International Journal of Signal Processing, Image Processing and Pattern Recognition
Vol.8, No.11 (2015), pp.265-272
http://dx.doi.org/10.14257/ijsip.2015.8.11.24

Experimental Review of "Grey Level Modification" Steganography

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

[1]Department of Computer Science & Information Technology, The Islamia University of Bahawalpur, Pakistan
[2]Department of Electrical Engineering, NUCES, FAST, Pakistan
[1]aqsarashid2@gmail.com, [2]khurrumrahim@gmail.com

Abstract

Steganography is the science of hidden writing schemes in which the presence of concealed information is not noticeable. It is a gifted approach for secure electronic communication and transmission of secret data safely over the internet. This paper is the detailed experimental analysis and review of "Grey Level Modification Steganography for Secret Communication". Analysis is based on popular image quality measures, security analysis, visual analysis, bit plane analysis and worst case situation. Experimental result of selected method of steganogrphgy is compared with the basic Least Significant Bit substitution and Least Significant Bit matching method of steganography. All these results are checked for both the color and grayscale images. Moreover this review and analysis could be a deep understanding of most popular and simple steganography method such as Grey Level Modification, Least Significant Bit substitution, Least Significant Bit matching etc and will be a helpful analysis for presenting new approaches in this field.

Keywords: *IQM, Bit Plane Analysis, GLM, LSB, Steganography, Steganalysis, Security Analysis*

1. Introduction

Steganography is an exceptional loom in the existing era of digital technology. Due to its usefulness it is attaining importance swiftly. Steganography has established a lot of concern in not many years. In analysis of the detail of September 11th, 2001, some people have suggested that Al Qaeda utilize Steganography scheme to synchronize the World Trade Centre assail. But afterwards, nothing was making available as verification. Some scientific and commercial application of the hidden writing includes that it is the most important tool for the secure electronic transmission of important information, document authentication, document tracking, digital election and electronic money. Beside these, information collected in a radar station, or during medical imaging, can be put together with the pictures.

1.1. Important Terminologies of Steganography

A complete steganography system consists of the cover object, stego object, embedding algorithm, extraction process and secret message and some time a stego key which is used to extract the message from stego object. Embedding of message is performed in the sender side and extraction process is carried out at recipient side. Only the sender and intended recipient know the secret transmission of information.

Explanations of the important terminologies of the stego system are following:

- **Cover Object:** It is the input medium in which concealment of secret data is to be performed. It could be an image, video file, audio file or a text file.
- **Stego-Object:** After the concealment of secret data into the cover medium, the cover object becomes the stego-object.
- **Embedding:** Embedding is the process of making a stego-object from a cover object. Or we can define it as the process of concealment of secret message into some digital medium.
- **Extraction:** This is the reverse process of embedding. In this process, the conceded message is recovered from stego-object to read it.
- **Message:** It is the secret information that is to be embedded in the cover object for safe transmission of data from sender to receiver.

2. Methodology

The "Grey Level Modification Steganography for Secret Communication" [1] dos not hide or embed data inside the image; it is a one-to-one mapping method. This method uses the concept of even and odd pixel value and a mathematical function to select the pixels for mapping. Even pixels represent 0 and odd pixels represent 1.

Main logic behind this method is mentioned in the following steps:

a. A mathematical function is used for the selection of pixels for mapping data.
b. Pixels having odd grey levels, from the selected pixels, are incremented by one to make even grey levels.
c. If the bit stream is zero no change in the pixel value is required.
d. If the bit stream is one, decrement of pixel by one is required to map bit stream.

The reverse process is used for collecting all the message bits.

a. By using the same mathematical function that was used at the time of mapping, pixels are selected.
b. Even value of grey level represents 0 bit stream.
c. Odd value of grey level represents 1 bit stream.

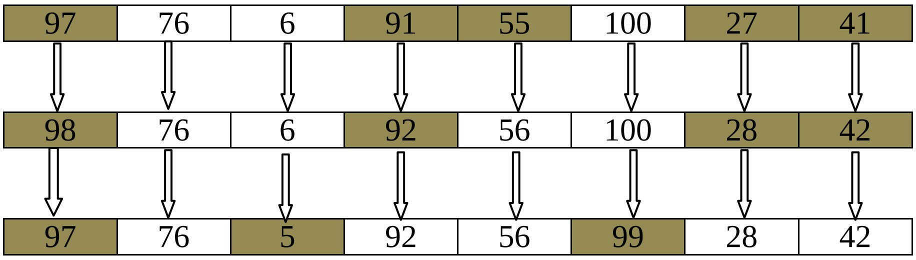
Below is the example of the GLM method of steganography.

Figure 2 shows the hypothetical grey levels. Highlighted pixels are selected pixels for mapping based on some mathematical function. Suppose that the mapping bit stream is 10100100.

12	97	55	34	77	34	221	22	254	81
45	67	76	65	87	22	223	84	222	79
33	45	44	6	7	32	54	82	147	78
23	44	45	2	91	56	67	74	85	48
4	123	32	5	121	55	94	65	123	51
7	111	24	3	222	42	100	26	245	56
88	4	78	5	56	98	57	27	11	74
90	56	0	67	34	111	144	23	41	51

Figure 1. Pixels Selected using Mathematical Function from the Hypothetical Grey Levels

Figure 2 shows processing of the second, third and fourth step of the algorithm. In second step all the odd value pixels are incremented to make them even. In third step, if the bit stream is even then no change is required. In fourth step, if the bit stream is odd then the decrement of one is carried out on the selected pixel for mapping.



97	76	6	91	55	100	27	41
98	76	6	92	56	100	28	42
97	76	5	92	56	99	28	42

Figure 2. Processing of Step 2 and 3 of the Algorithm

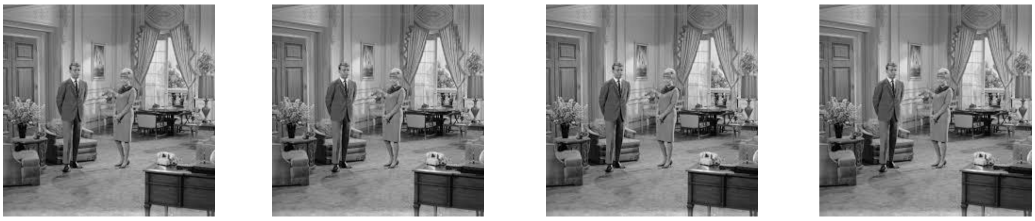
3. Tools Used for Analysis and Review

Tools used for the analysis and review include Image Quality Measures, Security Analysis, Bit Plane Analysis, Worst Case Analysis and Noise Level Estimation. These tools are used as steganalysis tools in steganography. Brief overview of these tools is mentioned below:

- **Visual Appearance [2-7]:** This is the stego-image appearance by human perception.
- **Image Quality Measure (IQM) [2-11]:** Most widely used image quality measures for steganography , including Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Universal Image Quality Index (UIQI), Structural Similarity Index Measure (SSIM), Image Fidelity (IF), Normalized Cross Correlation (NCC), Average Difference (AD) *etc* are used for the evaluation.
- **Security Analysis (SA) [2-7 and 12]:** For Security analysis Paterson Correlation Coefficient, Jacaard Measure, Intersection Coefficient Measure, Bhattacharya and Chi-Square Measure are computed between the normalized histograms of cover image and stego images.
- **Bit Plane Analysis (BPA) [2-7]:** A greyscale image has eight bit planes. Each bit plane has a correlation with the other bit plane. Process of substitution will create a change in the bit plane that will be visible in bit plane analysis.
- **Worst Case Analysis (WCA):** In this analysis the possibility when the selected steganography scheme gives the bad result is analyzed.

4. Experimental Results and Discussion

This section presents the experimental results for the GLM method for the grayscale and color images. Figure 3 shows the visual appearance of grayscale cover image and stego image. Figure 2 (a) is the grayscale Couple cover image with dimensions 225x225, (b) is the stego Couple image with 23904 mapped bits, (c) is the stego Couple image with 37448 mapped bits and (d) is the stego Couple image with 45348 mapped bits. It is clear from the Figure 3 that visual appearance of the stego images is very good. It is impossible to make a distinction between cover image and stego images by human perception.



(a) Cover Image

(b) Stego-Image with 23904 Bits

(c) Stego-Image with 37448 Bits

(d) Stego-Image with 45348 Bits

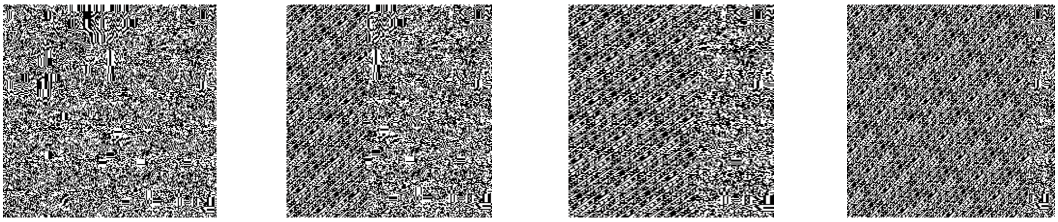
Figure 4. Cover and Stego Grayscale Images

Table 1 shows the result of image quality measures (IQMs) and security analysis (SA) evaluated between the cover image and stego images of the Figure 2.

Table 1. Result of IQMs and SA between the Cover Image and Stego Images of Figure 3

IQMs	23904	37448	45348	SA	23904	37448	45348
MSE	0.23569	0.36999	0.44620	**Jaccard**	0.99999	0.99998	0.99997
PSNR	54.4073	46.50716	51.6354	**Intersection**	0.99894	0.09983	0.99797
UIQI	0.99999	0.99990	0.99988	**Correlation**	0.99994	0.99990	0.99988
SSIM	0.99999	0.99990	0.99988	**Chi-Square**	0.00097	0.00153	0.00184
IF	0.99994	0.99998	0099997	**Bhattacharya**	0.00252	0.00281	0.00331
NCC	0.99984	0.99972	0.99966				
AD	0.02204	0.03818	0.04632				

Figure 5 shows the BPA of the images of Figure 4. If 0 to 7 are the eight bit planes of the grayscale image, then the 7th bit plane of the images of Figure 4 are shown in Figure 5. In Figure 5 (a) is the 7th bit plane of the cover image of Figure 4(a). In Figure 5(b, c and d), inconsistency of the 7th bit plane is clearly visible.



(a) 7th bit plane of Couple Cover image

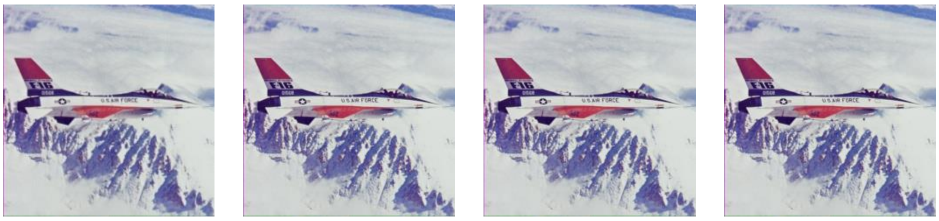
(b) 7th bit plane of Couple Stego image with 23904 bits

(c) 7th bit plane of Couple Stegor Image with 37448 bits

(d) 7th bit plane of Couple Stego image with 45348 bits

Figure 5. Bit Plane Analysis (BPA) of Cover and Stego images of Figure 4

Figure 6 shows the visual appearance of color cover image and stego image. Figure 2 (a) is the color Airplane cover image with dimensions 512x512, (b) is the stego Airplane image with 31064 mapped bits, (c) is the stego Airplane image with 74832 mapped bits and (d) is the stego Airplane image with 96144 mapped bits. It is clear from the Figure 6 that visual appearance of the stego images is very good. It is impossible to make a distinction between cover image and stego images by human perception.



(a) Cover image (b) Stego image with 31064 bits (c) Stego image with 74832 bits (d) Stego image with 96144 bits

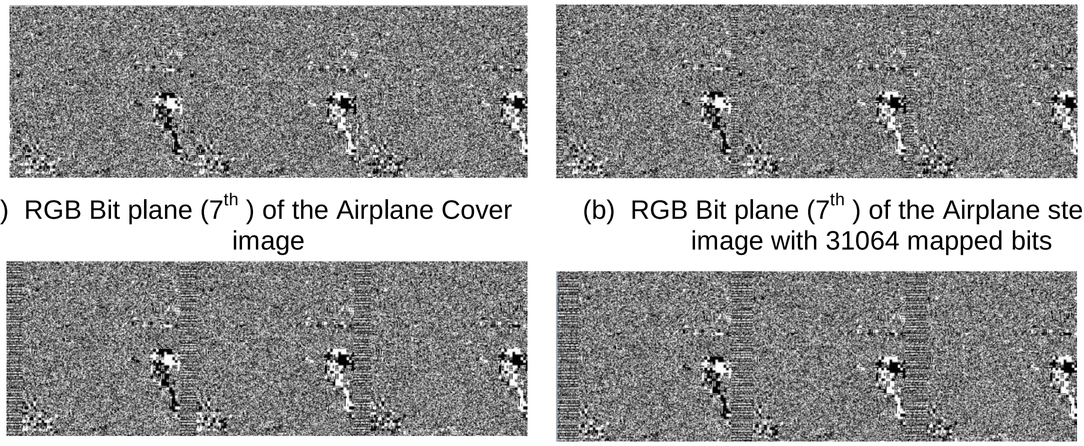
Figure 6. Cover and Stego Color images

Table 2 shows the result of image quality measures (IQMs) and security analysis (SA) evaluated between the cover image and stego images of the Figure 6.

Table 2. Result of IQMs and SA between the Cover Image and Stego Images of Figure 6

IQM	31064	74832	96144	Security Analysis	31064	74832	96144
MSE	0.01956	0.04764	0.06132	Jaccard	0.99999	0.99999	0.99998
PSNR	65.1548	58.6599	60.2502	Intersection	0.99993	0.09999	0.99981
UIQI	0.99999	0.99999	0.99998	Correlation	0.99999	0.99998	0.99998
SSIM	0.99999	0.99999	0.99998	Chi-Square	5.46461	0.00013	0.00017
IF	0.99999	0.99999	0099999	Bhattacharya	0.00028	0.00046	0.00054
NCC	0.99999	0.99999	0.99999				
AD	0.00223	0.00502	0.00663				

Figure 7 shows the BPA of the images of Figure 6. If 0 to 7 are the eight bit planes of the R component, 0 to 7 are the eight bit planes of the G component and 0 to 7 are the eight bit planes of the B component of a RGB image, then the 7th bit plane of the RGB component of the color images of Figure 6 are shown in Figure 7. In Figure 7 (a) is the 7th bit planes of RGB component of the cover image of Figure 6 (a). In Figure 7 (b, c and d), inconsistency of the 7th bit planes of RGB component is clearly visible.



(a) RGB Bit plane (7th) of the Airplane Cover image

(b) RGB Bit plane (7th) of the Airplane stego image with 31064 mapped bits

(c) RGB Bit plane (7th) of the Airplane stego image with 74832 mapped bits

(d) RGB Bit plane (7th) of the Airplane stego image with 96144 mapped bits

Figure 7. Bit Plane Analysis (BPA) of Cover and Stego Images of Figure 6

Table 3 shows the investigation of all the grayscale levels for formulating the rules for the worst case situation. BP denotes the boundary pixel. In GLM method, boundary pixels, having grey level 0 and 255, will not be used for mapping as BP does not fulfill the criteria.

Table 3. Investigation of Gray Levels for Worst Case Analysis

Grey Level	Even	Insertion of 0	Insertion of 1
0	BP	BP	BP
1	+1	NC	-1
2	NC	NC	-1
3	+1	NC	-1
4	NC	NC	-1
5	+1	NC	-1
. . .	. . .	. . .	. . .
253	+1	NC	-1
254	NC	NC	-1
255	BP	BP	BP

From Table 3, following conclusion and worst case situation are drawn:

1. As the BP are not used for mapping so there are 99.21% chances of mapping at first attempt.
2. If the image contains large number of BP then the other pixels then this is a situation of worst case.
3. When the selected pixels are all odd and bit stream contains mostly the odd bits. This is also a worst case situation. In such case all selected pixel will incremented by one before mapping.

4. Comparison with the LSB Matching and Substitution [3, 5, 13]

LSB substitution and LSB matching method of steganography are simple and old methods. Table 4 shows the comparison between LSB substitution/matching and GLM method of steganography.

Table 4. Comparison of LSB Substitution/Matching with GLM Steganography

LSB Substitution/ LSB Matching [3, 5, 13]	GLM Method
Simple to implement.	Simple to implement.
Perform replacement for LSB substitution and adjustment for LSB matching.	Perform one-to-one mapping.
Creates least changes in image statistical properties.	Creates least changes in image statistical properties.
100% chances of insertion at first chance.	99.21% of chances of mapping at first attempt as the boundary pixels are not used in mapping.
In retrieval process, if the LSB is 0 then 0 is the message bit and if the LSB is 1 then 1 is the message bit.	In retrieval process, it the pixel value is even then 0 is the bit stream and if the value is odd then 1 is the bit stream.
Due to noise or hardware imperfection message bits can be lost.	Due to noise or hardware imperfection, an even pixel become odd and odd becomes even resulting in loss of bit stream.
Least bit plane show visual inconsistency due to substitution/matching.	Least bit plane show visual inconsistency due to mapping.

5. Conclusions

This paper presents the deep analysis of the GLM method of steganography. Analysis shows that the scheme is good in terms that it maps the bit stream with such a technique that visually and statistically changes are least. For human perception, it is impossible to make difference between the cover and stego image. As it uses a concept of even and odd pixels, so the drawback associated with this scheme is that the noise, due to hardware imperfection or transmission medium, can make the odd pixels to even and vice versa resulting in annihilation of bit stream. Moreover its comparison to LSB substitution and LSB matching shows that in both the cases the drawback is similar with the difference being that GLM performs mapping while substitution perform replacement and matching perform adjustment. This review is the helpful analysis for the people who want to work in the field of information security to understand the basic steganographic schemes and present new schemes.

References

[1] V. M. Potdar and E. Chang, “Grey Level Modification Steganography for Secret Communication”, 2nd IEEE Conference on Industrial Informatics, Berline Germany, **(2005)** June 24th -26th.

[2] A. Rashid and M. K. R. Rashid, “Stego-Scheme for Secret Communication in Grayscale and Color Images”, British Journal of Mathematics and Computer Sciences, vol. 10, no, 1 **(2015)**, pp. 1-9.

[3] M. K. R. Rashid, A. Rashid, N. Salamat and S. Missen, “Experimental Analysis of Matching Technique of Steganography for Grayscale and Color Image”, International Journal of Computer Science and Information Technology, vol. 6, no. 6, **(2014)**, pp. 157-166.

[4] A. Rashid, “Robust Electronic Communication Scheme in Spatial Domain”, British Journal of Mathematics and Computer Sciences, vol. 7, no. 3, **(2015)**, pp. 218-228.

[5] A. Rashid, “Experimental Analysis and Comparison of LSB Substitution and LSB Matching Method of Information Security”, IJCSI, vol. 12, no.1, **(2015)**, pp. 91-100.

[6] M. K. R. Rashid, N. Salamat, S. Missen and A. Rashid, “Robust Increased Capacity Image Steganographic Scheme”, International Journal of Advanced Computer Science and Applications, vol. 5, no. 11, **(2014)**, pp. 125-131.

[7] I. Avcibas, B. Sankur and K. Sayood, “Statistical Evaluation of Image Quality Measure”, Journal of Electronic Imaging, vol. 11, no. 2, **(2002)**, pp. 206-223.

[8] Z. Wang, Member and H. R. Sheikh, “Image Quality Assessment: From Error Visibility to Structural Similarity”, IEEE Transactions On Image Processing, vol. 13, no. 4, **(2004)**.

[9] Y. A. Y. Al. Najjar and Dr. D. C. Soong, “Comparison of image quality assessment: PSNR, HVS, UIQI, SSIM”, IJSER, ISSN2229-5518, vol. 3, no. 8, **(2012)**.

[10] A. Saffor, A. R. Ramli and K.H. Ng, “A Comparative Study Of Image Compression Between Jpeg And Wavelet”, Malaysian Journal of Computer Science, vol. 14, no. 1, **(2001),** pp. 39-45.

[11] H. R. Sheikh, M. F. Sabir and A. C. Bovik, “A Statistical Evaluation of Recent Full Reference Image Quality Assessment Algorithms”, IEEE TRANS. IMAGE PROCESSING, **(2006)**.

[12] V. Asha, P. Nagabhushan and N. U.Bhajantri, “Similarity Measures for Automatic Defct Detection on Patterned Texture”, International Journal of Image Processing and Vision Science, vol. 1, **(2012)**.

[13] N. F.Johnson and S. J. G. Mason University, “Exploring Steganography: Seeing the Unseen”, 0018-916/98/$10.00© IEEE, **(1998)**.

Authors

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 received her Master's degree in Computer Sciences (MCS) (Gold Medalist) from 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.