Comparison of Least Significant Bit, Pixel Value Differencing, and Modulus Function on Steganography to Measure Image Quality, Storage Capacity, and Robustness

Comparison of Least Significant Bit, Pixel Value Differencing, and Modulus Function on Steganography to Measure Image Quality, Storage Capacity, and Robustness

D Darwis[a,b] N B Pamungkas[a], Wamiliana[c]

[a] Faculty of Engineering and Computer Science, Universitas Teknokrat Indonesia, Indonesia
[b] Postgraduate Doctor of Mathematics and Natural Sciences, Universitas Lampung, Indonesia
[c] Department of Mathematics, Universitas Lampung, Indonesia

email: darwisdedi@teknokrat.ac.id[a,b], nurhuda.budi@teknokrat.ac.id[a], wamiliana.1963@fmipa.unila.ac.id[c]

Abstract. Information security is an important aspect of information. The importance of the value of information in every aspect can result in attempts to transfer access or theft of data and information by unauthorized parties. One technique for securing data and information is by applying the digital image steganography technique. Many methods can be used in steganography, some of which are Least Significant Bit (LSB), Pixel Value Differencing (PVD), and Modulus Function (MF). Good steganography must produce a stego-image with an image quality that is not different from the original image or what is called a cover image and has the storage capacity to store confidential data and is resistant to robustness. The purpose of this study was to compare the LSB, MF, and PVD methods to serve as alternatives to the use of steganography techniques. The results of this study indicate that the LSB method has the best image quality compared to the MF and PVD methods. For storage capacity, the PVD algorithm has a better capacity than the LSB and MF methods. Meanwhile, the robustness of the LSB, PVD, and MF methods has resistance to cropping with a percentage of 10% at the bottom of the stego-image.

Keyword: Fidelity, Image Steganography, LSB, MF, PVD, Robustness

1. Introduction

Nowadays almost everything is communicated using digital technology, from everyday conversations to sensitive or confidential information [1]. Security issues in the exchange of data from sender to receiver are of the utmost concern because the importance of the value of information in every aspect can support attempts to transfer access or steal data and information by ignorant parties [2, 3]. The media for storing and distributing data or information used is one of the reasons for the vulnerability of data or information being easily retrieved by irresponsible parties. This is due to the inefficient security system in protecting the confidentiality of data and information [4, 5]. Many techniques can be used to secure information including encryption, watermarking, digital watermarking, reversible watermarking, cryptography, steganography and others [6].

This research discusses how to secure data using digital image steganography. Steganography is a science that deals with the secret security of data embedded in media such as images, text, audio and video to make it difficult for third parties to detect messages but can obtain confidential data when data is sent via public channels [7]. Steganography techniques recommend several algorithms or methods that can be used to secure classified information. Some of the methods that are often used are the Least Significant Bit (LSB) method, Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), Pixel Value Differencing (PVD), Modulus Function (MF), and other methods.

A good image steganography technique has several main aspects, first is capacity (the maximum data that can be stored in the cover image), second is fidelity (measuring image quality) and the last is robustness [8, 9]. Concealing confidential data into a digital image will change the quality of the original image, therefore in using the steganography method, good aspect criteria must be considered. Steganography has several techniques for hiding data with a larger size, but if the size of the data is larger, the image quality will deteriorate, so the method of image steganography is not feasible to achieve good steganography characteristics.

A common problem in steganography is that the quality of the image produced by the stego-image decreases due to changes in pixels on the cover image. Changes in pixel value due to messages inserted in the cover image cause the storage capacity in the stego-image to be larger. Besides, the resistance of stego-images to attacks such as cropping is a problem in steganography because in general the message on the cropped stego-image cannot be extracted. [10]. This research discusses the comparison between the Least Significant Bit (LSB), Pixel Value Differencing (PVD), and Modulus Function (MF) methods to find out which method is the best in terms of image quality, storage capacity, and resistance to attack so that it can be used as an alternative material consideration when using any of the three methods. The LSB method was chosen because the quality in the LSB method can be measured by calculating the Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) values. The LSB method is a technique commonly used in encryption and decryption in steganography, the way it works is to change the cover image bit which does not significantly affect the bits of the secret message. The stego-image produced by the LSB method is not too different from the cover image so that it can avoid suspicion from the human perspective. [11]. Two further methods were utilized to perform image comparison analysis to the LSB. The first is the PVD method which uses the difference value between two consecutive blocked pixels to determine how many secret bits must be embedded. The second one is the MF method which is the development of the PVD method by generating new pixel values adjusted in the process of planting and to recover classified information [12]. This study aims to determine the comparative value of image quality, storage capacity, and image resilience, especially when the stego-image is cropped.

2. Data and Method

2.1. Data

The data used in this study is a cover image in the form of *.jpg* or *.png* format with an image resolution of 512 x 512 in the form of grayscale images and RGB images from primary images and secondary images (images taken from the internet) [6]. Meanwhile, for the secret messages using text is stored in a *.txt* file format.

2.2. Method

1. Least Significant Bit (LSB)

The Least Significant Bit (LSB) method is a fairly simple method in steganography. The working method of the LSB method is that the message is inserted into the cover image at the last bit or the bit that is less meaningful so that changes to the cover image are not significant. Each 1 byte of the image size is 8 bits long. The message bit is inserted in the last bit of the cover image so that the changes in the resulting stego-image are almost the same as the cover image used. [13]. In this study, the approach of the LSB method for the message insertion process is as follows:

1. Convert the message to an 8-bit binary number.
2. Insert message bits into image pixels starting from MSB (Most Significant Bit) in the following way:
   a) If (message bit = 1 and pixel_image mod 2 = 1) or (message bit = 0 and pixel_image mod 2 = 0) then: new_pixels_image = old_pixels_image (Fixed)
   b) If (message bit = 1 and pixel_image mod 2 = 0) then: new_pixels_image = old_pixels_image + 1
   c) If (message bit = 0 and pixel_image mod 2 = 1) then: new_pixels_image = old_pixels_image - 1
   d) Save the new image as a stego-image.

Furthermore, the approach methods used for the message extraction process in the LSB method are as follows:

1. Get the message from the stego image in the following way:
   a) If the pixel value of the stego-image mod 2 = 0 then the message bit = 0.
   b) If the pixel value of the stego-image mod 2 = 1 then the message bit = 1.
2. Arrange the message bits starting from the MSB, so that an 8-bit binary number is formed.
3. Change the binary number to 8 bits.

2. Pixel Value Differencing

The PVD method works on a neighboring pair of pixels. The process of inserting messages is done by modifying the difference in pixel values. The range of gray values proposed by Wu and Tsai is (8 8 16 32 64 128) with the number of n bits (3 3 4 5 6 7) [14, 15]. The goal is to define the initial and final limits on neighboring pixel values. But in this study, a modification was made with a range of gray values (8 8 16 32 64 128) with the number of n bits (3 3 3 3 3 3). The message insertion process in the PVD method is as follows:

1. Convert the message to an 8-bit binary number.
2. Calculate the difference between the two neighboring pixels on the cover image
3. Specify the lower limit value and the number of bits n.
4. Take n bits of the message, then convert it to decimal (b)
5. Calculate the difference between the new pixel values.
6. Save the new image as a stego-image

The message extraction process in the PVD method is as follows:

1. Calculate the difference in neighboring pixel values in the stego-image
2. Specify the lower limit value and the number of bits n.
3. Calculate the decimal value (b)
4. Convert the value of b (decimal) to binary n bits
5. Fetch Message = bit n.

3. Modulus Function (MF)

MF method is the process of inserting messages by modifying the remainder value of neighboring pixels [16, 1]. In this study, how to insert a message using the MF method is as follows:

1. Convert the message to an 8-bit binary number.
2. Calculate the difference between the two neighboring pixels on the cover image.
3. Specify the lower limit value and the number of bits n.
4. Take n bits of the message, then convert it to decimal (b).
5. Calculate the remaining quotient value (remainder) using equation (1).

$$r = (g_i + g_{i+1}) mod\ 2^n \quad (1)$$

The value of r is the remainder or the remainder of the quotient while $g_i + g_{i+1}$ is two neighboring pixels on the cover image

6. Save the new image as a stego-image

The message extraction process in the MF method is as follows:

1. Calculate the difference between the two neighboring pixels in the stego-image
2. Determine the lower limit value and the number of bits n.
3. Calculate the remaining quotient value (remainder) using equation (1)
4. Retrieve Message = bit n.

3. Result and Discussion

The test was conducted to compare the methods discussed, namely Least Significant Bit, Pixel Value Differencing, and Modulus Function in inserting text messages into the cover image. In this research, the message to be inserted is stored in **.txt* format and the cover image used is Grayscale and RGB images with **.png* format.

To measure image quality and storage capacity in steganography, the test method used is fidelity by testing the comparison of the cover image and the stego-image to determine changes in image quality and stego-image size.[17] . Fidelity testing is done by calculating the MSE and PSNR values using equations (2) and (3)[18].

$$\mathrm{MSE}_{\mathrm{AVG}} = \frac{\mathrm{MSE_R}+\mathrm{MSE_G}+\mathrm{MSE_B}}{3} \quad (2)$$

$$\mathrm{PSNR} = 10_{\log 10}\left(\frac{255^2}{\mathrm{MSE}}\right) \quad (3)$$

3.1 LSB Method Fidelity Testing

The results of the fidelity test of the LSB method are presented in Table 1.

Table 1. LSB Test Results Based on Fidelity

Cover Image	Cover Dimensions	Message Size (byte)	Stego Image Size (byte)	MSE (db)	PSNR (db)
 Subulatgrey.png	512 x 512	22.820	126.673	0.347	52.341
 *Rosegrey.png*	512 x 512	22.820	98.054	0.354	52.191
 *Orchidgrey.png*	512 x 512	22.820	110.816	0.351	52.673
 *Tulip.png*	512 x 512	22.820	391.762	0.182	55.525

Cover Image	Cover Dimensions	Message Size (byte)	Stego Image Size (byte)	MSE (db)	PSNR (db)
 *Lily.png*	512 x 512	22.820	392.159	0.120	57.341
 *Dandelion.png*	512 x 512	22.820	234.874	0.119	57.380
 *Colors.png*	512 x 512	22.820	623.809	0.117	57.466

Table 1 shows the tests of cover images with the same dimensions and the same message. The message inserted is a file called message.txt with a size of 22.820 bytes, having dimensions of 512 x 512 pixels. From the results of the stego-image, it can be concluded that the size of the stego-image has increased to be bigger than the original or cover image. The increase in stego size is due to the insertion stage of the cover image with a 1-value bit inserted in the LSB of the image. So that the LSB which initially has a value of 0 becomes 1. Fidelity testing using the LSB method shows that the PSNR value between the cover image and the stego-image is very good. The average PSNR value is more than 52.0 dB and has already exceeded 40 dB. Meanwhile, the MSE value is between 0 and 1 dB. This shows that the quality of the cover image has not changed significantly.

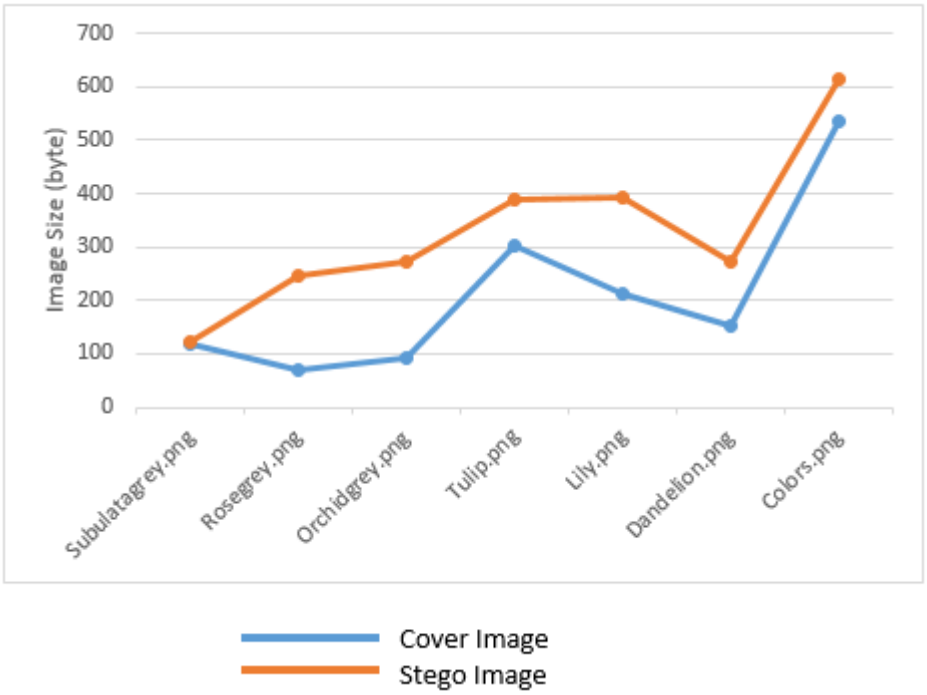


Figure 1. Graph of Fidelity Test Results on the LSB Method

Table 1 and the graph in Figure 1 show that the size of the stego image file increases compared to the size of the cover image or original image before the message is inserted.

3.2 PVD Method Fidelity Testing

The results of the fidelity test of the PVD method are presented in Table 2.

Table 2. PVD Test Results Based on Fidelity

Cover Image	Cover Dimensions	Message Size (byte)	Stego Image Size (byte)	MSE (db)	PSNR (db)
 Subulatgrey.png	512 x 512	22.820	133.852	9.523	37.960
 *Rosegrey.png*	512 x 512	22.820	109.744	6.976	39.240
 *Orchidgrey.png*	512 x 512	22.820	123.959	15.654	36.185
 *Tulip.png*	512 x 512	22.820	394.839	5.786	40.507
 *Lily.png*	512 x 512	22.820	401.361	1.119	47.644
 *Dandelion.png*	512 x 512	22.820	252.672	0.594	50. 391
 *Colors.png*	512 x 512	22.820	607.603	100.364	28.115

Table 2 shows the test results for the cover image with the same dimensions and the same message. The message inserted is a file called message.txt with a size of 22.820 byte, having dimensions of 512 x 512 pixels. Based on the results of the stego-image, it can be concluded that the size of the stego-image has increased to be bigger than the original or cover image. The increase in stego size is due to the insertion stage of the cover image in each pixel that can accommodate a minimum of 3 message bits and each bit is inserted in channels R, G, and B.

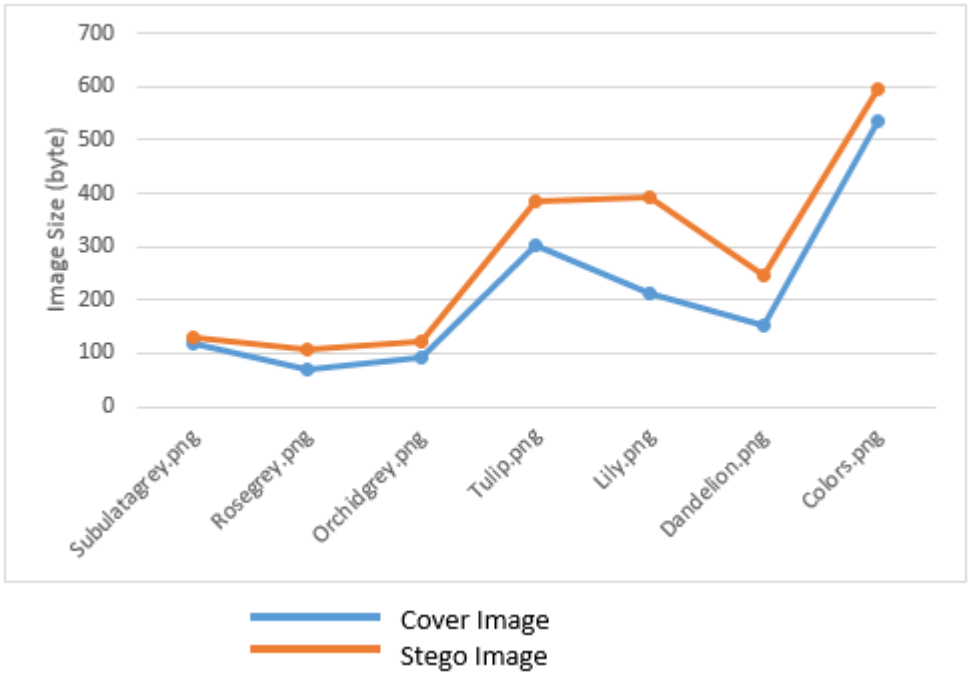


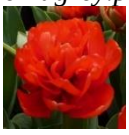
Figure 2. Graph of Fidelity Test Results on the PVD Method

Table 2 and the graph in Figure 2 show that the size of the stego-image file increases compared to the size of the cover image or original image before the message is inserted. The increase in stego size is because at the insertion stage n bits are carried out, while in each iteration it results in a significant change in pixel value.

3.3 MF Method Fidelity Testing

The results of the fidelity test of the MF method are presented in Table 3.

Table 3. MF Test Results Based on Fidelity

Cover Image	Cover Dimensions	Message Size (bytes)	Stego Image Size (bytes)	MSE (db)	PSNR (db)
 Subulatgrey.png	512 x 512	22.820	126.335	0.694	49.335
 *Rosegrey.png*	512 x 512	22.820	97.000	21.848	34.282
 *Orchidgrey.png*	512 x 512	22.820	112.951	6.373	40.088
	512 x 512	22.820	391.185	6.381	40.082

Cover Image	Cover Dimensions	Message Size (bytes)	Stego Image Size (bytes)	MSE (db)	PSNR (db)
Tulip.png 	512 x 512	22.820	391.208	7.204	39.555
Lily.png 	512 x 512	22.820	232.354	0.232	54.482
Dandelion.png 	512 x 512	22.820	623.279	10.068	38.101
Colors.png					

Table 3 shows the test results for the cover image with the same dimensions and the same message. The message inserted is a file called message.txt with a size of 22.820 bytes, having dimensions of 512 x 512 pixels. From the results of the stego image, it can be concluded that the size of the stego image has increased to be bigger than the original or cover image. The increase in stego size is due to the insertion stage of the cover image in each pixel can accommodate a minimum of 3 message bits and each bit is inserted in channels R, G, and B.

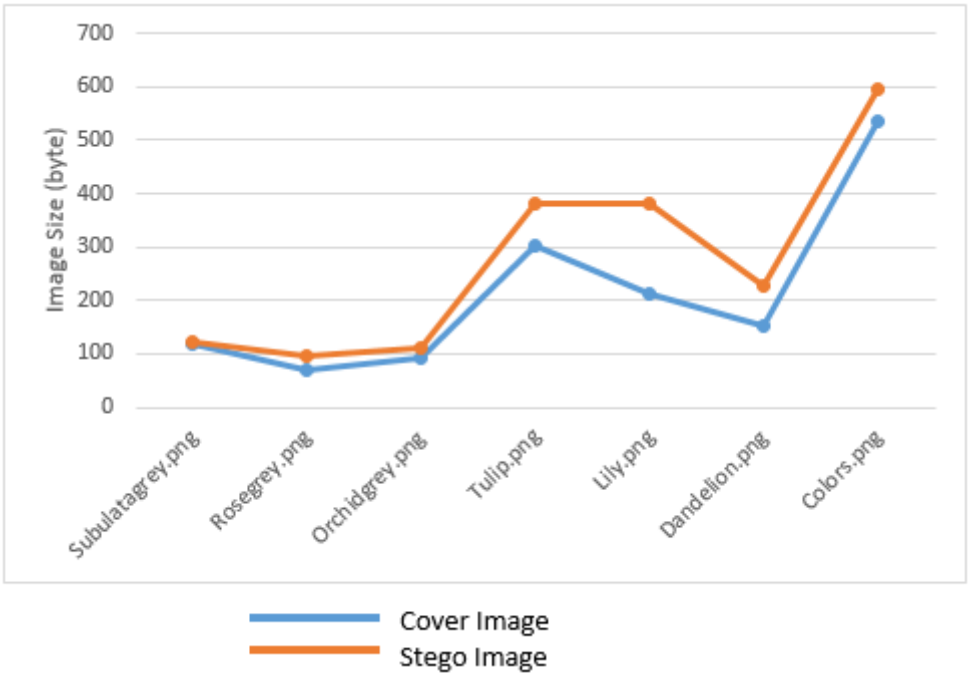


Figure 3. Graph of Fidelity Test Results on the MF Method

The graphic in Figure 3 shows a change in the size of the stego-image, but the change in the Subulatagrey.png stego-image does not change too much. But when compared in terms of quality, the

quality of Dandelion.png stego image is much better with the comparison of the MSE value for Lily.png stego image of 0.623db and Dandelion.png of 0.232 db.

3.4 Robustness Testing using Cropping

Good steganography should be resistant to attacks in the form of steganalysis or image manipulation [19]. Robustness testing will be done by attacking the stego-image with image processing attacks such as cropping. Then the data will be tried to be extracted whether the extracted data remains intact or damaged. In this study, testing was carried out by cutting the stego-image with a cutting percentage of 10% from various directions. The results of robustness testing using cropping with the LSB, PVD, and MF methods are presented in Table 4.

Table 4. Robustness Testing using Cropping

Stego image (Subulatgrey.png)	Crop Position	% Crop	Extraction
	Right	10%	Failed
	Top	10%	Failed
	Bottom	10%	Success
	All Position	10%	Failed

In the tests presented in Table 4, the results of cropping testing using the LSB, PVD, and MF methods on the stego-image with a cropping percentage of 10%. Stego-image cuts from the left, right, up and down, and all directions. Messages that can be extracted are only in the cut position at the bottom of the stego-image, while others have failed due to the messages are partially missing, truncated, or damaged. The intact message is caused by cutting in several parts causing some message bits to be lost due to being cut.

3.5 Robustness Testing Using Image Resize

This test is done by attacking the stego-image with the Resize image. Then the message will be tried to be extracted whether the extracted data remains intact or corrupted. If the extracted data remains intact, the level of resistance to image resizing is good. The results of robustness testing using image resize with the LSB, PVD, and MF methods are presented in Table 5.

Tabel 5. Robustness Testing using Image Resize

Stego image (Subulatgrey.png)	% Resize	Extraction
	10 %	Failed
	20 %	Failed
	30 %	Failed

In Table 5 shows the results of robustness testing on the LSB, PVD, and MF methods with image resizing attacks, the percentage of 10% to 30% of the inserted message can still be extracted again but the message cannot be read because the resizing operation is performed to reduce the pixel size of the stego-image.

4. Conclusion

The LSB method has the best image quality between the PVD and MF methods because it produces a stego-image change that is almost the same as the cover image or the resulting change is insignificant. This is evidenced by the average MSE value generated from the LSB method which is close to 0, which means that the pixel values in the cover image and stego-image do not change much. The test results for the storage capacity of the PVD method have a better capacity than the LSB and MF methods because the PVD method has a relatively smaller stego-image size. Meanwhile, for testing image resilience, the LSB, PVD, and MF methods can extract the message complete with a 10% cropping percentage at the bottom of the stego-image.

References

[1] P. W. Adi, F. Z. Rahmanti and N. A. Abu, "High Quality Image Steganography on Integer Haar Wavelet Transform using Modulus Function.," in *International Conference on Science in Information Technology (ICSITech)*, Yogyakarta, 2015.

[2] B. Bhatu and H. y. Shah, "Customized Approach to Increase Capacity and Robustness in Image Steganography," Coimbatore, 2016.

[3] G. Swain and S. K. Lenka, "A novel steganography technique by mapping words with LSB array Gandharba Swain," *International Journal Signal and Imaging Systems Engineering,* vol. 8, pp. 115-121, 2015.

[4] M. Tang, J. Hu, M. Fan and W. Song, "A steganalysis by adjacency pixel bits structure," *Comput Electr Eng,* pp. 488-496, 2013.

[5] J. Tao, S. Li, X. Zhang and Z. Wang, "Towards Robust Image Steganography," *IEEE Transactions on Circuits and Systems for Video Technology,* vol. 29, no. 2, pp. 594 - 600, 2019.

[6] D. Darwis, A. Junaidi and W. Wamiliana, "A New Approach of Steganography Using Center Sequential Technique," *Journal of Physics: Conference Series,* vol. 1338, 2019.

[7] R. Rejani, D. Murugan and V. Krishnan, "Pixel Pattern Based Steganography on Images," *ICT ACT Journal on Image and Video Processing,* vol. 5, no. 3, pp. 991-997, 2015.

[8] O. J. Sandoval, M. C. Hernandez and G. S. Perez, "Compact Image Steganalysis for LSB-Matching Steganography," in *International Workshop on Biometrics and Forensics (IWBF)*, 2017.

[9] G. Swain, "Digital Image Steganography using Nine-Pixel Differencing and Modified LSB

Substitution," *Indian Journal of Science and Technology,* vol. 7, no. 9, p. 1444–1450 , 2014.

[10] A. S. Vignesh and J. Mukherjee, "Secure Steganography Using Randomized Cropping," in *Springer-Verlag Berlin Heidelberg*, 2015.

[11] W. Wamiliana, M. Mustofa, W. Warsito and R. Setiawan, "The Hybrid Method Of Column Transposition With Adaptive Minimum Error Least Significant Bit Replacement (AMELSBR) using file jpg/jpeg and png," *International Journal of Computer Science and Network Security,* vol. 17, no. 7, pp. 174-179, 2017.

[12] Awate and M. M. Patil, "Modulus Function and Pixel Value Differencing Coupled with Modified Pixel Indicator Based Secret Data Hidding Method," *International Journal of Advances in Science Engineering and Technology*, vol. 4, no. 2, pp. 26-29, 2016.

[13] Z. Zhu, T. Zhang and B. Wan, "'A Special Detector for the Edge Adaptive Image Steganography based on LSB Matching Revisited," in *IEEE International Conference on Control and Automation*, Hangzhou, China, 2013.

[14] J. X. Q. Zhao, "Data Embendding Based on Pixel Value Differencing and Modulus Function using Indeterminate Equation" *The Journal of China Universitas of Posts and Telecommunications,* vol. 22, no. 1, pp. 95-100, 2015.

[15] R. C. Tyagi, "High Capacity Image Steganography Based on Pixel Value Differencing and Pixel Value Sum," in *Second International Conference on Advances in Computing and Communication Engineering*, Dehradun, India, 2015.

[16] H. Li, "Steganography With Pixel Value Differencing and Modulus Function Based on PSO," *Journal of Information Security and Applications,* no. 43, pp. 47-52, 2018.

[17] S. Singh and T. J. Siddiqui, "Robust Image Steganography Using Complex Wavelet Transform," *Impact,* p. 56–60, 2013.

[18] D. A. Silverstein and J. E. Farrell, "The relationship between image fidelity and image quality," *IEEE*, no. 1, p. 881–884, 1996.

[19] M. Mishra and P. Mishra, "Digital image data hiding techniques," *ANSVESA,* vol. 7, no. 2, pp. 105-115, 2012.