cover Images only remaining are the results of experiments) and facility of conversion of image into different format for research and experiments.

7. REFERENCES

[1] M. Steinebach, J.Dittmann, "Watermark Based Digital Audio Data Authentication" , EURASIP Journal of Applied Signal Processing, vol. 10, pp. 1001-1015, 2003.

[2] Rajkumar Yadav, RaviSaini, Kamaldeep, A Novel Image Steganography Approach for Information Security Using Gray Level Images in Spatial Domain, International Journal on Computer Science and Engineering, Vol.3 No.7 July 2011

[3] M. Khurrum Rahim Rashid, Nadeem Salamat, Saad Missen and Aqsa Rashid. "Robust Increased Capacity Image Steganographic Scheme" International Journal of Advanced Computer Science and Applications (IJACSA), 5(11)., 2014

[4] Ismail Avcibas, Bulent Sankur, Khalid Sayood, Statistical Evaluation of Image Quality Measure, *Journal of Electronic Imaging*, 11(2), 206-223, 2002

[5] Zhou Wang, *Member*,Hamid R. Sheikh, Image Quality Assessment: From Error Visibility to Structural Similarity, *IEEE Transactions On Image Processing*, (VOL. 13, NO. 4), 2004

[6] Yousra A. Y. Al. Najjar, Dr. D. C. Soong, Comparison of image quality assessment: PSNR, HVS, UIQI, SSIM, IJSER, (Vol. 3, Issue8). ISSN2229-5518 ,2012

[7] Amhamed Saffor, Abdul Rahman Ramli, Kwan-Hoong Ng, A Comparative Study Of Image Compression Between Jpeg And Wavelet, *Malaysian Journal of Computer Science*, (Vol. 14 No. 1), pp. 39-45 , 2001

[8] Hamid Rahim Sheikh, Muhammad Farooq Sabir, Alan C. Bovik, A Statistical Evaluation of Recent Full Reference Image Quality Assessment Algorithms, IEEE TRANS. IMAGE PROCESSING, 2006

[9] V.Asha, P.Nagabhushan, N.U.Bhajantri, Similarity Measures for Automatic Defct Detection on Patterned Texture, International Journal of Image Processing and Vision Science, Volume-1, 2012

[10] N.F.Johnson, Sushil Jojadia George Mason University, Exploring Steganography: Seeing the Unseen, 0018-916/98/$10.00© IEEE 1998

[11] Muhammad Khurrum Rahim, Aqsa Rashid, Nadeem Slamat and Saad Missen, Experimental Analysis of Matching Technique of Steganography for Grayscale and Color Images, International Journal of Computer Science and Information Technology, Vol 6, No6, December 2014

[12] Aqsa Rashid, Experimental Analysis and Comparison of LSB Substitution and LSB Matching Method of Information Security, IJCSI,Volume 12, Issue1, No,1, 2015

8. AUTHOR PROFILE

Muhammad Khurrum Rahim

Muhammad Khurrum Rahim currently is a student of Electrical Engineering BS (EE) in NUCES FAST Islamabad, Pakistan for the session 2013-2017. He has won the competition of English Creative writing in 2007 held in Pano Akil Region, Pakistan by APS&CS. He has one gold and three silver medals in Inter School Mega Competition 2012 and Inter School Mega Competition 2013 in Pano Akil Region, Pakistan by APS&CS. His fields of interest include Robotics, Image Processing, Signal Processing, Circuit theory, Differential and Telecommunication.

Aqsa Rashid

Aqsa Rashid received her Master's degree in Computer Sciences (MCS) (Gold Medalist) from The Islamia University of Bahawalpur, Pakistan in November, 2012 with specialization in Digital image processing and Information security. Currently she is a student of MSCS in The Islamia University of Bahawalpur; Pakistan. Her fields of interest include Information security, Robotics, Digital image Processing, Computer Vision, Artificial Intelligence, Pattern recognition, Data mining and Web Designing and Development. Currently she is engaged in real time image processing and computer vision projects.