TEXT IN IMAGE STEGANOGRAPHY BASED ON A DYNAMIC NON-SEQUENTIAL LEAST SIGNIFICANT BIT TECHNIQUE IN GRAYSCALE AND RGB IMAGES

[1]HAYFAA ABDULZAHRA ATEE, [2]ABIDULKARIM K.I.YASARI, [3]ROBIAH AHMAD, [4]NORLIZA MOHD NOOR

[1]Institute of Administration/ Al-Rusaffa, Middle Technical University, Baghdad, Iraq
[2]College of Engineering, Al-Muthanna University, Al-Muthanna, Iraq
[3,4]Department of Engineering, UTM Razak Faculty of Technology and Informatics, Kuala Lumpur, Malaysia

E-mail: [1]hayfaa_Atee@ioar.org, [2]abidulkarim@mu.edu.iq, robiah@ic.utm.my, norliza@ic.utm.my

ABSTRACT

Information hiding is one of the considerable objects in secret communication. Steganography is a vital research area in recent years relating several applications. Image steganography is the mode of embedding information (e.g. text) in an image, such an impossible to be seen by human eyes or so-called visual system (HVS). This study presents a steganography scheme based on a dynamic non-sequential Least Significant Bit (LSB) procedure for concealing text information into two kinds of images; include RGB images and Grayscale images, where the efficiency of using each of these kinds is studied. the spatial domain is used to perform the LSB procedure, where the bits of the secret message are inserted into the host or cover image using LSB process to outcome a stego-image. The results show that the secret message can be hidden securely and undetectable against HVS, and using RGB image shows better performance. Comparing with some other methods, the proposed scheme is superior in terms of MSE and PSNR.

Keywords: *LSB, Image steganography, PSNR, MSE, HVS.*

1. INTRODUCTION

Due to the increase of the World Wide Web, digital media, and data transformation applications, information security becomes a primary key of information and communication technology. The information hiding is an old idea; appeared early in olden Greece, there were numerous efforts to cover the messages with different means. relies on delivered through enemy territory. Recently, due to the global of virtual and digital communication, numerous techniques are utilized for embedding information in a medium such as steganography [1][2][3]. In this mechanism, virtual media, particularly digital images, are utilized as a wherewithal for concealing data in the textual content form, images, videos, and even the audio record may be used as an invisible message. In other word, steganography is the procedure of hiding a confidential message in a type of media in order to protect from the third party. Such in facts the hiding systems take benefit of human perceptual weaknesses [1][4][3]. Consequently, steganography systems are widely used as a satisfactory solution to protect the presence of messages. While, if the existence of hidden data is doubtful or discovered, the reason for the concealment of information has been partially defeated [2][3][4][5]. Wherein, it tries to prohibit the third party from suspecting that the data is there [3][6][7].

Image steganography could be defined as the term of covering a message in an image. Inserting the secret message into the cover image in the image steganography technique, performs either by special domain or transform (frequency) domain. The LSB is the most famous scheme belongs to the spatial domain, in which the text embeds directly in the last right bit (8th) of the pixel. Conversely, in the transform domain, the text conceals by changes the frequency coefficients of the host image. In standard LSB technique, only the last bit of the selected pixel has to be changed. Consequently, there are little changes in the host image and additional information could be concealed in the image.

On another side, several steganographic methods had been offered, the simple and widely known method is the LSB-based method, which hiding the confidential data in the LSB of each pixel in the host image (i.e. Grayscale image). Based on LSB scheme, the process concealing the secret data in RGB image (i.e. true color image) is progressed with enhanced stego-image quality [2][3][8].

In the traditional LSB scheme, a secret message is concealing sequentially in a host image. Hence, the attacker can easily extract the hidden text. In order to overcome the weaknesses in traditional LSB technique, the study presents a steganography scheme based on LSB technique in which the confidential text is concealed into the cover image in a dynamic non-sequential arrangement to decrease the image corruption and raise the level of security. Because the block size is not fixed, it varies from a secret message to another; it mainly depends on the length of the message. Hence, this method is dynamic and renewable from a message to another. Consequently, any attack for obtaining the secret message or the concealment algorithm is very difficult. The proposed study provides an efficient concealment scheme, especially for short messages.

In this study, a dynamic non-sequential LSB based spatial domain area utilized in picture steganography, where less significant parts of the image pixels are chosen to be substituted for hiding a confidential message. The proposed scheme including two main processes; embedding process and extraction process. The proposed method has been performed in both image types, 8-bits image (i.e. Grayscale) and 24-bits image (RGB image). Consequently, this study has discussed the efficiency of using these two types as a host image.

2. LITERATURE REVIEW

Steganography, which means "Covered Writing" has been taken from Greek language and used fundamentally in numerous forms for centuries [2][3][9]. To cover the secret message, Histaiacus shaved the head of a messenger, then writing the mysterious message on the scalp of the messenger, therefore, they wait for the hair to be grown again. Hereby, a messenger travels and arrived his destination freely, then his head is shaved to get the secret message by the receiver [10] [11] [12]. On another side, the Germans build up a steganographic technique named as microdot. A microdot is content or a picture significantly lessened in size onto a little plate to prevent and counteract detection by unintended beneficiaries. On a very basic level, it is a steganographic way to deal with message protection. Microdots are typically circular and around one millimeter in breadth, however, can be made into various shapes and sizes and produced using different materials, for example, polyester or metal. Therefore, the microdots are so small, it could be printed on envelope or a letter and sent unnoticeable [3] [13].

Steganography is categorized into two types; the first one is the fragile steganography and the other one is the robust steganography. In the fragile steganography, the data is embedded into a file that is damaged in case if any wrong modification on the file. Meanwhile, in the robust steganography, the data is embedded into a file (i.e. image) in a way that it cannot be easily detected and destroyed [13] [14]. Many studies in steganography to hiding data image have been done in literature, where a different number of steganography techniques have been offered in different studies [15] [16] [17] [18] [19] [20] [21] [22] [23]. Among the steganographic techniques, the best well known and most straightforward technique is the LSB. LSB technique has been detailed in several studies like in [24] [25] [26] [27] [28] [29].

The study aims to protect confidential data that transform via Internet using image steganography based on a dynamic non-sequential LSB technique, which is the best inexpensive ways.

3. LEAST SIGNIFICANT BIT (LSB)

The simplest and straightforward process for hiding data in a media's digital is LSB. LSB data hiding mechanism does not impact the image's visual characteristic. Only the LSB's of the host media's digital pixels are used for hiding the confidential message [1] [25A straightforward, a data's bits such as a message or a text file are embedding in LSB's of a cover image, whereas the yield image from this process called stego-image, as described in the following formula [3] [25] [28].

Host image + hidden information = stego-image (1)

The image can be Grayscale or colour image. In Grayscale image, 8-bit are represented for each pixel, while in a standard colour image 24-bit are represented for each pixel [1][2][3] [28]. For example, suppose that it is needed to hide 8 bits of a message (i.e. 8-bit) in a host image, and suppose an 8-pixel in the Top-Left of this host image (i.e. 8-bytes), as in the following encoding:

An 9-bits of a secret message = 110010010, is supposed to be covered in:

An 9-pixel of a host image:

00101101	00011101	11001100
10100110	11000100	01001101
10010000	10101000	01100011

Based on LSB method, each bit of the message is hided in 1-byte of the host image, resulting as follows:

00101101	00011101	11001100
10100110	1100010**1**	0100110**0**
10010000	1010100**1**	0110001**0**

Where the bits in colored bold indicates to the changed bits in the host image. It's observed that the number of changed bits is 4, which about half numbers of LSB in the selected pixels.

On another side, the steganography performance is different from one to another. Image quality is the vital pointer for the performance of the image steganography technique PSNR and MSE are the superlative matrices for evaluating the image's quality. Thus, the Image goodness performance can be determined primarily by calculating PSNR and MSE metrics for stego-image evaluation.

PSNR metric is applied as a statistical instrument for assessing a video quality or a digital quality [1][2][3] [30] [31]. PSNR, simply defined by MSE of y*z grayscale images A and B, in which one of the used images is a noisy approximation of the second image [28] [31].

The MSE is an error metric of the image quality, represents the squared error between A and B images. It is a permanently positive number; the better results are approximate to zero. MSE can be performed by matching the original image (host-image) and the stago-image byte by byte. The MSE is defined as [32][33] :

$$MSE = \frac{1}{y*z} \sum_{m=0}^{x-1} \sum_{n=0}^{y-1} [A(m,n) - B(m,n)]^2$$
(1)

where:

y: denotes the row's number of the host image

z: denotes the row's number of the host image

A(m,n): denotes the pixel's value of the (A) host image

B(m,n): denotes the pixel's value of the (B) stego-image

PSNR is the measurement metric of the peak signal-to-noise ratio between two images, which are the original image (host-image) and the noisy image (stego-image). The higher PSNR is indicating to high quality image. The PSNR metric is described as below [34] [35]:

$$PSNR = 10.log_{10}\left(\frac{MAX_A^2}{MSE}\right) = 20.log_{10}\left(\frac{MAX_A}{\sqrt{MSE}}\right) \quad (2)$$

Where:

MAX_A: represents the maximum probable image's pixel value that is 255, when the pixels denoted by 8 bits.

The higher PSNR demonstrates getting better goodness of the stego-image or in other words lesser deformation. Moreover, it demonstrates the least chance of visual human eye to reveal [30][31][36].

Spatial domain based on a dynamic non-sequential LSB hiding technique is utilized in this work.

4. METHODOLOGY

Figure 1 illustrates a general glance of the steganography scheme used in this study. To hide the text information, the LSB-based embedding is used. The two main processes in this method are; first is the LSB-embedding process, which is non-sequential bits of the confidential message concealed in the host image in order to produce the stego-image. On the other side, the second process is extraction of the hidden text from the stego-image to get the concealed message. The two processes are performed as in the following steps.

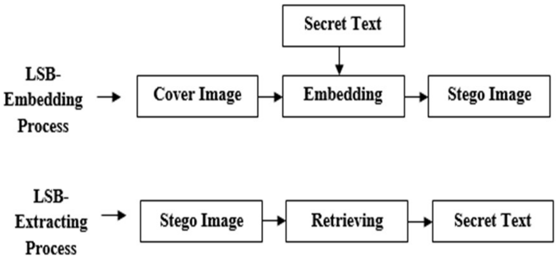


Figure 1: Text-Hiding Steganography Scheme.

4.1 LSB Embedding Process

The LSB embedding technique is performed as the following:

Step1: Read the host or cover image.

Step2: Read the confidential message.

Step3: Change each confidential message's character into ASCII code (Decimal number).

Step4: Determine the length of the message and change each ASCII code to its 7-bits binary equivalent.

Step5: Depending on the number of bits of the confidential message, the host image is separated into blocks. After that, each block is divided into sub-blocks of 6 Bytes in order to conceal the message bits.

Block size = Host image size (pixels)/secret message length (bits)

Step6: Separate the host image into RGB plane (in case of RGB color image) and insert the 1st bit of the secret message into the last bit of 1st pixel of the first sub-block, then insert the 2nd bit of the secret message into the last bit of the first pixel of the 2nd sub-block, and so on, until the whole message is embedded within the host image.

Step7: Output a stego-image containing the secret message.

Figure 2 illustrates the pictorial embedding procedure of the proposed scheme.

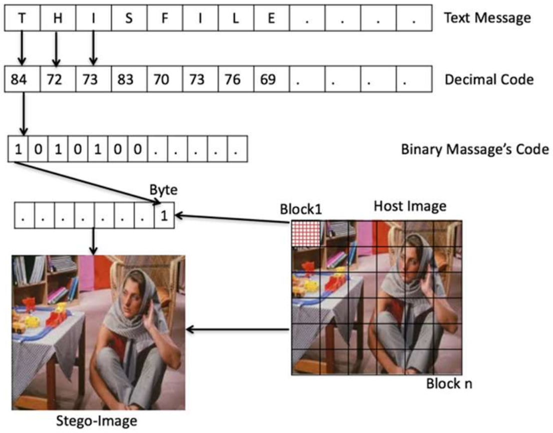


Figure 2: The embedding process.

4.2 LSB Extracting Process

The steps for extracting secret message are described as follows:

Step1: Read the stego-image.

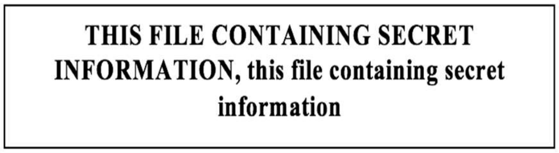
Step2: Separate (divide) the host image into RGB plane (in case of RGB image) and divide the image size over the message's bit length to get the block size. Then separate each block into sub-blocks of 64 bytes (8*8). After that, extract the last bit of the 1st pixel in the 1st sub-block to obtain the first bit of the hidden secret message, and then extract the last bit of the 1st pixel of the 2nd sub-block to obtain the second bit of the hidden secret message, and so on, until the whole message is retrieved from the stego-image.
Step3: Convert binary code of the derived secret message into its decimal-ASCII value.

Step4: Convert each decimal ASCII code to its represented character.

Step5: Output the covert message.

The input host images can be a Grayscale image (8-bits image per pixel) or RGB color image (24-bits image per pixel). LSB is performed on six test images, a three are RGB (i.e. true colour image) and the other three images are Grayscale images, which are related to Lena, Peppers, and Baboon images. Each one of the test images has a size 512×512 and PNG image type. On another side, the following textbox contains the secret message that taken to be hidden as secret message in a host image.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195



THIS FILE CONTAINING SECRET INFORMATION, this file containing secret information

The MSE and PSNR metrics are utilized for calculating the performance of the used mechanism and the quality of the stego-images using equation (2) and (3) respectively. Whereby, the lower MSE value indicates better performance, while the greater value of PSNR denotes a superior quality of the stego-image.

5. EXPERIMENTAL RESULTS

The experimental results demonstrate the achievements of the LSB-based steganography process in two different map images (i.e. Grayscale and RGB images). Three images namely Baboon, Lena, and Peppers are used as host images. The secret message which is adapted to be concealed is covered into the host image using the LSB technique. Then, stego-image is produced. The host images along with corresponding stego-images are illustrated in Figure 3, Figure 4, and Figure 5 for both RGB and Grayscale images, for Lena, Peppers, and Baboon images respectively. Meanwhile, Figure 6, Figure 7, and Figure 8 respectively are illustrated their histogram results.

The secret message is covered within the top-left side of the host image. It can be noticed that the deformation occurs in the stego-images due to hiding the secret message are unrevealed to the human eye.

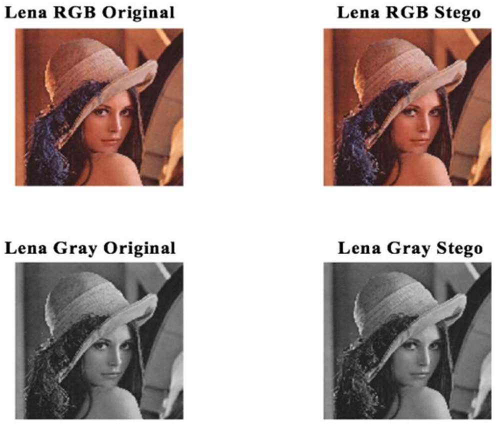


Figure 3: Steganography results for Lena images.

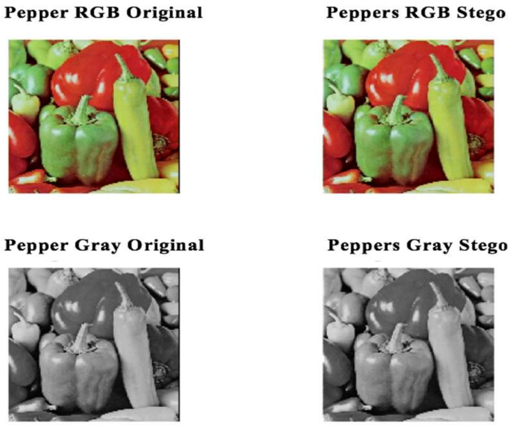


Figure 4: Steganography results for Pepper images.

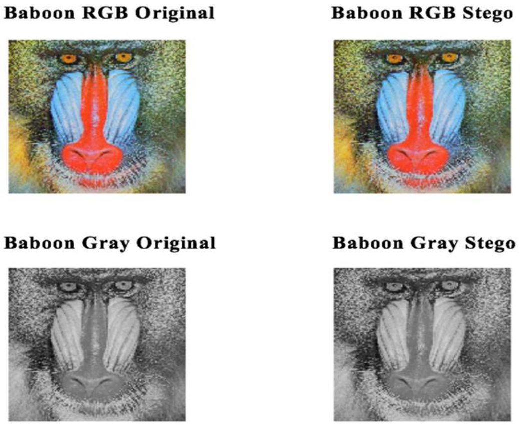


Figure 5: Steganography results for Baboon images.

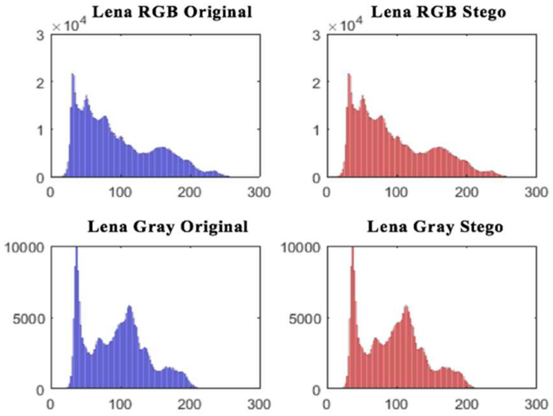


Figure 6: Histogram results for Lena images.

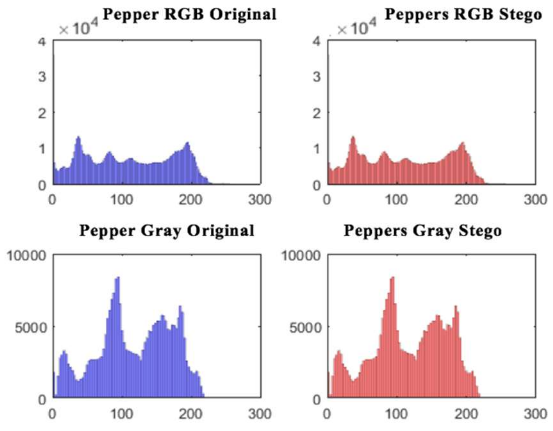


Figure 7: Histogram results for Pepper images

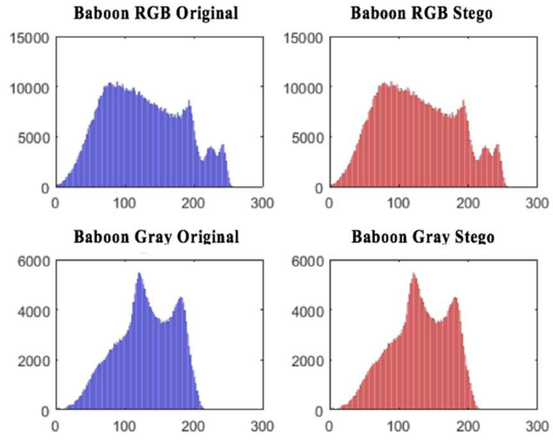


Figure 8: Histogram results for Pepper images

On another side, Table 1 illustrates the steganography performance results based on MSE and PSNR measurements. Generally, it can be noticed that using RGB color image as a host image for concealing the secret message provide better performance compared to that when using Grayscale image as a host image. For example, Lena_RGB host gets MSE value at 4.3360e-04, and PSNR value at 81.7598. Meanwhile, Lena Grayscale host gets MSE value at 0.0013, and PSNR value at 77.1442. In Pepper_RGB host gets MSE value at 3.5858e-04, and PSNR value at 82.5849. Meanwhile, Pepper Grayscale host gets MSE value at 0.0011, and PSNR value at 77.7223. Moreover, it is the same superior is obtained in the Baboon image.

Table 1: Steganography Performance Based on MSE and PSNR Values.

Image	MSE	PSNR
Lena_RGB	0.00043360	81.7598
Lena_Grayscale	0.00130000	77.1442
Pepper_RGB	0.00035858	82.5849
Pepper_Grayscale	0.00110000	77.7223
Baboon_RGB	0.00043106	81.7854
Baboon Grayscale	0.00140000	76.8262

The PSNR and MSE are utilized for evaluating and comparing the security achievement of this study with the method presented in [28]. The Lena_RGB image is used for conducting the tests. Despite the length of the tested message in [28] is shorter than the text message tested in this study, the proposed scheme is achieved better results as shown in Table2.

Table 2: Steganography Performance Based on MSE and PSNR Values for the Proposed Scheme and [28] method.

Image	Kamdar *et al.* [28]		Proposed scheme	
	MSE	PSNR	MSE	PSNR
Lena_RGB	0.012	77.45	0.00043360	81.7598

Moreover, the performance of this study is compared with [29] in terms of PSNR and MSE metrics for Lena_RGB, Lena_Grayscale, Baboon_RGB, and Baboon_Grayscale images. The obtained results are presented in Table 3.

Table 3: Steganography Performance Based on MSE and PSNR Values for the Proposed Scheme and [29] method.

Image	Khan et al. [29]		Proposed scheme	
	MSE	PSNR	MSE	PSNR
Lena RGB	3.20	43.11	0.00043360	81.7598

Lena Grayscale	1.09	43.71	0.00130000	77.1442
Baboon RGB	1.27	47.10	0.00043106	81.7854
Baboon Grayscale	2.40	44.37	0.00140000	76.8262

The higher PSNR and lower MSE in Table 2 and 3 indicate the best quality and less distortion in the resulted image, which leads to less chance to reveal by HVS.

6. DISCUSSION

Based on the results presented in the experimental part, the secret information could be covered securely in images, and it seems to be impossible to be recognized by the visual system of human eyes. On another side, the results show that using RGB host image is better than using Grayscale image; the reason behind this is only because the RGB image is represented by 24-bit per pixel while the Grayscale image is represented by the 8-bit per pixel. Consequently, when using the RGB photo as a host image, the rate of alternative changes would be more indistinguishable to the human eye compared with the Grayscale image.

7. CONCLUSION

This study provides a steganography scheme using non-sequential LSB mechanism for covering text message in an image by two main processes; include embedding and extraction process. This embedding is applied in two kinds of images (i.e. RGB and Grayscale images). It is concluded that using the RGB photo as a host image seems to be more secure and with better imperceptibility. On another side, using RGB image provides a higher capacity in accommodating information; three times more than the Grayscale image. The proposed scheme overpowers other methods presented by other studies in terms of security performance. Though the proposed technique provides properly confidentiality, it has some cons, which represented in lost the covered data when exposed to image manipulation.

REFERENCES:

[1] Bawaneh, M. J., & Obeidat, A. A. (2016). A secure robust gray scale image Steganography using image segmentation. Journal of Information Security, 7(03), 152.

[2] Prasad, S., & Pal, A. K. (2017). An RGB colour image Steganography scheme using overlapping block-based pixel-value differencing. Royal Society open science, 4(4), 161066.

[3] Jassim, F. A. (2013). A novel Steganography algorithm for hiding text in image using five modulus method. arXiv preprint arXiv:1307.0642.

[4] Amin, M. M., Salleh, M., Ibrahim, S., Katmin, M. R., & Shamsuddin, M. Z. I. (2003, January). Information hiding using steganography. In Telecommunication Technology, 2003. NCTT 2003 Proceedings. 4th National Conference on (pp. 21-25). IEEE.

[5] Wang, H., & Wang, S. (2004). Cyber warfare: steganography vs. steganalysis. Communications of the ACM, 47(10), 76-82.

[6] Rawat, D., & Bhandari, V. (2013a). A steganography technique for hiding image in an image using lsb method for 24 bit color image. International Journal of Computer Applications, 64(20).

[7] Westfeld, A., & Wolf, G. (1998, April). Steganography in a video conferencing system. In International Workshop on Information Hiding (pp. 32-47). Springer, Berlin, Heidelberg.

[8] Rawat, D., & Bhandari, V. (2013b). Steganography technique for hiding text information in color image using improved LSB method. International Journal of Computer Applications, 67(1).

[9] Muhammad, K., Ahmad, J., Farman, H., & Zubair, M. (2015). A novel image steganographic approach for hiding text in color images using HSI color model. arXiv preprint arXiv:1503.00388.

[10] Johnson, N. F., & Jajodia, S. (1998). Exploring Steganography: Seeing the unseen. Computer, 31(2).

[11] Moulin, P., & Koetter, R. (2005). Data-hiding codes. Proceedings of the IEEE, 93(12), 2083-2126.

[12] Swain, G., & Lanka, S. K. (2012). A quick review of network security and Steganography. International Journal of Electronics and Computer Science Engineering, 1(2), 426-435.

[13] Dhanarasi, G. O. W. T. H. A. M., & Prasad, A. M. (2012). Image Steganography using block complexity analysis. International Journal of engineering science and technology, 4(7).

[14] Channalli, S., & Jadhav, A. (2009). Steganography an art of hiding data. arXiv preprint arXiv:0912.2319.

[15] Al-Shatnawi, A. M. (2012). A new method in image Steganography with improved image

quality. Applied Mathematical Sciences, 6(79), 3907-3915.

[16] Chan, C. K., & Cheng, L. M. (2004). Hiding data in images by simple LSB substitution. Pattern recognition, 37(3), 469-474.

[17] Chang, C. C., Hsiao, J. Y., & Chan, C. S. (2003). Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy. Pattern Recognition, 36(7), 1583-1595.

[18] Yang, C. H., & Wang, S. J. (2010). Transforming LSB substitution for image-based Steganography in matching algorithms. Journal of information science and engineering, 26(4), 1199-1212.

[19] Chen, P. Y., & Wu, W. E. (2009). A modified side match scheme for image Steganography. International Journal of Applied Science and Engineering, 7(1), 53-60.

[20] Chang, C. C., & Tseng, H. W. (2004). A steganographic method for digital images using side match. Pattern Recognition Letters, 25(12), 1431-1437.

[21] Atee, H. A. (2018). In Improved Chaotic Radial Basis Resonance Theoritic Neural Network Integrated with Genetic Algorithmfor Enhancing Security In Image Transmission.ARPN Journal of Engineering and Applied Sciences, 13(9).

[22] Atee, H. A., Ahmad, R., Noor, N. M, Ilijan, A. (2017). Advanced Encryption Standard Algorithm Versus Extreme Learning Machine Based Weight: a Comparative Study. ARPN Journal of Engineering and Applied Sciences, 12(3).

[23] Atee, H. A., Ahmad, R., Noor, N. M, Ilijan, A. Rahma, A., S., and Aljeroudi, Y. (2017). Extreme Learning Machine Based Optimal Embedding Location Finder for Image Steganography. Plose One.

[24] Rifa, H., Rifa, J., & Ronquillo, L. (2010, February). Perfect Z2Z4-linear codes in Steganography. International Symposium on Information Theory and Its Applications (ISITA).

[25] Wu, D. C., & Tsai, W. H. (2003). A steganographic method for images by pixel-value differencing. Pattern Recognition Letters, 24(9-10), 1613-1626.

[26] Steganalysis, H. C. D. B., & Westfeld, A. (2001, November). F5—A Steganographic Algorithm. In Information Hiding: 4th International Workshop, IH 2001, Pittsburgh, PA, USA, April 25-27, 2001. Proceedings (Vol. 2137, p. 289). Springer Science & Business Media.

[27] Cachin, C. (1998, April). An information-theoretic model for Steganography. In International Workshop on Information Hiding (pp. 306-318). Springer, Berlin, Heidelberg.

[28] Kamdar, N. P., Kamdar, D. G., Khandhar. D. N. (2013). Performance Evaluation of LSB based Steganography for Optimization of PSNR and MSE. Journal of Information, Knowledge and Research in Electronics and Communications Engineering, 2(2), 505-509.

[29] Khan, Z., Shah, M., Naeem, M. et al,. (July 2016). Threshold-based Steganography: A Novel Technique for Improved Payload and SNR. The International Arab Journal of Information Technology, 13(4), 380-386.

[30] Karim, S. M., Rahman, M. S., & Hossain, M. I. (2011, December). A new approach for LSB based image Steganography using secret key. 14th International Conference on Computer and Information Technology (ICCIT). 286-291. IEEE.

[31] Hossain, M., Al Haque, S., & Sharmin, F. (2009, December). Variable rate Steganography in grayscale digital images using neighbourhood pixel information. 12th International Conference on In Computers and Information Technology, 2009. ICCIT'09. 267-272. IEEE.

[32] Modi, A., and Bansal, M. (2015). International Journal of Advanced Research in Computer Science and Software Engineering. International Journal of Advanced Research in Computer Science and Software Engineering. 5(5), 224-229.

[33] Kasapbas, M. C.¸ and Elmasry, W. New LSB-based colour image steganography method to enhance the efficiency in payload capacity, security and integrity check. Sådhanå (2018). Indian Academy of Sciences, (pp 1-14). https://doi.org/10.1007/s12046-018-0848-4.

[34] Almohammad, A., and Ghinea, G. (2010). Stego image quality and the reliability of PSNR. International Conference on Image Processing Theory, Tools and Applications. IEEE.

[35] Majeed, M. A., and Sulaman R. A. (2015). An Improved LSB Image Steganography Technique Using Bit-Inverse In 24 Bit Colour Image. Journal of Theoretical and Applied Information Technology. 80(2). 342-348.

[36] Atee, H. A., Ahmad, R., Noor, N. M, and Ilijan, A. K. (2016). A Combined Crypto-Stego System Using Dynamic Encryption Assisted Intensity Color Steganography. International Journal of Control Theory and Applications, 9(30), 175-184.