Experimental Analysis and Comparison of LSB substitution and LSB Matching Method of Information Security

Aqsa Rashid[1]

[1] **Department of Computer Science and Information Technology, The Islamia University of Bahawalpur, Pakistan**
Rahim Yar Khan, 64200, Pakistan

Abstract

Steganography is an art of covert communications. Its core function is to conceal the occurrence of communication over a civic channel. Hiding the occurrence of communication can be done by embedding a secret message into cover medium which no one else than the correspondent and the addressee can expect and steganalysis is the art and science of recognizing a clandestine communication. The purpose of this paper is the analysis of chosen technique experimentally, evaluate the technique, compare results on literature and give direction on what can be done for new and better approach of steganography and steganalysis.

Keywords: *LSB, Matching, Robust, Spatial Domain, Steganography, Substitution*

1. Introduction

Inclusive clandestine information's are exchanged over internet where the information security plays a main function. Cryptography and steganography are two approaches used to achieve the security while transmitting the data over the internet. Staganography is similar to cryptography in sense that both are used to keep information secret and secure with the difference being that cryptography just makes the message secret by converting the message into cipher text, i.e. message is there but no one can understand the meaning of message. In steganography existence of message cannot be detected.

In current era Steganography is considered as an exceptional approach [2] [3] [4] [5] for protected electronic communication. Image least significant bit (LSB) matching and substitution methods [1] are the steganographic techniques that create the least change in statistics after hiding the message in image. Although lots of techniques have been presented in last few years but LSB substitution and matching are the oldest methods and analysis and comparison of these methods will help to present new steganographic methods.

The paper is arranged as Section 2 describes the Method, Section 3 gives comparison of both methods, Section 4 discusses the tools used for analysis, Section 4 includes Experimental results and discussion, Section 5 is the conclusion and references are in last section.

2. Method

This section presents the embedding and extraction steps for the substitution and matching methods.

2.1 Substitution

Embedding steps for LSB Substitution Stego-method are:

1: $forj = 1, \dots, l(m)$
2: $lsb = \text{LSB}\ (p_j)$
3: $if lsb \neq m_j then$
4: $lsb \leftarrow m_j$
5: $endif$
6: $endfor$

$l(m)$ Contain the message bits. It first takes the pixel p_j of the image and its $\text{LSB}\ (p_j)$ value. If the number is even the lsb will be 0 and a 1 if the number is odd. We then contrast this with the message bit m_j. If they are before now the same, then nothing to be done, but if they are dissimilar it should change lsb with m_j. This process goes on even as $l(m)$ is not zero.

The Extraction steps for LSB Substitution Stego-method are:

1: $forj = 1, \dots, l(s)$
2: $rm_j \leftarrow (s_j)$
3: $endfor$

$l(s)$ is the total number of pixels of supposed image. Run

the loop $l(s)$ in place of $l(m)$. This is because the embedding is different from the retrieval process. We just recover the LSB value of each pixel rm and translate this to ASCII; the message will be understandable and in readable format up to the point that the message was embedded, and will then come into view as claptrap when we are see the LSBs of the image data. If we know the length of the message that was embedded, then the loop will be ended when the length of message is completed and only the message will be retrieved.

2.2 Matching

Matching steps for matching LSB Stego-method are:

1: $for\ k = 1, \dots, l(n)$
2: $lsb = \text{LSB}\ (p_k)$
3: $if\ lsb \neq n_k\ then$
4: $p_k = p_k + 1\ or\ p_k = p_k - 1$ to make $lsb = n_k$
5: $end\ if$
6: $end\ for$

$l(n)$ Contain the message bits. It first takes the pixel p_k of the image and its $\text{LSB}\ (p_k)$ value. If matching bit and $\text{LSB}\ (p_k)$ are now the same, then nothing to be done, but if they are dissimilar then increment or decrement in p_k in such a way that the $\text{LSB}\ (p_k)$ become the matching bit. This process goes on even as $l(m)$ is not zero.

Steps for sequential LSB Substitution Stego-method

1: $for\ k = 1, \dots, l(s)$
2: $rm_k \leftarrow (s_k)$
3: $end\ for$

$l(s)$ is the total number of pixels of supposed image. Run the loop $l(s)$ in place of $l(n)$. This is because the embedding is different from the retrieval process. We just recover the LSB value of each pixel rm and translate this to ASCII; the message will be understandable and in readable format up to the point that the message was embedded, and will then come into view as claptrap when we are see the LSBs of the image data. If we know the length of the message that was embedded, then the loop will be ended when the length of message is completed and only the message will be retrieved i.e., no gibberish will be seen at the end of the message.

3. Comparison of LSB substitution and LSB matching:

This section compares the substitution and matching techniques.

3.1Similarities:

1. Both are spatial domain method.
2. Both are the easy and simplest methods of steganography to implement.
3. Both schemes use the least significant bit (LSB) for hiding message.
4. Both techniques create same change in statistical properties of the image.
5. For both techniques the embedding rate is 1.
6. For both techniques the rate of change is 50%.
7. Both techniques have the same disadvantage that message can be lost due to:
    a. Hardware imperfection
    b. Intruder inverts all the LSBs
8. In both cases the message can be easily recovered by unauthorized person as the message is in LSBs.
9. Both are the static method i.e. they sequentially hide the message in LSBs of the image pixel value.
10. Both techniques have same retrieval process.

4. Difference:

LSB Substitution

1. Process of replacement is performed for substitution of message bit.
2. Only the LSB of the pixel will be change.

For example:
Suppose 11111110 is the pixel binary value and 254 is its decimal equivalent and 1 is the message bit you want to substitute. After the substitution, the pixel binary values will

LSB Matching

1. Process of adjustment is performed for matching of message bit.
2. Matching produces more bit modification. There are possibilities that all bits may have change.

For example:
Suppose 01111111 is the pixel binary value and 127 is its decimal equivalent and 0 is the message bit you want to

be11111111. This shows that only the bit that is in purple color is having a change; remaining seven bits are same as before now.

3. In Visual attack, only the LSB bit plane will be altered.

4. LSB substitution is intrinsically asymmetric, i.e. an even valued pixel will either keep its value or be incremented by one. However, it will never be decremented. The reverse is true for odd-valued pixels. This asymmetry is the key for steganalysis.

5. Tools Used for Analysis

The section is further subdivided into three sections. First is named as "Security Analysis" and second is named as "Robustness Analysis" [6].

5.1 Steganalysis

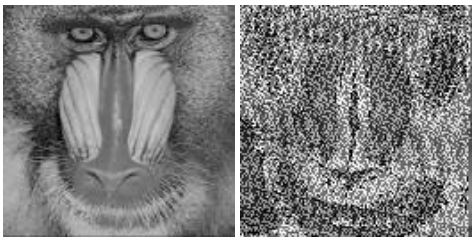
This section discusses the attacks on LSB substitution and LSB matching. The result of steganalysis depends on what the steganalyst wishes to recognize. For example, one steganalyst might just desire to identify whether two parties are communicating. Whereas another steganalyst might desire to identify how two parties are communicating.
Image Steganalysis system first detect that whether the system is a stego-image or not. Further processing i.e. to modify the embedded message or destroy the message is done after that. Some common stegabalysis approaches are:

5.1.1 Visual Appearance**:**

Small change in pixel value, increment or decrement by one, creates least change in statistical properties of the image. This change in statistical measure is so small that visually it cannot be detected by human eye. If the most significant bit (MSB) is used instead of LSB than the distortion is clearly visible to human eye. Fig 1 shows the effect of visual change at great extinct. Figure 1 (a) is the cover image and (b) is the stego-image.

embed. After the adjustment, the pixel binary values will be**10000000.** This shows that all the bits have been changed.

3. In Visual attack, least bit plane has change at great extinct and remaining all bit planes may also have some change. The reason is that adjustment process can modify all the bits of pixel.
4. Rather than simple substitution of the message bit in LSB, the consequent pixel value is arbitrarily incremented or decremented, thus removing the asymmetry of even and odd pixels.



(a)Cover image (b) Stego-image
Fig 1 Effect of Visual change

Fig 2 shows the visual appearance of two the Cover Images (CI) used for the experiment. Figure 2 (a) is the Barbara Gray Cover image having dimensions 89x119 and (b) is the Baboon Color Cover image having dimensions 131x131. All the experimental results are shown for these two images.

(a)Barbara Gray (b) Baboon Color
Fig 2 Cover Images used in Experimental Analysis

5.1.2 Histogram Analysis:

LSB substitution creates pair of values (POV) which can be detected in steganalysis. Figure 3 shows the effect of substitution on the histogram. Fig 3 (a) shows the histogram of cover image. Fig 3 (b) shows the histogram of stego-image.

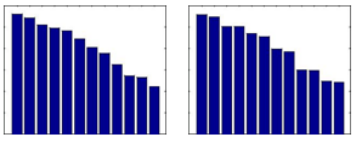


Fig 3 Histogram of Cover image and Stego-image

After LSB matching the local maxima of the histogram of image will decrease and the local minima will increase. Steganalysis of LSB matching is difficult as compare to LSB substitution. Fig 4 shows the effect of adjustment on the histogram. Fig 4 (a) shows the histogram of cover image and (b) is the effect of matching.

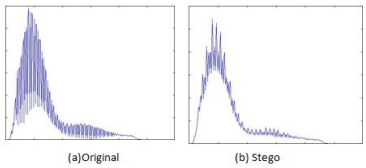
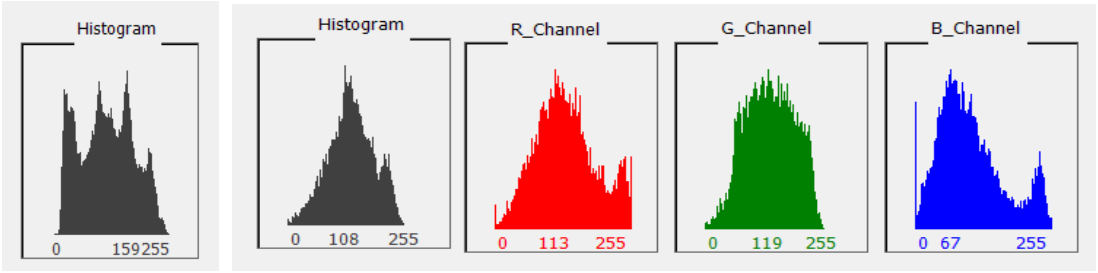


Fig 4 Histogram of Cover image and Stego-image

Fig 5 shows the histograms of Cover images used for experiment. Histogram also shows the number of pixels having the same color. Fig 5 (a) is the histogram of Barbara Gray Cover image. Fig 5 (b) is the histogram of Baboon Color Cover image; (b) also shows the channel based histograms of the Baboon color cover image.



(a)Histogram of Barbara Gray Cover Image (b) Histogram of Baboon Color Cover Image
Fig 5 Histograms of Cover Images

5.1.3 Visual Attack:

Visual hit distinguish whether or not a hypothetical image has been subjected to LSB matching steganography, the steganalyst will be looking to obtain a visual inconsistency in the bit plan that will successfully point out signs of embedding. Fig 5 shows the concept of bit plans for grayscale image.

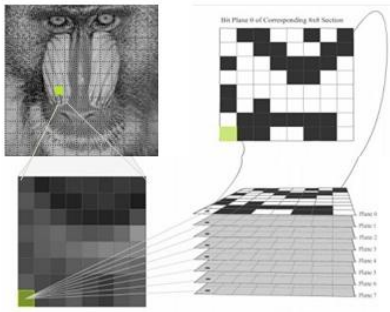
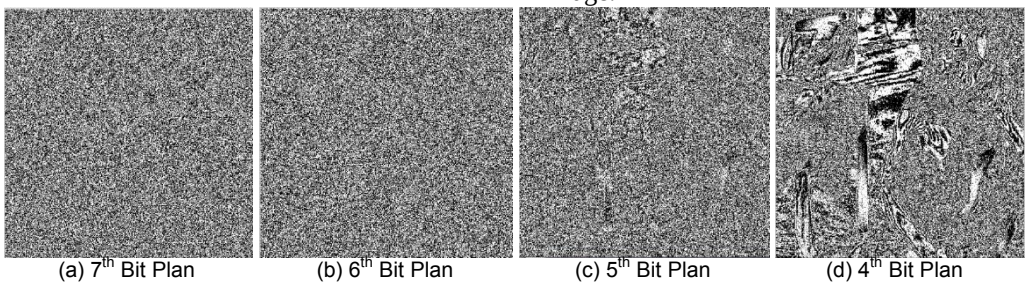


Fig 6 Bit Plan Concept for 8 Bit per pixel images

Fig 6 (a-h) shows the bit plans of Barbara Gray cover image.

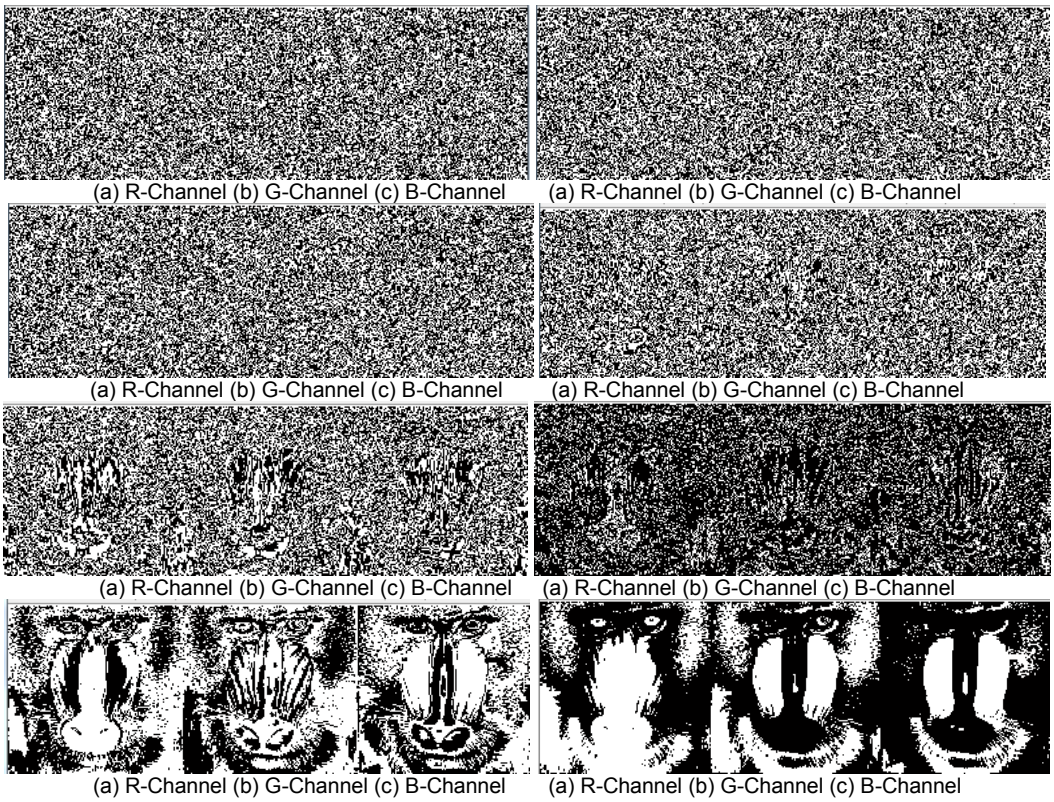


(a) 7th Bit Plan (b) 6th Bit Plan (c) 5th Bit Plan (d) 4th Bit Plan

(e) 3rd Bit Plan (f) 2nd Bit Plan (g) 1st Bit Plan (h) 0th Bit Plan

Fig 7 (a-h) Shows the bit plans of Barbara Gray Cover image

Fig 8 (a-h) shows the channel based bit plans of Baboon Color cover image.



(a) R-Channel (b) G-Channel (c) B-Channel (a) R-Channel (b) G-Channel (c) B-Channel

(a) R-Channel (b) G-Channel (c) B-Channel (a) R-Channel (b) G-Channel (c) B-Channel

(a) R-Channel (b) G-Channel (c) B-Channel (a) R-Channel (b) G-Channel (c) B-Channel

(a) R-Channel (b) G-Channel (c) B-Channel (a) R-Channel (b) G-Channel (c) B-Channel

Fig 8 (a-h) Shows the 0th to 7th Channel based bit plans of Baboon Color Cover image

5.2 Security Analysis:

Comparing the normalized histograms of cover image and the stego-image gives the clear idea of security. The security examination evaluates the cover image with the stego-image on the basis of histograms of Images. For histogram comparison Jaccard measure, Correlation, Chi-square, Intersection and Bhattacharya distance [6] are computed between the histogram of cover image and stego-image.

All these comparisons are performed on normalized histogram. The value of Jaccard and correlation varies between 1 and -1. Perfect match is 1 and total mismatch is -1. For Chi-square ideal value is 0 and mismatch value is unbound, for intersection 1 is ideal matching value and 0 is mismatched value and Bhattacharya distance gives 0 for the exact match and 1 for mismatch. When these comparison matrices gives ideal values or values that are closer to ideal values then the change in histogram is very least and this is the evidence for Stego-System to be a secure system.

5.3 Image Quality Evaluation:

Robustness and quality of any method depends on different parameters. In the paper four most

important and widely used Image quality measures [7, 9, 10, 11, 12] namely MSE, PSNR, UIQI and SSIM are computed for comparison.

Mean Square Error computes the perceived error. It is pixel value difference based quality measure. Peak Signal to Noise Ratio [10] is inversely proportional to MSE. Less MSE gives High PSNR which is the proof of the fact that image has good quality.

Image Quality Index split the judgment of similarity between Cover Image (CI) and Stego-Image (SI) into three comparisons: Luminance, Contrast and Structural Information. SSIM estimates "Perceived change in structural information". It computes the similarity between two images of common size.

The value of UIQI and SSIM varies between 1 and -1. Closer the highest positive value denotes too much less change in two images and -1 shows totally mismatch. UIQI and SSIM are considered as more consistent and accurate than MSE and PSNR.

6. Experimental results

This section presents the experimental results obtained after implementing the proposed method in .NET Framework (C#). A system is designed and implemented in .NET Framework (C#) that shows the working of LSB substitution and LSB matching Steganography method.
This section is also divided into two subsections. First will give the experimental results for grayscale images and second subsection will give for color images.

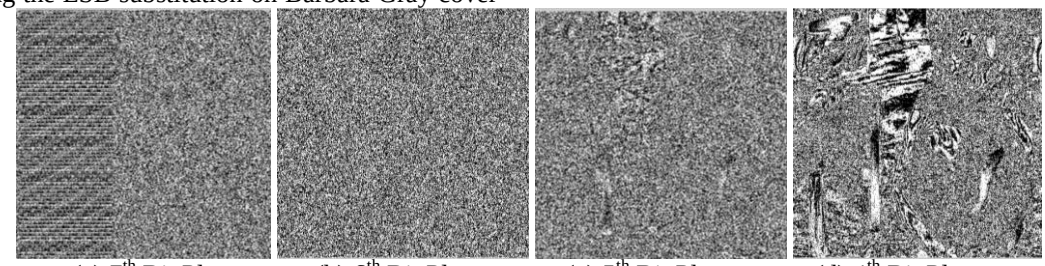
6.1 Grayscale Images:

This section gives the experimental results for grayscale images. Fig 9 shows the visual appearance of grayscale images after applying the LSB substitution and LSB matching. Fig 9 (a) is the Stego-Barbara Gray image after applying LSB substitution, (b) is the Stego-Barbara Gray after applying LSB matching, (c) is the histogram of Fig 9 (a) and (d) is the histogram of Fig 9 (b).

(a)Stego-Barbara Gray after applying LSB substitution (b)Stego-Barbara Gray after LSB matching (c)Histogram of Stego-Barbara Gray (d) Histogram of Stego-Barbara Gray

Fig 9 Visual appearances of Stego-Gray images and their Histograms

Fig 10 (a-h) shows the bit plans of Stego-Barbara Gray after applying the LSB substitution on Barbara Gray cover image. 7th bit plan clearly shows the inconsistency due to message substitution.

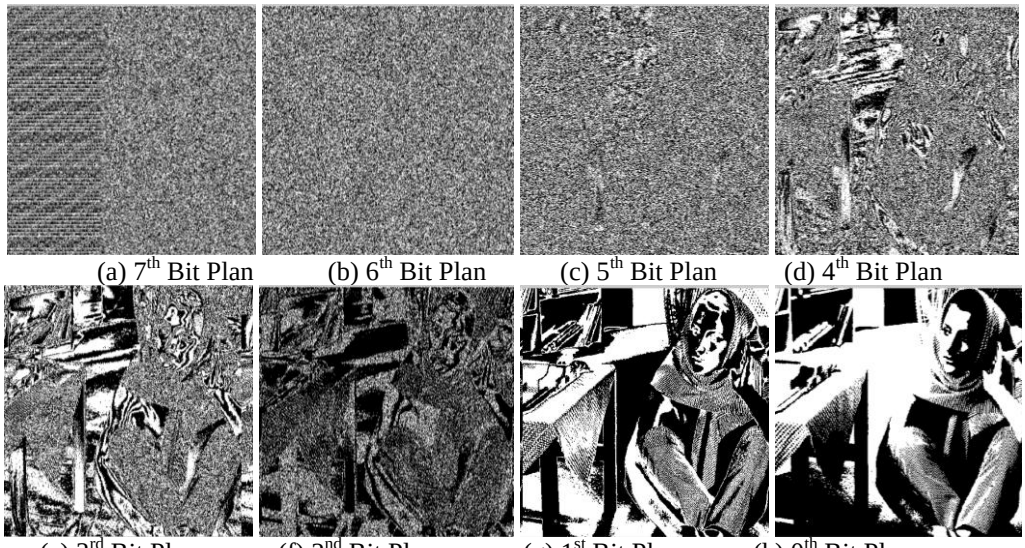


(a) 7th Bit Plane (b) 6th Bit Plane (c) 5th Bit Plane (d) 4th Bit Plane

(e) 3rd Bit Plan (f) 2nd Bit Plan (g) 1st Bit Plan (h) 0th Bit Plan

Fig 10 Bit plans of Stego-Gray images after substitution

Fig 11 (a-h) shows the bit plans of Stego-Barbara Gray after applying the LSB matching on Barbara Gray cover image. 7th bit plan clearly shows the inconsistency.



(a) 7th Bit Plan (b) 6th Bit Plan (c) 5th Bit Plan (d) 4th Bit Plan

(e) 3rd Bit Plan (f) 2nd Bit Plan (g) 1st Bit Plan (h) 0th Bit Plan

Fig 11 Bit plans of Stego-Gray images after matching

Table 2 shows the result of security analysis and image quality evaluation, computed between the Barbara Gray and Stego-Barbara Gray after applying LSB substitution and LSB matching.

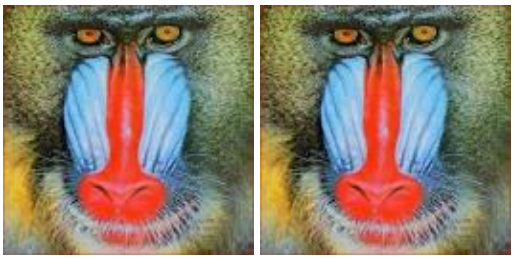
Table 2: Result of security analysis and Image quality for the Barbara Gray image

Method	Substitution	Matching	Method	Substitution	Matching
Jaccard	0.99999	0.99999	**MSE**	0.18377	0.18377
Intersection	0.99913	0.99913	**PSNR**	55.48808	55.48808
Correlation	0.99997	0.99997	**UIQI**	0.99997	0.99997
Chi-Square	0.00078	0.00078	**MSSIM**	0.99997	0.99997
Bhattacharya	0.00159	0.00159			

Table 2 shows the same result for substitution and matching because for both the methods the change in pixel will not exceed to 1.

6.2 Color Images:

This section gives the experimental results for color images. Fig 12 shows the visual appearance of color images after applying the LSB substitution and LSB matching. Fig 12 (a) is the Stego-Baboon Color image after applying LSB substitution, (b) is the Stego-Baboon Color after applying LSB matching.



(a)Stego-image after substitution (b) Stego-image after matching
Fig 12 Visual Appearance of stego-image

Fig 13 shows the histogram of the image of Fig 12 (a). Histogram also shows the channel based histogram and maximum number of pixel having the same color.

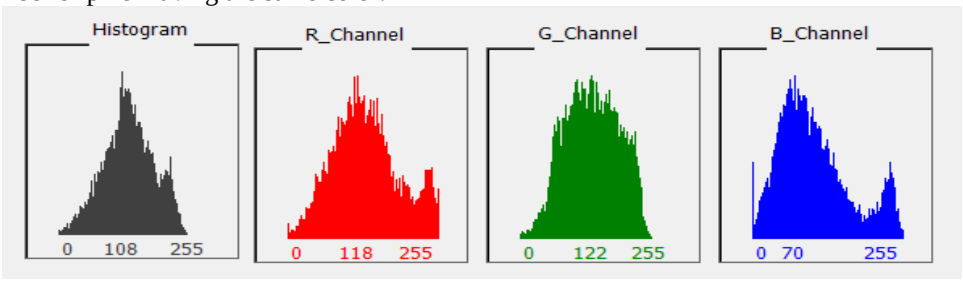


Fig 13 Histogram of Baboon Color Stego image after LSB substitution

Fig 14 (a) shows the histogram of Fig 12 (b).

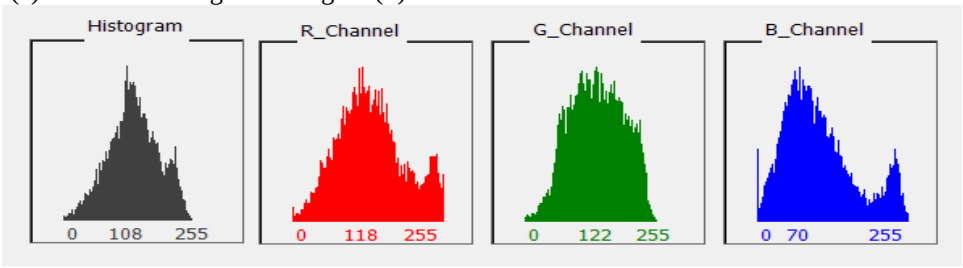
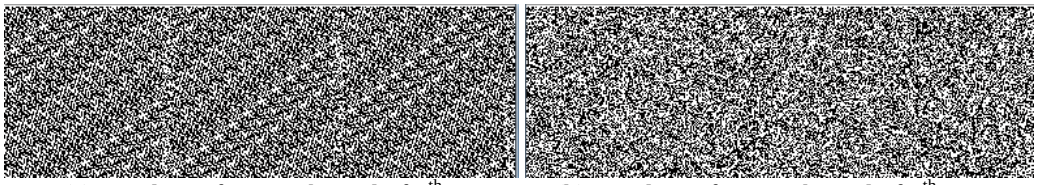
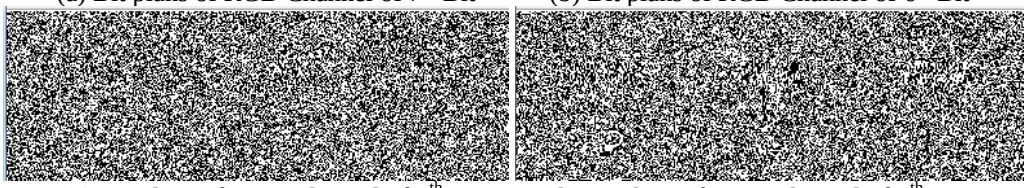


Fig 14 Histogram of Baboon Color Stego image after LSB substitution

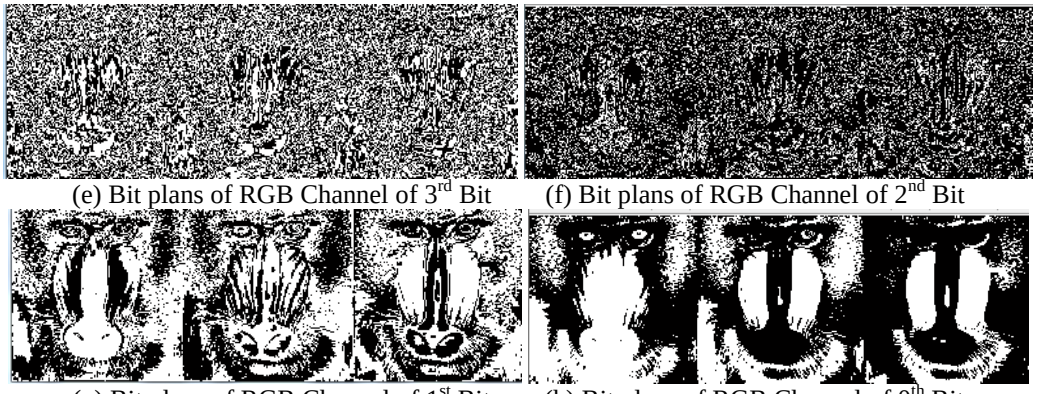
Fig 15 (a-h) shows the bit plans of Stego-Baboon color after applying the LSB substitution on Baboon Color cover image. 7th bit plan clearly shows the inconsistency due to message substitution.
Fig 16 (a-h) shows the bit plans of Stego-Baboon after applying the LSB matching on Baboon cover image. 7th bit plan clearly shows the inconsistency due to message matching.



(a) Bit plans of RGB Channel of 7th Bit (b) Bit plans of RGB Channel of 6th Bit



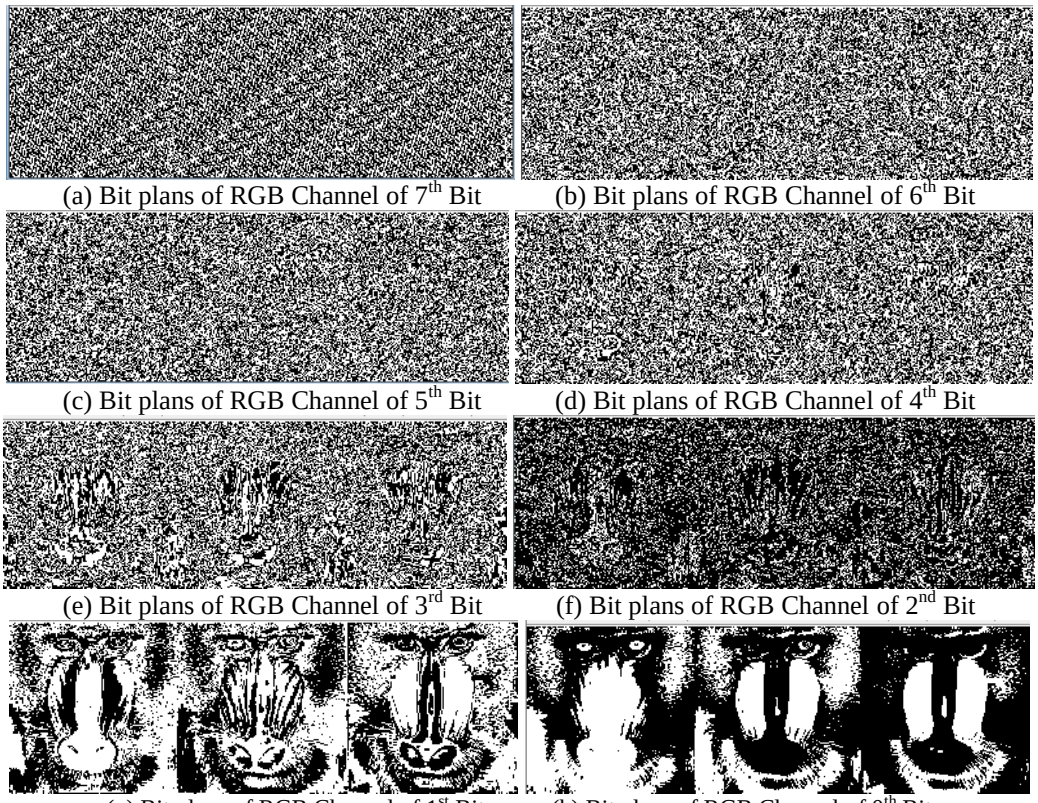
(c) Bit plans of RGB Channel of 5th Bit (d) Bit plans of RGB Channel of 4th Bit



(e) Bit plans of RGB Channel of 3rd Bit (f) Bit plans of RGB Channel of 2nd Bit

(g) Bit plans of RGB Channel of 1st Bit (h) Bit plans of RGB Channel of 0th Bit

Fig 15 Bit plans of Stego-Color images after substitution



(a) Bit plans of RGB Channel of 7th Bit (b) Bit plans of RGB Channel of 6th Bit

(c) Bit plans of RGB Channel of 5th Bit (d) Bit plans of RGB Channel of 4th Bit

(e) Bit plans of RGB Channel of 3rd Bit (f) Bit plans of RGB Channel of 2nd Bit

(g) Bit plans of RGB Channel of 1st Bit (h) Bit plans of RGB Channel of 0th Bit

Fig 16 Bit plans of Stego-Color images after matching

Table 3 shows the result of security analysis and image quality measure for Baboon image.

Table 3: Result of security analysis and Image quality for the Baboon Color image

Method	Substitution	Matching	Method	Substitution	Matching
Jaccard	0.99998	0.99998	**MSE**	0.46858	0.46858
Intersection	0.99782	0.99782	**PSNR**	51.42222	51.42222
Correlation	0.99993	0.99993	**UIQI**	0.99992	0.99992
Chi-Square	0.00198	0.00198	**MSSIM**	0.99992	0.99992
Bhattacharya	0.00366	0.00366			

7. Conclusions

This paper presents the detail study of LSB substitution and LSB matching steganography schemes and types of attacks on them. Both methods are good in terms of that they show the same good quality of image after hiding the message and simpler to implement. But, in view of experimental results, the steganalysis of LSB matching method is quite difficult as compare to that of LSB substitution. So in terms of steganalysis, LSB matching technique is better choice for secure electronic communication over the internet. This comparison is very helpful analysis for those who want to do work in the field of steganography and steganalysis.

References

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

[2] R.Poornima, R.J.Iswarya, An Overview of Digital Image Steganography, *International Journal of Computer Science & Engineering Survey* (Vol.4, No 1),February 2013

[3] T.Morkel, T.H.P.Eloff, M.S.Olivier, An Overview of Image Steganography, ICSA Research Group, Department of Computer Science.

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

[5] Shikha Sharda, Sumit Budhiraja , Image Steganography:A Review, *International Journal of Emerging Technology and Advance Engineering* (volume 3, Issue 1), January 2013

[6] V. Asha, P. Nagabhushan, N. U. Bhajantri, Similarity Measures for Automatic Defect Detection on Patterned Textures, International Journal of Image Processing and Vision Sciences (IJIPVS) Volume-1 Issue-1, 2012

[7] Rajkumar Yadav, Analysis of Various Image Steganography Techniques Based Upon PSNR Metric, *International Journal of P2P Network Trends and Technology*-(Volume1, Issue2)- 2011, ISSN: 2249-2615

[8] M. Pavani, S. Naganjaneyulu, C. Nagaraju, A Survey on LSB Based Steganography Methods, *International Journal Of Engineering And Computer Science* ISSN: 2319-7242 (Volume 2 Issue 8) August, 2013 Page No. 2464-2467

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

[10] Zhou Wang, *Member*,Hamid R. Sheikh, Image Quality Assessment: From Error Visibility to Structural Similarity, *IEEE Transactions On Image Processing*, (VOL. 13, NO. 4), APRIL 2004 1

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

[12] 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), June 2001, pp. 39-45

Aqsa Rashid received her Master's degree in Computer Sciences (MCS) (Gold Medalist) from Islamia of Bahawalpur, Pakistan in November, 2012. Currently she is a student of MSCS (session Feb, 2013-2015 spring) in The Islamia University of Bahawalpur; Pakistan. She is a Visiting Faculty member of The Islamia University of Bahawalpur, Department of CS&IT since Nov, 2012 to present. Her fields of interest include Robotics, Digital image Processing, Artificial Intelligence, Data Mining and Web Designing and Development. At present, she is engaged in Image Steganography and Steganalysis.