International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

Data Hiding in Image Using Modified Minimum Reference Pixel-Based Steganographic Method with Random Pixel Block Selection Algorithm

May Htet[1], Jay R. Rajasekera[2]
[1]Department of Computer Engineering and Information Technology, Mandalay Technological University, Mandalay, Mandalay Division, Myanmar, +95
[2]Graduate School of Business and Commerce, Tokyo International University, Kawagoe, Saitama Prefecture, Japan, +81
Email address: [1]mayhtet@mtu.edu.mm, [2]jrr@tiu.ac.jp

***Abstract*—*Nowadays, most of the information are kept electronically due to the advances in information and communication technology. Consequently, information security becomes a fundamental issue. Steganography can be employed to secure the secret data by hiding its presence in multimedia carriers (text, image, audio, and video.) during storage and transmission. Among different carrier formats, digital image are the most popular objects due to the presence of redundant information in image which can be modified without perceptual transparency in embedding process. Hence, the main aim of this paper is to propose an efficient image steganographic technique for secure data hiding system based on Minimum Reference Pixel-Based Steganographic Algorithm (MRPSA). In the proposed system, the pixel positions in image are randomly selected using proposed Random Pixel Block Selection Algorithm (RPBSA) before hiding the secret message in order to make more difficult steganalysis for intruders. In addition, using proposed embedding algorithm, only two bits of secret message is hidden in Red channel of each pixel of the cover image depending on the random selected position to preserve the image quality. Therefore, the generated stego image will not attract much attention to intruders and meet the security requirement of steganographic system.*

***Keywords*—** *Average Difference (AD), Image Steganography, Peak Signal-to-Noise Ratio (PSNR), Proposed Embedding Algorithm, Random Pixel Block Selection Algorithm.*

I. INTRODUCTION

The wide spread use of internet for communication has increased the attacks to users. One of the reasons that intruders can be successful is that most of the information they acquire from a system is in a form that they can read and comprehend. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. One solution to this problem is through the use of steganography.

Steganography is a technique of hiding information in digital media. The main goal of steganography is to communicate securely in a completely undetectable manner [1] and to avoid drawing suspicion to the transmission of the hidden data. It is not to keep others from knowing the hidden information, but it is to keep others from thinking that the information even exists. If a steganography method causes someone to suspect the carrier medium, then the method has failed [2]. Depending on the type of the cover object, steganography is classified by text steganography, image steganography, audio steganography and video steganography.

In this paper, image file is considered as cover medium and an efficient embedding method which can provide better security level for secret message is employed for hiding the secret message into the cover image so as to provide a more secure information hiding system

The rest of the paper is organized as follows: Section II presents earlier works and recent researches on image steganography. Section III depicts the general model of the proposed system. Section IV and V discusses research methods. Section VI shows the performance analysis of the proposed approach. Section VII draws the conclusion.

II. RELATED WORKS

There has been tremendous research in the field of image steganography to ensure the secure data transmission through unreliable communication media. Some of the previous image steganography works are listed below.

T. Morkel, J. H. P. Eloff, and M. S. Oliver [3] mentioned that image steganography is a process which hides the message into cover image and generates a stego image. To hide a message inside an image without changing its visible properties, the cover source can be altered in noisy areas with many color variations, thus less attention will be drawn to the modifications. The most common methods to achieve these modifications involve the usage of the least significant bit or LSB, masking, filtering and transformations on the cover image. These techniques can be used on different types of image files with varying degrees of success.

In the paper [4], P. M. Tanvir and G. A. Abdul-Aziz presented a pixel indicator technique with variable bits; it chose one channel among red, green and blue channels and embedded data into variable LSB of chosen channel. The intensity of the pixel decided the variable bits to embed into cover image. The channel selection criteria were sequential and the capacity depends on the bits of channel in cover image. This technique has almost the same histograms of cover and stego images.

Then, R. K. Venkata, B. B. Raveendra, and B. Sri-Ratna, proposed a secure data hiding algorithm for color image using random transformation and file hybridization. Random transformation and file hybridization makes the tasks of steganalysis difficult. However, this method can hide the secret message of only 26 English alphabets and 10 digits [5].

Besides, A. Sneha and A. Sanyam [6], proposed a technique to hide the text data into the color images using

May Htet and Jay R. Rajasekera, "Data hiding in image using modified minimum reference pixel-based steganographic method with random pixel selection algorithm," *International Research Journal of Advanced Engineering and Science*, Volume 4, Issue 1, pp. 34-39, 2018.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

edge detection method. The alteration in edges cannot be distinguished well so edges can hide more data without losing quality of an image. In this technique, Edges of an image are detected by scanning using 3x3 window and then text message is concealed in edges using the first component alteration technique. The proposed scheme achieved high embedding capacity and high quality of encoded image.

Moreover, B. Indradip, B. Souvik, and S. Gautam [7] proposed a novel Pixel Factor Mapping (PFM) method based on spatial domain with the help of Gray scale images (512x512). In this method, random pixel are selected by pixel selection algorithm using mathematical member function based on pixel intensity value and pixel position on image and four bit pair of secret message is embedded in a separate pixel using the mapping technique with the help of maximum prime factor value of pixel intensity value and pixel selection method. Embedding four bit per pixels can extend the embedding capacity four times than other methods but it causes much degradation to the cover image.

In accordance with literature and ideas from earlier works, the primary intention of this research is to provide an efficient image steganographic technique based on the modification of Minimum Reference Pixel-Based Steganographic Algorithm (MRPSA) for achieving the better security level of secret message through random pixel block selection approach.

III. Proposed System Achitecture

The proposed system is organized with two portions: sender site and receiver site as shown in Fig. 1.

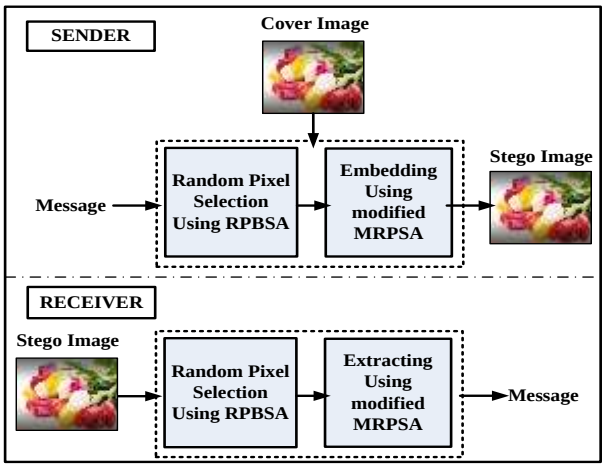


Fig. 1. Proposed system design.

A. Processes of Sender Site

1. Get the secret message.
2. Select the cover image.
3. Choose the random pixel blocks from cover image using RPBSA.
4. Perform secret message embedding using the modified MRPSA method to obtain stego image.
5. Send the stego image to the receiver site over the communication channel.

B. Processes of Receiver Site

1. Get the stego image.
2. Choose the random pixel blocks from stego image using RPBSA.
3. Extract the secret message from the stego image using the modified MRPSA.
4. Obtain the original message.

IV. Minimum Reference Pixel-Based Steganographic Algorithm

In this minimum reference pixel-based steganographic algorithm (MRPSA), the color image is used as a cover image. Then, the cover image is divided into blocks of size (3 by 3) pixels. If the width or height of the image is not a multiple of 3, zero pixels values are added as padding pixels. Second step is to manipulate the values of pixels in every pixel block. The pixel with minimum intensity value is selected as reference pixel (P_{min}) for each pixel block. Then, the difference (D) values are calculated between the reference pixel and remaining pixel values ($D= P-P_{min}$). In addition, the maximum value of these differences is determined in the block (Max (D)). Third step is to determine the greatest value of all maximum differences among all blocks (greatest Max (D) in whole image). After that, the number of bits (N), which is enough to store this greatest Max (D) value, is determined. Fourth, the pixel values of cover image and the secret message are converted into binary values (M_b). Fifth step is a frequent swap process for each pixel other than the minimum pixel. The N rightmost bits are swapped to N leftmost places and the rightmost bits (8−N) are replaced with secret message bits. The embedding process is repeated by sequentially selecting the pixel blocks until all the message bits are hidden. Finally, the pixel blocks are combined together to obtain the stego image.

At the receiver site, firstly the stego image is divided into blocks of size (3 by 3) pixels. Secondly, the value of N is checked. From the sequential positions, the reference pixel (P_{min}) is checked for each pixel block. In third step, every pixel values of stego image (I') are converted into binary values. Fourth step is a frequent swap process. For each pixel block, the N leftmost bits of stego pixel are swapped with (8−N) rightmost bits. After that, left-side binary data are extracted and it is stored in a temporary list (M'). At last, all the bits in the M' are concatenated to obtain the message bit stream (M_b). Then, all the message bit streams are converted into original secret message (M) [8]. The example embedding and extracting processes of MRPSA are demonstrated from Fig. 2 to Fig. 9.

8	1	6	124	127	126	115	118	113	25	28	33
3	5	7	124	123	125	111	116	120	27	29	30
4	9	1	116	128	129	118	113	113	22	25	24
13	16	28	101	103	109	115	108	101	14	29	16
30	20	27	112	108	116	110	108	101	14	29	29
25	25	22	116	109	115	113	108	101	14	28	15
89	82	87	146	145	141	125	128	121	13	19	16
84	86	88	148	148	142	123	128	121	13	25	20
85	90	83	141	140	143	123	128	121	13	20	28
36	28	29	119	120	112	113	108	101	13	28	22
39	24	26	113	122	120	113	108	101	13	28	16
26	28	39	114	124	126	113	108	101	13	28	23

Fig. 2. Dividing the pixel block and finding reference pixel.

May Htet and Jay R. Rajasekera, "Data hiding in image using modified minimum reference pixel-based steganographic method with random pixel selection algorithm," *International Research Journal of Advanced Engineering and Science*, Volume 4, Issue 1, pp. 34-39, 2018.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

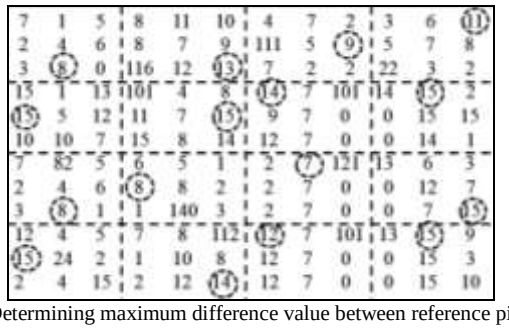


Fig. 3. Determining maximum difference value between reference pixel and other pixels.

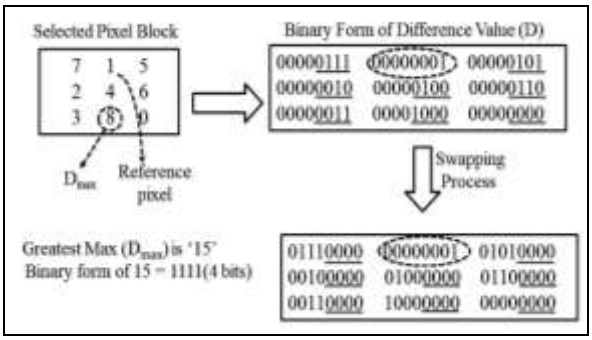


Fig. 4. Swapping the binary value according to Max (D_{max}).

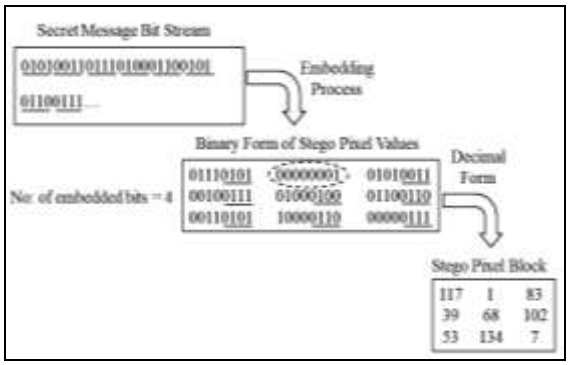


Fig. 5. Embedding the secret bits in selected pixel block.

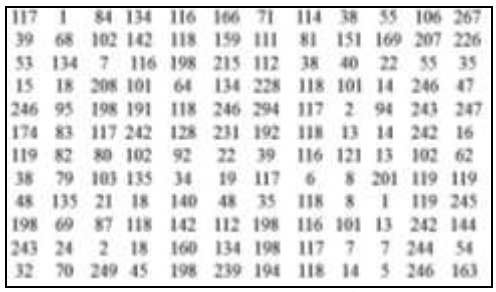


Fig. 6. Merging the stego pixel blocks to form stego image.

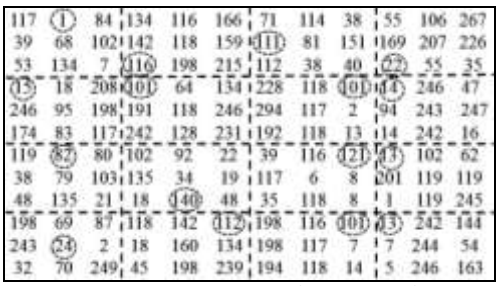


Fig. 7. Dividing the stego image and finding the reference pixel

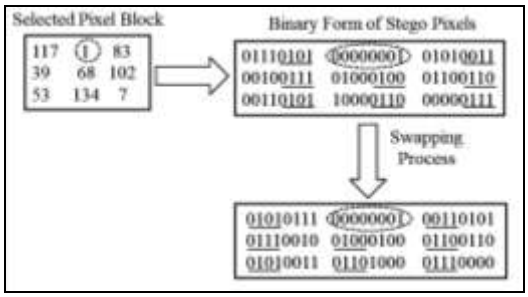


Fig. 8. Swapping the binary value of stego pixel and extracting the leftmost 4 bits.

0101 0011 0111 0100 0110 0101 0110 0111…

Fig. 9. Original message.

As mentioned above, the original MRPSA choose the sequential pixel blocks from the cover image and used the swap operation in embedding process, there is much degradation in image quality causing the stego image looks suspicious compared to the original cover image.

Hence, in this paper, it is considered to modify it. The modified MRPSA algorithm is discussed in next section.

V. Modified Minimum Reference Pixel-based Steganographic Algorithm

In this modified MRPSA algorithm, the random pixel blocks are selected according to the random pixel block selection algorithm (RPBSA) prior to embedding process in order to scatter the secret message. In addition, for the goodness of image quality, it is considered to replace the secret message bits in 2LSB bits of only one channel of each pixel in the selected block. (Red channel is considered in this paper and either Green, or Blue can also be used).

A. Random Pixel Block Selection Algorithm

The proposed Random Pixel Block Selection Algorithm (RPBSA) is used before the embedding process for choosing the random pixel blocks. The step-by-step procedures of RPBSA are shown in Fig. 10.

Step 1: Divide image (I) of size (m x n) into 3 x 3 pixel blocks, if $m\%3 \neq 0$ or $n\%3 \neq 0$, pad with additional zeros.
Step 2: Compute the difference (D) in absolute value between the product of 1st pixel value and 9th pixel value and that of 3rd pixel value and 7th pixel value in each pixel block.
Step 3: Determine the largest value of the difference (D_{max}) among the pixel blocks.
If $D = D_{max}$, then select the pixel block and use it as a first pixel block for embedding process.
Or else, skip the block and check another block.
Step 4: Select the remaining pixel block according to the descending order of D_{max}.
Step 5: If the difference of the pixel values of the blocks are the same, then select the pixel block at the leftmost position and use it as a first pixel block for embedding process.
Step 6: Repeat step 3 to 5 until all pixel blocks are selected.

Fig. 10. The step-by-step procedures of RPBSA.

The example of proposed RPBSA is illustrated in Fig. 11 to Fig. 14.

May Htet and Jay R. Rajasekera, "Data hiding in image using modified minimum reference pixel-based steganographic method with random pixel selection algorithm," *International Research Journal of Advanced Engineering and Science*, Volume 4, Issue 1, pp. 34-39, 2018.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

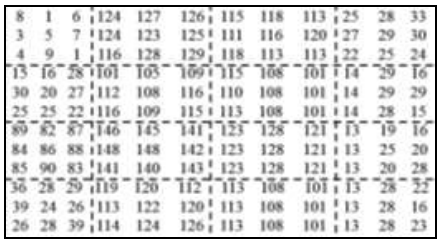


Fig. 11. Dividing the cover image to pixel blocks.

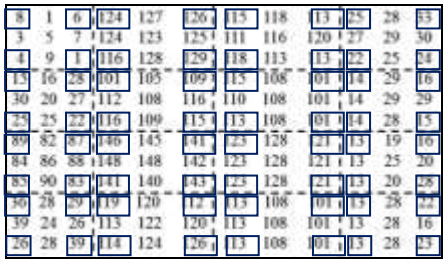


Fig. 12. Selecting the four pixel values at the corners of each block.

Then, the difference (D) in absolute value is calculated for each pixel block as shown in Fig. 13.

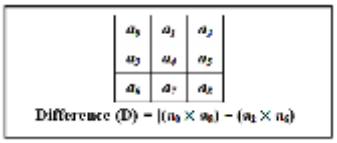


Fig. 13. Example calculation of difference value.

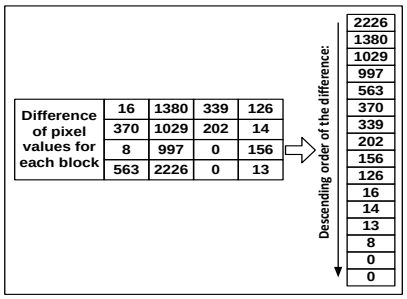


Fig. 14. Choosing the order of pixel block according to the difference of pixel values at the corners of each block.

B. Embedding Procedure

The step-by-step procedures of message embedding process are described in Fig. 15.

Input: Cover image (I), Secret message (M)
Output: Stego image (I')
Step 1: Select the pixel block in cover image (I) according to the Random Pixel Block Selection Algorithm.
Step 2: Exclude the pixel values at the corners and select the remaining pixel values in each block for embedding process.
Step 3: Convert every pixel values of image (I) to its binary values.
Step 4: Convert the secret message characters to binary values (Mb).
Step 5: If M_b size $\neq 0$, then
2LSB of difference (D) values are replaced with 2 bits of M_b for each pixel in the block B other than the pixels at the corner and is stored as stego pixel (P_s).
Go to step 7.
Step 6: Else
Step 7: Convert the binary pixel values to the decimal values and get the final pixel block with embedded message.
Step 8: Merge all the pixel blocks after embedding the secret message (Mb) into the cover image (I).

Fig. 15. The step-by-step procedures for embedding process.

The example embedding process of modified MRPSA is shown in Fig. 16 to Fig. 19.

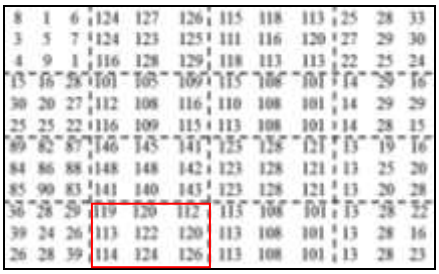


Fig. 16. Selecting the pixel block according to the proposed RPBSA.

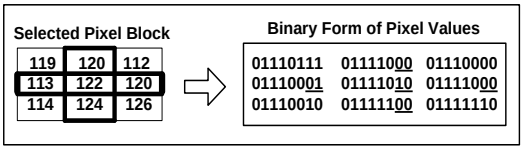


Fig. 17. Converting the pixel values of selected pixel block to binary form.

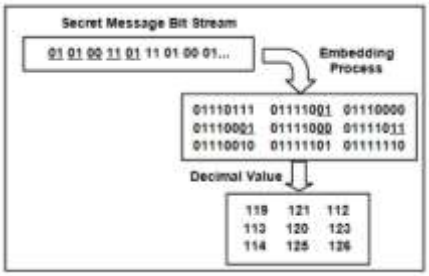


Fig. 18. Embedding the secret bits in selected pixel block

8	0	6	124	125	126	115	119	113	25	29	33
3	6	7	125	123	125	112	116	120	26	29	31
4	8	1	116	127	129	118	112	113	22	25	24
15	14	28	101	104	109	115	107	101	14	27	16
31	20	26	111	107	116	111	108	102	13	28	28
25	26	22	116	108	115	113	109	101	14	29	15
89	81	87	146	144	141	123	129	121	13	18	16
85	87	88	147	148	143	115	119	113	13	26	21
85	91	83	141	139	143	115	119	113	13	22	28
36	27	29	119	122	112	113	107	101	13	29	22
38	24	26	114	123	121	114	108	102	14	27	17
26	27	39	114	124	126	113	109	101	13	29	23

Fig. 19. Merging the stego pixel blocks to form stego image.

C. Extracting Procedure

The step-by-step procedures of message extracting process are shown in Fig. 20.

Input: Stego image (I')
Output: Cover image (I), Secret message (M)
Step 1: Select the pixel block in stego image (I') according to the Random Pixel Block Selection Algorithm.
Step 2: Exclude the pixel values at the corners and select the remaining pixel values in each block for extracting process.
Step 3: Convert every pixel values of stego image (I') to its binary values.
Step 4: Extract 2LSB of each data embedding pixel in the block B other than the pixel at the corners and store them in a temporary list (M').
Step 5: Repeat step 2 to 4 until all the hidden bits are extracted.
Step 6: Concatenate all the bits in the M' to obtain the message bit stream (M_b).
Step 7: Convert the M_b back to its original format to get the original secret message (M).

Fig. 20. The step-by-step procedures for extracting process.

May Htet and Jay R. Rajasekera, "Data hiding in image using modified minimum reference pixel-based steganographic method with random pixel selection algorithm," *International Research Journal of Advanced Engineering and Science*, Volume 4, Issue 1, pp. 34-39, 2018.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

The example extracting process of modified MRPSA is depicted in Fig. 21 and Fig. 22. The pixel order is selected using the same Random Pixel Block Selection Algorithm as the sender site.

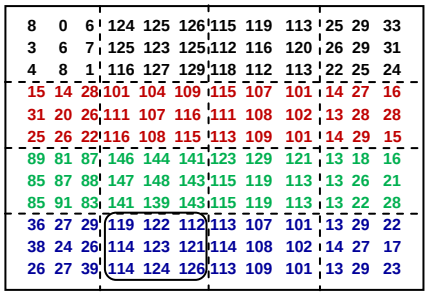


Fig. 21. Dividing the stego images into pixel blocks and selecting the first pixel block

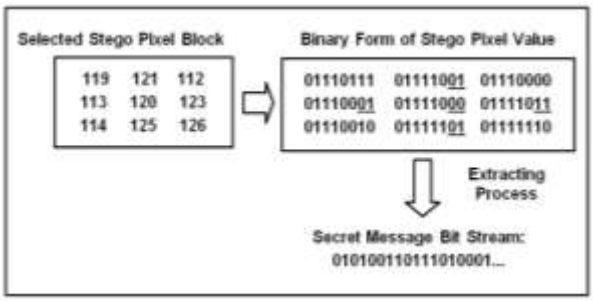


Fig. 22. Extracting 2LSB of each pixel to obtain secret message

VI. Experimental Results

To aware how much distortion caused by embedding effect, image quality is needed to be measured before and after inserting the data in cover image. In this paper, the quality of image is measured in terms of Peak Signal-To-Noise Ratio (PSNR) and Average Difference (AD) based on four different image resolution (128*128), (256*256), (512*512) and (1024*1024) of Lena image with text message size of 356 bytes to evaluate the performance of original and proposed MRPSA.

A. Peak Signal-to-Noise Ratio

Peak Signal-to-Noise Ratio (PSNR) is the measure of image quality by comparing the cover image with the stego image. PSNR is inversely proportional to the MSE. It is expressed in logarithmic decibel (dB). The PSNR is defined by using (1).

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{255}{\sqrt{\mathrm{MSE}}}\right)\mathrm{dB} \quad (1)$$

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

where Mean Square Error (MSE) is the measure of error between the original image and the reconstructed image, f represents the matrix data of original image, g represents the matrix data of stego image, m represents the number of rows of pixels in the images and i represents the index of that row, n represents the number of columns of pixels in the image and j represents the index of that column.

B. Average Difference

Average Difference (AD) is the percentage of the modified pixel values between the cover and the stego images [9]. The AD is defined by using (3).

$$\mathrm{AD} = \left(\frac{1}{\mathrm{m}\times\mathrm{n}}\right)\sum_{i=0}^{m}\sum_{j=0}^{n}\left(f(i,j) - g(i,j)\right) \quad (3)$$

The experimental results prove that the PSNR and AD values of modified MRPSA are higher when comparing that of MRPSA as shown in Table I. Therefore, the modified algorithm provides better stego image quality and there is no major change for the quality of stego image generated by modified MRPSA. In addition, the maximum numbers of characters which can be hidden in different cover image sizes are also described in Table II.

TABLE I. Comparison results of PSNR, MSE and AD values.

Image Resolution	Original MRPSA			Modified MRPSA		
	PSNR (dB)	MSE	AD	PSNR (dB)	MSE	AD
(128*128)	29.60	2.07	2.12	59.9	0.0150	0.0160
(256*256)	35.62	0.53	0.53	65.52	0.006	0.0048
(512*512)	41.80	0.15	0.13	71.80	0.0017	0.0020
(1024*1024)	48.05	0.04	0.03	77.70	0.0019	0.0002

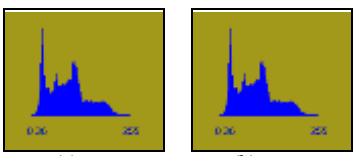
TABLE II. Maximum number of embedded characters.

Image Resolution	Maximum Number of Embedded Characters	
	Original MRPSA	Modified MRPSA
(128*128)	Variable Number of Characters Depending on Swap Operation in Embedding Process	2170
(256*256)		9102
(512*512)		36408
(1024*1024)		145636

Besides, the experiments have been done using histogram analysis [10] for evaluating the performance of modified MRPSA. The test is carried out based on three different original images. The cover images and stego images of size (512×512) with text data (356 bytes) and their respective histograms are illustrated in Fig. 23 to Fig. 28.

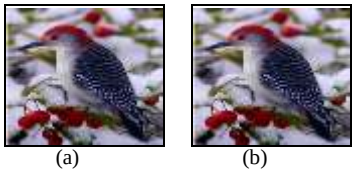
(a) (b)

Fig. 23. Lena.bmp (a) cover image (b) stego image with text data.



(a) (b)

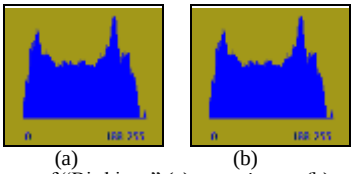
Fig. 24. Histogram of "Lena.bmp" (a) cover image (b) stego image with text data.



(a) (b)

Fig. 25. Bird.jpeg (a) cover image (b) stego image with text data.

May Htet and Jay R. Rajasekera, "Data hiding in image using modified minimum reference pixel-based steganographic method with random pixel selection algorithm," *International Research Journal of Advanced Engineering and Science*, Volume 4, Issue 1, pp. 34-39, 2018.

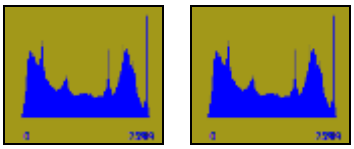


(a) (b)

Fig. 26. Histogram of "Bird.jpeg" (a) cover image (b) stego image with text data.

(a) (b)

Fig. 27. "MTU.jpg" (a) cover image (b) stego image with text data.



(a) (b)

Fig. 28. Histogram of "MTU.jpg" (a) cover image (b) stego image with text data.

As it can be seen in figures, there is no damage in cover image since the histograms of cover images and stego images are almost identical in appearance and no one can see the differences between the two files. Hence, it can be said that the proposed embedding algorithm provides the good stego image quality as cover image and is efficient for the proposed system.

VII. Conclusion

The performance comparison of proposed embedding method and MRPSA is presented in this paper. In this paper, the modified MRPSA produces stego image with better quality as it does not use swap operation in embedding process. Besides, only two LSB bits of every pixel in each block is modified in embedding process instead of variable numbers of bits modified in original MRPSA. In addition, the modified method provides better security level as it uses the Random Pixel Block Selection algorithm as a pre-processing step prior to embedding process. Therefore, even if the interceptors knows the method of embedding, only disseminated secret message can be obtained leading to difficult situation for getting the real order of secret message. Moreover, histogram analysis, the histograms of cover image and stego image are almost identical before and after inserting the data. Hence, even if the interceptors get both cover and stego files, they cannot discriminate any discrepancy between the two files.

This proposed method can be applied in any security awareness applications. As further extensions, it can be enhanced by integrating with other embedding methods to achieve more efficient method.

Acknowledgment

The authors would like to thank all the anonymous reviewers in Myanmar and Japan who helped in making improvement the quality of this journal. The author would also like to acknowledge the Department of Computer Engineering and Information Technology, Mandalay Technological University, Ministry of Education, Myanmar and Graduate School of Business and Commerce, Tokyo International University, Japan for giving the opportunity of this research submission.

References

[1] N. F. Johnson and S. Jajodia, "Steganalysis of images created using current steganography software", *in Proceedings The Second Information Hiding Workshop, Portland Oregon, USA*, pp. 273-277, 1998.

[2] N. Provos and P. Honeyman, "Detecting steganography content on the internet", CITI Tech. Rep. 01-11, 2001.

[3] T. Morkel, J. H. P. Eloff, and M. S. Oliver, "An overview of image steganography", *in Proceedings ISSA'05*, pp. 1-11, 2005.

[4] P. M. Tanvir and G. A. Abdul-Aziz, "RGB intensity based variable-bits image steganography", *IEEE Asia-Pacific Services Computing Conference, 1st International Workshop on Multimedia, Information Privacy and Intelligent Computing Systems*, pp. 1322-1327, 2008.

[5] R. K. Venkata, B. B. Raveendra, and B. Sri-Ratna, "A randomized secure data hiding algorithm using file hybridization for information security," *International Journal on Computer Science and Engineering (IJCSE)*, vol. 3, no. 5, May 2011, pp. 1878-1889.

[6] A. Sneha and A. Sanyam, "A proposed method for image steganography using edge detection, *International Journal of Emerging Technology and Advanced Engineering*, vol. 3, issue 2, pp. 22-25, 2013.

[7] B. Indradip, B. Souvik, and S. Gautam, "Study and analysis of steganography with pixel factor mapping method", *International Journal of Application or Innovation in Engineering & Management (IJAIEM'13)*, vol. 2, issue 8, pp. 258-266, 2013.

[8] E. Mohammad, E. Mohammed, A. Ahamed, and E. Rasha "A proposed technique for data hiding in video files", *International Journal of Computer Science Issues*, vol. 11, issue 2, pp. 68-77, 2014.

[9] P. Vidya, S. Veni, and K. A. Narayanankutty, "Performance analysis of edge detection methods on hexagonal sampling grid", *International Journal of Electronic Engineering Research*, vol. 6, issue 1, pp. 313-328, 2009.

[10] X. Zhang and S. Wang, "Vulnerability of pixel value differencing steganography to histogram analysis and modification for enhanced security", *Pattern Recognition Letters*, vol. 25, issue 3, pp. 331-339, 2004.