International Journal of Engineering Technology Research & Management

Published By:

https://www.ijetrm.com/

DCI NORMALIZATION TO INCREASE THE HIDING CAPACITY

Prof. Ziad AlQadi¹ Prof. Yousif Eltous² ^{1, 2} Professors, Albalqa Applied University,

ABSTRACT

An efficient method of message steganography will be introduced, the method will use 16_bits binary presentation to represent the covering-stego data item, the digital color image will be normalized to use fractional decimals values for data hiding; this will increase the capacity hiding to reach the covering image size. Various LSB bits order and various in length sets of LSBs will be examined to show the effect of using each of them on the quality of the stego image, and it will be shown that using 8 bits of the covering data items will always produce a stego image with high quality. The proposed method will give the user the ability to select the used LSB or the used set of LSBs. The proposed method will use a simple presentation to represent the secret message and the covering-stego image, and the hiding-extracting process will be implemented by using a simple assignment operation. The proposed method will be tested and implemented using various messages and various sets of LSBs, the obtained results will be used to prove the efficiency improvements provided by the proposed method, the proposed method will always provide a stego image steganography comparing with other existing methods of data steganography.

Keywords:

Steganography, DCI, normalized DCI, LSB, set of LSBs, quality, speed up.

INTRODUCTION

Secret message steganography [1-10] is one of the easiest methods to protect the message, and it can be applied by hiding a message in a covering image to produce a stego image, this process as shown in figure 1 will be implemented using hiding function. After receiving the stego image the data receiver executes the extracting function to process the stego image to produce the extracted secret message [11-16].

The quality of the stego image must be high and it must be closed to the covering image, while the extracted message must be the same a source hidden message, the stego method must satisfy the quality requirements listed in table 1. The speed of data hiding and data extracting must be high, this can be reached by decreasing both the hiding and extracting times [16-22].

Table 1: Stego method quality requirements [23-30]				
Quality parameter	Calculated between the covering	Calculated between the source and		
	and the stego images	the extracted messages		
Mean square error (MSE)	Low	Zero		
Peak signal to noise ratio (PSNR)	High	Infinite		

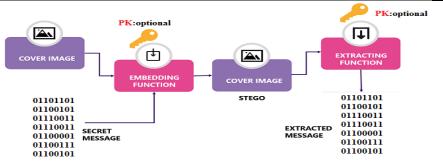


Figure 1: Stego method diagram

International Journal of Engineering Technology Research & Management

Published By:

https://www.ijetrm.com/

1.1 Data sets preparation

Secret message (SM) is a set of characters arranged in one row matrix, these characters can be easily converted to decimal (ASCII values) [31-36], the decimal values can be easily converted to binary using 8_bits binary presentation to form the message binary matrix (MBM), this matrix as shown in figure 2 reshaped to one column matrix, or two columns matrix, or 4 columns matrix or 8 columns binary matrix depending on the number of bits to be used for data hiding-extracting [37-42].

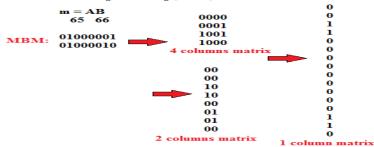


Figure 2: SM preparation

RGB digital color image (DCI) [43-50] is a set of colors values arranged in 3D matrix (2D matrix for the red color, 2D matrix for the green color and 2D matrix for the blue color), the value of each color is unsigned integer decimal with the range 0 to 255 [51-56]. Each color value can be presented by 8 binary bits [67-61]. A set of bytes can be easily selected to be used for SM hiding and extracting, these bytes must be converted to binary to form the image binary matrix as shown in figure 3, the selected number of bits in the covering bytes will replaced by the reshaped MBM in the hiding phase, and the selected number of bits can be extracted from the stego bytes to form the reshaped MBM.

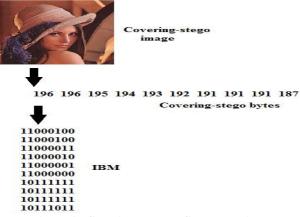


Figure 3: Covering-stego DCI preparation

1.2 Analysis of quality effects using various bits for SM hiding-extracting In this paper research we will refer to bits of the covering_stego byte using the bit index and the order of least significant bit (LSB) used as shown in table 2 [11-17]:

Table 2: LSBs indexes and orders								
Index	1	2	3	4	5	6	7	8
		Dec	imal value of	f the covering	g-stego byte:	185		
Binary value	1	0	1	1	1	0	0	0
LSB order	LSB8	LSB7	LSB6	LSB5	LSB4	LSB3	LSB2	LSB1

The quality of the stego image will depend the used order of LSB and the number of used LSBs for SM hiding, the best quality can be achieved when using LSB1 bit, but this choice will decrease the capacity hiding to be equal the image size divided by 8. Here we have to notice the following [18-22]:

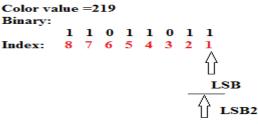
International Journal of Engineering Technology Research & Management

Published By:

https://www.ijetrm.com/

- Increasing the order LSB will decrease the quality of the stego image without affecting the hiding capacity.
- Increasing the number of used bits will decrease the quality of the stego image and it will increase the hiding capacity of the covering image.
- Most methods of message steganography used LSB1 or LSB2 with LSB1 for data hiding; here the changes in the covering byte value will be within the range -3 to +3 keeping the stego image closed to the covering image.

To show the effects of changing various bit the color byte shown in figure 4 was taken, table 3 shows the effects of changing 1 bit, while table 2 shows the effects of changing 2 bits (these effects can be measured by the mean square error (MSE), and peak signal to noise ratio (PSNR) calculated between the source value and changed value, the lower value of MSE and higher value of PSNR point to a small changes) [23-40]:



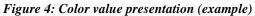


	Table	3: Effects of changing	one bu	
Order of changed	Range of changes	New value	MSE	PSNR
bits				
1	-1 to +1	218	1	107.7814
2	-2 to +2	217	4	80.0555
3	-3 to +3	223	16	80.4175
4	-7 to +7	211	64	66.1926
5	-15 to +16	203	256	52.3297
6	-31 to +31	251	1024	41.1943
7	-63 to +63	155	4096	24.6038
8	-127 to +127	91	16384	10.7408
1-2 LSB2	-3 to +3	216	9	85.8092
2-3 (2 bits)	-6 to +6	221	4	80.0555
3-4(2 bits)	-12 to +12	215	16	80.4175
1-4 (4 bits)	-15 to +15	212	49	68.8632

The covering DCI color values can be converted to fractional decimal values, and these fractions can be converted to binary using 16_bits binary presentation. DCI can be normalized by dividing each value in the image by 255, figures 5 and 6 show a sample image and the equivalent normalized image.

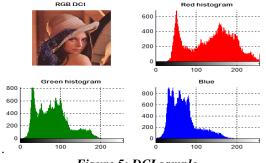
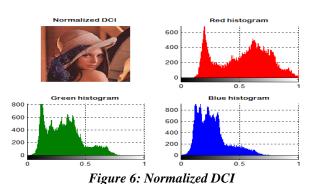


Figure 5: DCI sample

International Journal of Engineering Technology Research & Management

Published By: https://www.ijetrm.com/



Using normalized DCI and 16_bits binary representation will provide a normalized image binary matrix (NIBM) with 16 columns as shown in figure 7, this will make the process of selecting LSB and the sets of LSBs for data hiding more flexible. As shown in figure 8 replacing the least significant 8 bits will keep the stego value closed to the covering value, so we can raise the hiding capacity to the image size, and one character will require one covering value to be hidden

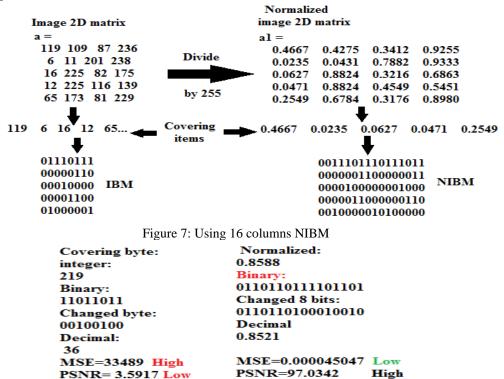


Figure 8: Changing the normalized value will keep the quality high

Using fractional colors values and 16_bits binary representation will give us the ability to use any set of bits starting from LSB1 and ending with LSB8, in the proposed method we will use a set of 8 bits; this will increase the hiding capacity to the image size, making the image capable to hid short and very long messages. A lot of data steganography methods were introduced, many of these methods were based on LSB (classical LSB: CLSB) and LSB2 methods. These methods use one or two bits from the covering bytes to hide the message bits, table 4 shows the main features of these methods [60-65]:

Table 4: Main features of LSB and LSB2 based method

Feature	LSB	LSB2
Used bits	LSB1	LSB2 and LSB1
Changes range	-1 to +1	-3 to +3

International Journal of Engineering Technology Research & Management

Published By:

https://www.ijetrm.com/

Capacity hiding in characters	Image size divided by 8	Image size divided by 4
Required operations	Sequence of logical and arithmetic	Sequence of logical and arithmetic
	operations	operations
Hiding/extracting scenario	Character by character in	Character by character in
	consecutive bytes	consecutive bytes
Quality of stego image	Good	Good
Speed	Moderate	Moderate

The proposed method will enhance the features of existing methods by providing the following:

- Possibility of a set of covering bytes bits (from1 bit to 8 bits) keeping the quality of the stego image good, see table 5.
- Increasing the hiding capacity to reach the covering image size.
- Replacing logical and arithmetic operations by simple assignment operation.
- Each character will be hidden in inconsecutive covering bytes.
- Speeding up the process of message hiding and extracting by reducing the hiding time and the extracting time.

Table 5: Effect of changing the number of used LSBs

Tuble 5. Effect of changing the number of used ESDs						
Covering byte=219, Normalized= 0.8588						
	Binary: 0110110111101101					
Changed LSBs	New value	MSE	PSNR			
LSB1	0.8588	3.4670e-009	191.7560			
LSB2 to LSB1	0.8588	4.6405e-012	257.9182			
LSB3 to LSB1	0.8587	1.4380e-008	177.5305			
LSB4 to LSB1	0.8585	1.3254e-007	155.3202			
LSB5 to LSB1	0.8589	1.5432e-008	176.8275			
LSB6 to LSB1	0.8580	7.2648e-007	138.3067			
LSB7 to LSB1	0.8560	7.8706e-006	114.4799			
LSB8 to LSB1	0.8521	4.5047e-005	97.0342			

OBJECTIVES

The main objective of the study is to enhance the hiding capacity and to introduce a simple, highly efficient, highly secure, method of data steganography.

METHODOLOGY

The hiding function of the proposed method will be implemented applying the following steps: *Step 1: SM preparation:*

- a) Get the message.
- b) Get the message length (L).
- c) Convert the message to binary to get MBM.
- d) Select the length of the set of the bits to be used to hole the message bits (N).
- e) Reshape MBM to N columns matrix to get RMBM.
- Step 2: Covering bytes preparation:
 - a) Get the covering image.
 - *b)* Normalize the image.
 - c) Get the image size.
 - *d) Reshape the image matrix to on row matrix.*
 - *e) Get a covering bytes (with length equal L*N/8);*
 - f) Use 16_bits binary presentation to convert the covering bytes to binary to get NIBM.

Step 3: Message hiding:

- a) Let the N bits of the NIBM equal RMBM.
- b) Convert the bytes back to binary to get the stego bytes.
- c) Return back the stego bytes to the image row matrix.
- *d) Reshape the image row matrix to 3D matrix to get the stego image.*

International Journal of Engineering Technology Research & Management

Published By: https://www.ijetrm.com/

The extracting function will be implemented applying the following steps:

Step 1: Stego image preparation:

- a) Get the stego image.
- *b) Get the image size.*
- c) Reshape the image 3D matrix to one row matrix.
- Step 2:Stego bytes processing:
 - a) Get the message length (L).
 - b) Get the length of the used bits (N)
 - c) Extract the stego bytes with length equal L*N/8.
 - *d)* Use 16_bits binary presentation to convert the stego bytes to binary to get NIBM.

Step 3: Message extraction:

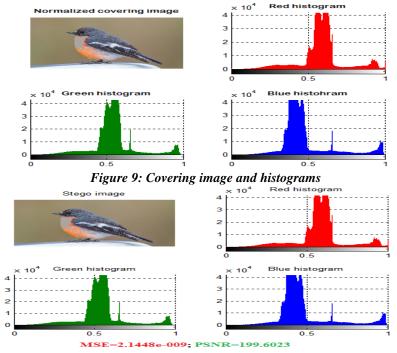
- a) From NIBM extract the N bits.
- b) Reshape the extracted matrix to 8 columns matrix to get MBM.
- c) Convert MBM to decimals.
- d) Convert the decimals results to characters to get the secret message.

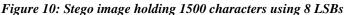
RESULTS AND DISCUSSION

The proposed method in this paper research was implemented in mat lab 7 environments with the following computer specifications:

Processor:	Intel(R) Core(TM) i5-3210M CPU @ 2.50GHz 2.50 GHz
Installed memory (RAM):	4.00 GB
System type:	64-bit Operating System
Pen and Touch:	No Pen or Touch Input is available for this Display
Pen and Touch:	No Pen or Touch Input is available for this Display

A message with 1500 characters length was selected and hidden in a covering image using various lengths the set of used LSBs. The quality of the stego image was always acceptable and good based on the received stego image and the calculated quality parameters between the covering and the stego images, figures 9 and 10 show sample outputs, while table 7 shows the values of the quality parameters.





ijetrm

International Journal of Engineering Technology Research & Management

Published By:

https://www.ijetrm.com/

Table 7: Quality parameters using various sets of LSBs

		8 3	
Used LSBs	MSE	PSNR	Hiding capacity (byte)
LSB1	1.5918e-012	271.6616	764907
LSB2	4.4395e-012	261.4048	764907
LSB3	1.6762e-011	248.1191	764907
LSB4	6.1867e-011	235.0603	764907
LSB5	2.1986e-010	222.3805	764907
LSB6	9.0868e-010	208.1903	764907
LSB7	3.7889e-009	193.9119	764907
LSB8	1.5034e-008	180.1296	764907
LSB9	6.1053e-008	166.1152	764907
LSB2 to LSB1	2.6733e-012	266.4771	1529814
LSB4 to LSB1	1.8070e-011	247.3675	3059628
LSB8 to LSB1	2.2662e-009	199.0518	6119256

From the obtained results shown in table 7 we can see the following:

- Any LSB from LSB1 to LSB8 can be used to hide the message bits keeping the quality of the stego image high.
- Two LSBs can be used to hide the message keeping the quality of the stego image high; in this case the capacity hiding will equal the image size divided by 4.
- A set of 4 LSBs can be used, keeping the quality of the stego image high, in this case the hiding capacity will equal the covering image size divided by 2.
- 8 LSBs can be used efficiently to hide the message bits, in this case the covering image will capable to hide very long messages, and the hiding capacity will equal the covering image size.

The speed of the proposed method was tested, several messages were selected, 8 LSBs were used for message hiding, the hiding time in seconds (HT), the extracting time in seconds (ET) were calculated, and the hiding throughput in K bytes per second, and the extracting throughput in K bytes per second were computed and table 8 shows the obtained speed results:

Message	HT	ET	Hiding throughput	Extracting
length(character)				throughput
100	0.0890	0.0090	1.0973	10.8507
250	0.0900	0.0110	2.7127	22.1946
500	0.0950	0.0120	5.1398	40.6901
750	0.0990	0.0150	7.3982	48.8281
1000	0.1020	0.0170	9.5741	57.4449
1500	0.1070	0.0210	13.6901	69.7545
2000	0.1160	0.0270	16.8373	72.3380
2500	0.1220	0.0280	20.0115	87.1931
5000	0.1580	0.0480	30.9039	101.7253
10000	0.2330	0.0890	41.9126	109.7261
50000	1.0660	0.4080	45.8050	119.6768
Average	0.2070	0.0623	17.7348	67.3111

Table 8: Proposed method speed results

The proposed method as shown in table 8 provided a good speed parameters, the hiding and extracting times grow slowly when increasing the message length and there is a linear relationship between each of the times and the message length (see figure 11).

IFTRA

International Journal of Engineering Technology Research & Management Published By:

https://www.ijetrm.com/

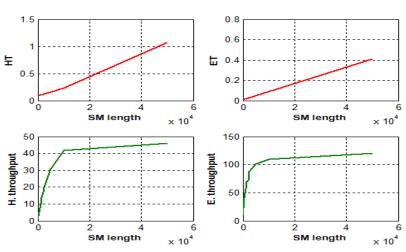


Figure 11: Speed parameters vs message length

Comparing with other existing methods of data steganography, the proposed method provided a speed up, it increased both the hiding and extracting throughputs (see table 9).

Table 9: Speed up of the proposed method					
Method	HTP	ETP	Hiding speed up of	Extracting speed up	
			the proposed	of the proposed	
			method	method	
Proposed	17.7348	67.3111	1.0000	1.0000	
CLSB[65]	15.7510	13.4389	1.1259	5.0087	
SLSB[65]	0.1562	13.4389	113.5391	5.0087	
DSLSB[65]	1.4236	13.4389	12.4577	5.0087	

CONCLUSION

A simple method of secret message steganography was proposed; the method used a normalized digital color image as a covering image. The proposed method was flexible; it allowed using any bits from LSB1 to LSB8 to be used to hold the message bits. A set of LSBs can be selected to hold the message bits, thus the capacity hiding was increased keeping the stego image in good quality. 8 LSBs bits in each covering image color values were used to hide the message bits and the obtained results showed that the quality of the stego image was always good and the hiding capacity was increased to reach the covering image size. The proposed method allowed the user to select the set of LSBs; this set can be used as a private key to protect the hidden message. The proposed method was implemented using various messages and various set of LSBs, the obtained results proved that the proposed method satisfied the quality requirements of good stego method. The proposed method increased the throughputs of message hiding and extracting and it speeded up the process of message steganography comparing with other existing methods.

REFERENCES

[1]Prof. Ziad A.A. Alqadi, Prof. Mohammed K. Abu Zalata, Ghazi M. Qaryouti, Comparative Analysis of Color Image Steganography, JCSMC, Vol.5, Issue. 11, November 2016, pg.37-43.

[2]M. Jose, "Hiding Image in Image Using LSB Insertion Method with Improved Security and Quality", International Journal of Science and Research, Vol. 3, No. 9, pp. 2281-2284, 2014.

[3]Emam, M. M., Aly, A. A., & Omara, F. A. An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection. International Journal of Advanced Computer Science & Applications,1(7), pp. 361-366, (2016). https://doi.org/10.14569/IJACSA.2016.070350.

[4]Mohammed Abuzalata; Ziad Alqadi; Jamil Al-Azzeh; Qazem Jaber, Modified Inverse LSB Method for Highly Secure Message Hiding, IJCSMC, Vol. 8, Issue. 2, February 2019, pg.93 - 103.

International Journal of Engineering Technology Research & Management

Published By:

https://www.ijetrm.com/

[5]Rashad J. Rasras, Mutaz Rasmi Abu Sara, Ziad A. AlQadi, Engineering, A Methodology Based on Steganography and Cryptography to Protect Highly Secure Messages Engineering Technology & Applied Science Research, Vol.9 Issue 1, Pages 3681-3684, 2019.

[6]Zhou X, Gong W, Fu W, Jin L. 2016An improved method for LSB based color image steganography combined with cryptography. In 2016 IEEE/ACIS 15th Int. Conf. on Computer and Information Science (ICIS), Okayama, Japan, pp. 1–4 . <u>https://doi.org/10.1109/ICIS.2016.7550955</u>.

[7]Wu D-C, Tsai W-H. A steganographic method for images by pixel value differencing. Pattern Recognition. Lett. 24, 1613–1626. 2003 <u>https://doi.org/10.1016/S0167-8655(02)00402-6</u>.

[8]Das R, Das I. Secure data transfer in IoT environment: adopting both cryptography and steganography techniques. In Proc. 2nd Int. Conf. on Research in Computational Intelligence and Communication Networks, Kolkata, India, pp. 296–301, 2016. <u>https://doi.org/10.1109/ICRCICN.2016.7813674</u>.

[9] Rashad J. Rasras, Mutaz Rasmi Abu Sara, Ziad A. AlQadi, Rushdi Abu zneit, Comparative Analysis of LSB, LSB2, PVD Methods of Data Steganography, International Journal of Advanced Trends in Computer Science and Engineering, vol. 8, issue 3, pp.748-754, 2019,

http://www.warse.org/IJATCSE/static/pdf/file/ijatcse64832019.pdf

[10] Ayman Al-Rawashdeh, Ziad Al-Qadi, using wave equation to extract digital signal features, Engineering, Technology & Applied Science Research, vol. 8, issue 4, pp. 1356-1359, 2018.

[11] K Matrouk, A Al-Hasanat, H Alasha'ary, Z. Al-Qadi Al-Shalabi, "Speech fingerprint to identify isolated word person", World Applied Sciences Journal, Vol. 31, No. 10, pp. 1767-1771, 2014.

[12] Saleh Khawatreh, Belal Ayyoub, Ashraf Abu-Ein, Ziad Alqadi , A Novel Methodology to Extract Voice Signal Features , International Journal of Computer Applications, Volume 179 – No.9, January 2018.

[13] Ziad Alqadi, Bilal Zahran, Qazem Jaber, Belal Ayyoub, Jamil Al-Azzeh, Enhancing the Capacity of LSB Method by Introducing LSB2Z Method, International Journal of Computer Science and Mobile Computing, vol. 8, issue 3, pp. 76-90, 2019.

[14] Ziad A. Alqadi, Majed O. Al-Dwairi, Amjad A. Abu Jazar and Rushdi Abu Zneit, Optimized True-RGB color Image Processing, World Applied Sciences Journal 8 (10): 1175-1182, ISSN 1818-4952, 2010.
[15] Waheeb, A. and Ziad AlQadi, Gray image reconstruction. Eur. J. Sci. Res., 27: 167-173, 2009.
[16] A. A. Moustafa, Z. A. Alqadi, "Color Image Reconstruction Using a New R'G'I Model", Journal of Computer Science, Vol.5, No. 4, pp. 250-254, 2009.

[17] Prof. Ziad A.A. Alqadi, Prof. Mohammed K. Abu Zalata, Ghazi M. Qaryouti, Comparative Analysis of Color Image Steganography, JCSMC, Vol.5, Issue. 11, November 2016, pg.37–43.

[18] H. Alasha'ary, K. Matrouk, A. Al-Hasanat, Z. A alqadi, H. Al-Shalabi (2013), Improving Matrix Multiplication Using Parallel Computing, International Journal on Information Technology (I.RE.I.T.) Vol.1, N. 6 ISSN 2281-2911.

[19] Bilal Zahran, Ziad Alqadi, Jihad Nader, Ashraf Abu Ein A COMPARISON BETWEEN PARALLEL AND SEGMENTATION METHODS USED FOR IMAGE ENCRYPTION-DECRYPTION, International Journal of Computer Science & Information Technology (IJCSIT) Vol 8, No 5, October 2016.

[20] Z.A. Alqadi, A. Abu-Jazar (2005), Analysis of Program Methods Used for Optimizing Matrix Multiplication, Journal of Engineering, vol. 15 n. 1, pp. 73-78.

[21] Jamil Al-Azzeh, Bilal Zahran, Ziad Alqadi, Belal Ayyoub, Muhammed Mesleh: A Novel Based On Image Blocking Method to Encrypt-Decrypt Color JOIV: International Journal on Informatics Visualization, 2019.
[22] Jamil Al-Azzeh, Bilal Zahran, Ziad Alqadi, Belal Ayyoub and Mazen Abu-Zaher: A Novel Zero-Error Method to Create a Secret Tag for an Image; Journal of Theoretical and Applied Information Technology 15th July 2018.

[23] Jamil Al Azzeh, Ziad Alqadi Qazem, M. Jabber: Statistical Analysis of Methods Used to Enhanced Color Image Histogram; XX International Scientific and Technical Conference; Russia May 24-26, 2017.

[24] Jamil Al Azzeh, Hussein Alhatamleh, Ziad A. Alqadi, Mohammad Khalil Abuzalata: Creating a Color Map to be used to Convert a Gray Image to Color Image; International Journal of Computer Applications (0975–8887). Volume 153 – No2, November 2016.

[25] Khaled Matrouk, Abdullah Al- Hasanat, Haitham Alasha'ary, Ziad Al-Qadi, Hasan Al-Shalabi Analysis of Matrix Ziad Alqadi et al, International Journal of Computer Science and Mobile Computing, Vol.8 Issue.3,

International Journal of Engineering Technology Research & Management

Published By:

https://www.ijetrm.com/

March- 2019, pg. 76-90.

[26] Mohammed Abuzalata; Ziad Alqadi, Jamil Al-Azzeh; Qazem Jaber Modified Inverse LSB Method for Highly Secure Message Hiding: International Journal of Computer Science and Mobile Computing, Vol.8 Issue.2, February- 2019, pg. 93-103.

[27] Qazem Jaber Rashad J. Rasras, Mohammed Abuzalata, Ziad Alqadi, Jamil Al-Azzeh; Comparative Analysis of Color Image Encryption-Decryption Methods Based on Matrix Manipulation: International Journal of Computer Science and Mobile Computing, Vol.8 Issue.2, 2019/3.

[28] Jamil Al-Azzeh, Ziad Alqadi, Mohammed Abuzalata; Performance Analysis of Artificial Neural Networks used for Color Image Recognition and Retrieving: International Journal of Computer Science and Mobile Computing, Vol.8 Issue.2, February- 2019.

[29] Rashad J. Rasras, Mohammed Abuzalata; Ziad Alqadi; Jamil Al-Azzeh; Qazem Jaber, Comparative Analysis of Color Image Encryption-Decryption Methods Based on Matrix Manipulation International Journal of Computer Science and Mobile Computing, Vol.8 Issue.3, March- 2019, pg. 14-26.

[30] AlQaisi Aws, AlTarawneh Mokhled, A Alqadi Ziad, A Sharadqah Ahmad , Analysis of Color Image Features Extraction using Texture Methods , TELKOMNIKA, vol. 17, issue 3, 2018.

[31] B. Zahran, J. AL-Azzeh, Z. Al Qadi, M. Al Zoghoul and S. Khawatreh, "A MODIFIED LBP METHOD TO EXTRACT FEATURES FROM COLOR IMAGES", Journal of Theoretical and Applied Information Technology(JATIT), Vol.96. No 10, 2018.

[32] J. AL-AZZEH, B. ZAHRAN, Z. ALQADI, B. AYYOUB, M. ABU-ZAHER, "A novel Zero-error Method to Create a Secret Tag for an Image", Journal of Theoretical and Applied Information Technology(JATIT), Vol.96. No 13, 2018.pp: 4081-4091.

[33] J. AL-AZZEH, B. ZAHRAN, Z. ALQADI," Salt and Pepper Noise: Effects and Removal", International Journal on Informatics Visualization, Vol.2. No 4, 2018.pp: 252-256.

[34] Jihad Nader, Ziad Alqadi, Bilal Zahran, "Analysis of Color Image Filtering Methods", International Journal of Computer Applications (IJCA), Volume 174, issue 8, 2017, pp:12-17.

[35] Ziad Alqadi, Bilal Zahran, Jihad Nader, "Estimation and Tuning of FIR Low pass Digital Filter Parameters", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 7, Issue 2, 2017, pp:18-23.

[36] Khaled Aldebei, Mua'ad M. Abu-Faraj, Ziad A. Alqadi, Comparative Analysis of Fingerprint Features Extraction Methods, Journal of Hunan University Natural Sciences, vol. 48, issue 12, pp. 177-182, 2022.[37] Dr. Mohamad Barakat Prof. Ziad Alqadi, Highly Secure Method for Secret Data Transmission,

[37] Dr. Monamad Barakat Prof. Ziad Alqadi, Highly Secure Method for Secret Data Transmissio International Journal of Scientific Engineering and Science, vol. 6, issue 1, pp. 49-55, 2022.

[38] Ziad A. Alqadi Mua'ad M. Abu-Faraj, Rounds Reduction and Blocks Controlling to Enhance the Performance of Standard Method of Data Cryptography, International Journal of Computer Science and Network Security, vol. 21, issue 12, pp. 648-656, 2021.

[39] Ziad Alqadi Mua'ad Abu-Faraj, Khaled Aldebei, DEEP MACHINE LEARNING TO ENHANCE ANN PERFORMANCE: FINGERPRINT CLASSIFIER CASE STUDY, JOURNAL OF SOUTHWEST JIAOTONG UNIVERSITY, vol. 56, issue 6, pp. 686-694, 2021.

[40] Ziad A. Alqadi Mua'ad M. Abu-Faraj, Improving the Efficiency and Scalability of Standard Methods for Data Cryptography, International Journal of Computer Science and Network Security, vol. 21, issue 12, pp.451-458, 2021

[41] Mua'ad M. Abu-Faraj Prof. Ziad Alqadi, Using Highly Secure Data Encryption Method for Text File Cryptography, International Journal of Computer Science and Network Security, vol. 20, issue 11, pp. 53-60, 2021.

[42] AlQaisi Aws, AlTarawneh Mokhled, A Alqadi Ziad, A Sharadqah Ahmad, Analysis of Color Image Features Extraction using Texture Methods, TELKOMNIKA, vol. 17, issue 3, 2018.

[43] Ziad A AlQadi Amjad Y Hindi, O Dwairi Majed, PROCEDURES FOR SPEECH RECOGNITION USING LPC AND ANN, International Journal of Engineering Technology Research & Management, vol. 4, issue 2, pp. 48-55, 2020.

[44] Ziad A Alqadi, Mohamad Tariq Barakat, A Case Study to Improve the Quality of Median Filter, International Journal of Computer Science and Mobile Computing, vol. 10, issue 11, pp. 19 – 28, 2021.
[45] Dr. Hatim Ghazi Zaini Prof. Ziad Alqadi, High Salt and Pepper Noise Ratio Reduction, International Journal of Computer Science and Mobile Computing, vol. 10, issue 9, pp. 88 – 97, 2021.

International Journal of Engineering Technology Research & Management

Published By:

https://www.ijetrm.com/

[46] Prof. Mohamad K. Abu Zalata, Hussein N. Hatamleh, Prof. Ziad A. Alqadi, Detailed Study of Low Density Salt and Pepper Noise Removal from Digital Color Images, IJCSMC, Vol. 11, Issue. 2, PP. 56 – 67, February 2022.

[47] [43] M. Abu-Faraj, A. Al-Hyari, K. Aldebei, B. Al-Ahmad, and Z. Alqadi, "Rotation Left Digits to Enhance the Security Level of Message Blocks Cryptography," IEEE Access, vol. 10, pp. 69388- 69397, 2022, doi:10.1109/ACCESS.2022.3187317.

[48] M. Abu-Faraj, A. Al-Hyari, and Z. Alqadi, "Experimental Analysis of Methods Used to Solve Linear Regression Models," CMC-Computers, Materials & Continua, vol. 72, no. 3, pp. 5699-5712, 2022, doi:10.32604/cmc.2022.027364. (Web of Science Indexed, Scopus Indexed).

[49] M. Abu-Faraj, A. Al-Hyari, and Z. Alqadi, "Complex Matrix Private Key to Enhance the Security Level of Image Cryptography," Symmetry, vol. 14, Iss. 4, pp. 664-678, 2022, doi:10.3390/sym0664. (Web of Science Indexed, Scopus Indexed)

[50] M. Abu-Faraj, K. Aldebei, and Z. Alqadi, "Simple, Efficient, Highly Secure, and Multiple Purposed Method on Data Cryptography," Traitement du Signal, vol. 39, no. 1, pp. 173-178, 2022, doi:10.18280/ts.390117. (Web of Science Indexed, Scopus Indexed)

[51] M. Abu-Faraj, and Z. Alqadi, "Rounds Reduction and Blocks Controlling to Enhance the Performance of Standard Method of Data Cryptography," International Journal of Computer Science and Network Security (IJCSNS), vol. 21, no. 12, pp. 648-656, 2021, doi: 10.22937/IJCSNS.2021.21.12.89. (Web of Science Indexed) [52] M. Abu-Faraj, and Z. Alqadi, "Improving the Efficiency and Scalability of Standard Methods for Data

Cryptography," International Journal of Computer Science and Network Security (IJCSNS), vol. 21, no.12, pp. 451-458, 2021, doi:10.22937/IJCSNS.2021.21.12.61. (Web of Science Indexed)

[53] M. Abu-Faraj, and Z. Alqadi, "Using Highly Secure Data Encryption Method for Text File Cryptography," International Journal of Computer Science and Network Security (IJCSNS), vol. 21, no.12, pp. 53-60, 2021, doi:10.22937/IJCSNS.2021.21.12.8. (Web of Science Indexed)

[54] M. Abu-Faraj, and M. Zubi, "Analysis and Implementation of Kidney Stones Detection by Applying Segmentation Techniques on Computerized Tomography Scans," Italian Journal of Pure and Applied Mathematics, iss. 43, pp. 590-602, 2020. (Scopus Indexed)

[55] Prof. Ziad Alqadi, Bits Substitution to Secure LSB Method of Data Steganography, International Journal of Computer Science and Mobile Computing, vol. 11, issue 8, pp. 9 – 21, 2022.

[56] Mohammad S. Khrisat Prof. Ziad Alqadi, Enhancing LSB Method Performance Using Secret Message
Segmentation, International Journal of Computer Science and Network Security, vol. 22, issue 7, pp. 1-6, 2022.
[57] Hatim Ghazi Zaini and Ziad A. Alqadi Mohammad S. Khrisat, Adnan Manasreh, COVER IMAGE
REARRANGEMENT TO SECURE LSB METHOD OF DATA STEGANOGRAPHY, Journal of Engineering

REARRANGEMENT TO SECURE LSB METHOD OF DATA STEGANOGRAPHY, Journal of Engineering and Applied Sciences, vol. 17, issue 3, pp. 294-302, 2022.

[58] Mohamad K Abu Zalata, Mohamad T Barakat, Ziad A Alqadi, Carrier Image Rearrangement to Enhance the Security Level of LSB Method of Data Steganography, International Journal of Computer Science and Mobile Computing, vol. 11, issue 1, pp. 182 – 193, 2022.

[59] Dr. Mohamad barakat Prof. Ziad Alqadi, IMAGE TRANSFORMATION TO INCREASE THE SECURITY LEVEL OF LBS METHOD OF DATA STEGANOGRAPHY, International Journal of Engineering Technology Research & Management, vol. 6, issue 1, pp. 42-53, 2022.

[60] Naseem Asad, Ismail Shayeb, Qazem Jaber, Belal Ayyoub, Ziad Alqadi, Ahmad Sharadqh, creating a Stable and Fixed Features Array for Digital Color Image, IJCSMC, Vol. 8, Issue. 8, August 2019, pg.50 –62.
[61] Majed O. Al-Dwairi, Amjad Y. Hendi, Mohamed S. Soliman, Ziad A.A. Alqadi, A new method for voice signal features creation, International Journal of Electrical and Computer Engineering (IJECE), vol. 9, issue 5, pp. 4092-4098, 2018.

[62] Akram A. Moustafa and Ziad A. Alqadi, A Practical Approach of Selecting the Edge Detector Parameters to Achieve a Good Edge Map of the Gray Image, Journal of Computer Science 5 (5): 355-362, 2009.

[63] ZA Alqadi, Musbah Aqel, Ibrahiem MM El Emary, Performance analysis and evaluation of parallel matrix multiplication algorithms, World Applied Sciences Journal, vol. 5, issue 2, pp. 211-214, 2008.

[64] Ismail Shayeb, Naseem Asad, Ziad Alqadi, Qazem Jaber, Evaluation of speech signal features extraction methods, Journal of Applied Science, Engineering, Technology, and Education is licensed under an Attribution-Non Commercial-Share Alike 4.0 International (CC BY-NC-SA 4.0)

International Journal of Engineering Technology Research & Management Published By:

https://www.ijetrm.com/

[65] Dr. Mohammed Abbas Fadhil Al-Husainy, COMPARISON STUDY BETWEEN CLASSIC-LSB, SLSB AND DSLSB IMAGE STEGANOGRAPHY, ICIT 2013 The 6th International Conference on Information Technology.