International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320-088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 11, Issue. 2, February 2022, pg.31 – 45

Protecting and Enhancing the Process of Data Steganography

Prof. Ziad Alqadi; Prof. Mohamad Abu Zalata

Albalqa Applied University
Faculty of Engineering Technology, Jordan – Amman

DOI: 10.47760/ijcsmc.2022.v11i02.005

Abstract: A method of data steganography will be proposed, this method will use simple operation to apply the process of data hiding and data extracting, it will be shown that using these operations will optimize the performance parameters values. The proposed method will use a simple way for message encoding-decoding to provide a necessary protection to LSB method. The proposed method will be implemented and compared with LSB method to show how the proposed method will enhance the values of MSE, PSNR, hiding time and extracting time. The proposed method will use bit plate from 1 (LSB) to 8 (MSB) to hide various messages (short and long messages) using various covering images, and it will be shown that even if use the MSB for data hiding the results will be acceptable.

Keywords: Steganography, encoding, decoding, MSE, PSNR, LSB, MSB.

Introduction

Text messages are now circulating through various social media, and some of these messages may be confidential or of a personal nature, which requires us to protect them from the danger of reading from unauthorized persons or entities and protect them from intruders and data thieves [1-5]. Text messages are classified into short text messages and long text messages, and regardless of the length of the secret text message, the necessary means of protection must be provided for it. Multiple methods are used to protect text messages, including encoding the message, by modifying the character values in the text message. In this research paper, we will adopt the process of subtracting the value of the ASCII symbol in the text message from a large value (and we will use the value 222), table 1 shows the results of encoding some messages [6-11]:

Table 1; Message encoding example

Message number	Message	Encoded message
1	Ziad Alqadi	u}z¾rm}zu
2	Albalqa Applied University	r} rm}¾nnruyz¾puhylkuje
3	Amman is the capital city of Jordan	qq}p¾uk¾jvy¾{ }nuj}r¾{uje¾ox¾olz}p
4	Protecting and enhancing LSB method	lojy{jupw¾}pz¾ypv}p{upw¾¾qyjvoz
5	Covering and stego images	ohylupw¾}pz¾kkywo¾uq}wyk

6	Data steganography using color images	š{j}³⁴kzyw}powl}nve³⁴ikupw³⁴{orol³⁴uq}wyk
7	Securing secret and private messages	y{ilupw³⁴ky{lyj³⁴}pz³⁴nluh}jy³⁴qykk}wyk
8	Simplifying and enhancing LSB method of data steganography	uqnruxeupw³⁴}pz³⁴ypv}p{upw³⁴³⁴qyjvoz³⁴ox³⁴zjj}³⁴kzyw}powl}nve

Data steganography can be used to protect encoded secret message by hiding it into a covering image to produce a stego_image as shown in figure 1 and 2 [12-15]:

Figure 1: Message steganography (Hiding process)

Figure 2: Message steganography (extracting process)

Colored digital images are one of the most important sources that can be used as a medium that carries the secret text message, and this is due to many reasons, the most important of which are [16-20]:

- Ease of obtaining the digital image at no cost due to the availability of various equipment for capturing and saving the digital image.
- Ease of processing the digital image by representing the digital image in a three-dimensional matrix, where each dimension is assigned to each of the three colors (red, green and blue) and as shown in the figure3
- Ease of reshaping the image by converting it to a one-dimensional vector and the possibility of using parts of the image in processing operations.
- The large size of the images, which provides the necessary environment to hide text messages in them without noticing changes in the carrier image with the naked eye.

Figure 3: Color image representation

- Match the pixel values in the digital image with the ASCII values of the symbols in the text message, all of which are within the range 0 to 255.

Data steganography and LSB method

Data steganography means hiding data such as secret messages into a covering color image to produce stego_image. The process of embedding secret message into color image must not affect too much the stego_image, the changes in the stego_image must be minimal and cannot be noticed by human naked eyes. The changes can be measured by mean square error (MSE) and/or peak signal to noise ratio (PSNR), these parameters can be calculated using equations 1 and 2 shown below [21-27]:

MSE of x channel

$$MSE_x = \frac{1}{N} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [S(i, j) - R(i, j)]^2, N = m * n \quad (1)$$

Total MSE

$$MSE_t = MSE_R + MSE_G + MSE_B$$

Calculate PSNR

$$PSNR = 10 * \log_{10} \frac{(MAX_I)^2}{MSE_t} \quad (2)$$

MSE between covering and stego images must be very small, while PSNR between them must be very high, this will indicate that the changes in the stego_image cannot be noticed by human eyes [28-30].

Many methods used for data steganography are based on the standard least significant bit method of data (LSB) hiding/extracting. LSB used the least significant bits of 8 covering bytes to hide one byte of the secret message to be hidden in the covering color image, as shown in figure 4. Replacing the least significant bit in the covering byte by one bit of the message byte will cause a change that ranges from 1 to -1, these changes in the covering pixel color will be not noticed.

Figure 4: The effects of bit replacing

Hiding process can be maintained by using other bits rather than least significant bit, here we can use a bit plane from 1 to 8 to hide the secret message, but the changes here will be increased, using most significant bit will cause a change within the range -127 to 127 [31-34].

LSB method of data steganography reserved 8 bytes of the covering image to hide 1 byte of the secret message, the covering image and the secret message must be converted to binary, and the bit from the message byte must be inserted in the associated LSB of the covering bytes as shown in figure 5 [35-38].

Figure 5: LSB method implementation example

The proposed method

The proposed method provides a protection procedure to secure the hidden message, this procedure can be implemented applying message encoding before hiding and message decoding after hiding as shown in figure 6. The encoding and decoding processes can be implemented applying the equation '222-message'. The process of LSB method for data hiding and data extraction was simplified this will improve the efficiency of the proposed method, also the proposed method can use any bit plate for data hiding starting from bit 1 (LSB) and ending with bit 8 (MSB).

Figure 6: Proposed method process

The proposed method for embedding the secret message will be implemented applying the following algorithm:

Algorithm: Hiding phase

Inputs:

Covering image (I), secret message (txt), bit plate (b).

Processing:

1. Retrieve image size(S), Retrieve message size (m), calculate message binary size ($N=m*8$).
2. Encode the message
3. Find p and h . ($p = 2^b$, $h = 2^{(b-1)}$).
4. Reshape the image I to one row array ($I1$).
5. Find the deference between S and N ($addl$).
6. From $I1$ get an array of size equal N ($I2$).
7. From $I2$ get a sign array (si) (1 if greater than zero, zero otherwise).
8. For $k = 1$ to N
9. If $si(k) = 0$ then $si(k) = 1$.
10. $I2(k) = \text{round}(I2(K))$.
11. If $I2(k) \bmod p \geq h$ then $I2(k) = I2(k) - h$.
12. End for
13. Convert encrypted message to binary (bt).
14. Reshape bt to one row array ($bint$).
15. Compute d ($d=h*48$).
16. Subtract d from $h*bint$ to get bi .
17. Add bi to $I2$ to get $I3$.
18. Concatenate bi with zeros (1, $addl$) to get $binadd$.
19. Multiply si by $I3$ to get $I4$.
20. Concatenate $I4$ with $I1$ ($N+1$: S) to get $I5$.
21. Reshape $I5$ to 3D matrix to get the stego_image ($intl$).

Output:

Stego_image (intl)

The process of data extraction will be implemented applying the following algorithm:

Algorithm: Extraction phase

Inputs:

Stego_image (I), *Length of secret message (siz)*, *bit plate (b)* (the same as in hiding phase).

Processing:

1. Retrieve image size (n), calculate message binary size ($bsiz=m*8$).
2. Find p and h .
3. Reshape the image I to one row array ($I1$).
4. Find the difference between n and $bsiz$ ($add1$).
5. From $I1$ get an array of size equal $bsiz$ ($I2$).
6. Create a zero array br of size ($1, bsiz$);
7. For $k = 1$ to $bsiz$
8. Divide $I2(k)$ by p .
9. If the remainder $\geq h$, then make $rb(k)$ equal 1.
10. End for
11. Get rbi by converting rb to binary ($rbi = (dec2bin(rb,1))'$)
12. Reshape rbi to get $rbin$ ($rbin = reshape(rbi, siz, 8)$)
13. Get the message $rectxt$ by converting $rbin$ to decimal ($rectxt = (bin2dec(rbin))'$).
14. Convert $drectxt$ to character to get the secret message m
15. Decode the message.

Output:

Secret message (drectxt).

Below is a calculated example which shows the process of hiding and extracting a secret message:

Figures 7 and 8 illustrate an example of data hiding and extracting:

Figure 7: Data hiding example

Figure 8: Data extracting example

Implementation and experimental results

The proposed method can be used to insert the message bit in any selected bit plate (1 (LSB) up to 8 (MSB)). Several color images were selected to be used as a carrier images, table 2 shows the basic information of these images, while figures 9 and 10 show the selected images.

Table 2: Used images information

Image number	Resolution	Size(byte)	Capacity, Message max size(byte)
1	151 333 3	150849	18856
2	152 171 3	77976	9747
3	360 480 3	518400	64800
4	1071 1600 3	5140800	642600
5	981 1470 3	4326210	540780
6	165 247 3	122265	15283
7	360 480 3	518400	64800
8	183 275 3	150975	18872
9	183 275 3	150975	18872
10	201 251 3	151353	18919
11	600 1050 3	1890000	236250
12	1144 1783 3	6119256	764907

Figure 9: Used images 1 to 6

Figure 10: Used images 7 to 12

The messages shown in table 1 were treated using the proposed method and LSB method, a small size image was selected (image 2) as a covering image, figure 11 shows a sample output while tables 3 and 4 show the obtained experimental results:

Figure 11: Sample outputs using small image as a covering image

Table 3: Quality parameters using small in size covering image(image 2)

Message number	Proposed method		LSB method	
	MSE	PSNR	MSE	PSNR
1	4.7450e-004	187.3577	0.0029	169.2615
2	0.0013	177.1195	0.0075	159.6996
3	0.0017	174.5633	0.0098	157.0681
4	0.0019	173.6308	0.0110	155.9208
5	0.0012	178.2489	0.0087	158.3197
6	0.0019	173.5625	0.0117	155.3104
7	0.0019	173.4274	0.0114	155.5322
8	0.0029	169.3951	0.0180	150.9889
Average	0.0017	175.9132	0.0101	157.7626

Table 4: Efficiency parameters using small in size covering image (image 2)

Message number	Proposed method		LSB method	
	Hiding time(second)	Extracting time(second)	Hiding time(second)	Extracting time(second)
1	0.0042	0.0083	0.0630	0.0330
2	0.0309	0.0107	0.0470	0.0360
3	0.0049	0.0094	0.0420	0.0330
4	0.0046	0.0126	0.0420	0.0340
5	0.0045	0.0064	0.0410	0.0330
6	0.0049	0.0065	0.0430	0.0570
7	0.0041	0.0072	0.0420	0.0330
8	0.0040	0.0065	0.0440	0.0330
Average	0.0078	0.0085	0.0455	0.0365

The same experiment was repeated by replacing the covering image and using big in size covering image (image 12), figure 12 shows a sample output while tables 5 and 6 show the obtained experimental results.

From the obtained results we can see that using big in size covering image will improve the values of MSE and PSNR without too much affecting the hiding and extracting time, and here we can recommend using covering image with big size to get an excellent values of MSE and PSNR, making the changes in the stego_image un noitcible by the naked eyes.

Figure 12: Sample outputs using big image as a covering image

Table 5: Quality parameters using big in size covering image(image 12)

Message number	Proposed method		LSB method	
	MSE	PSNR	MSE	PSNR
1	6.2099e-006	230.7189	3.9220e-005	212.2884
2	1.6342e-005	221.0431	9.5600e-005	203.3787
3	2.2879e-005	217.6784	1.2959e-004	200.3365
4	2.3042e-005	217.6072	1.3809e-004	199.7014
5	1.7322e-005	220.4604	1.0704e-004	202.2484
6	2.6147e-005	216.3430	1.5427e-004	198.5935
7	2.3532e-005	217.3966	1.4544e-004	199.1826
8	3.7913e-005	212.6274	2.3173e-004	194.5248
Average	0.000021673362	219.23437500	0.0001301225	201.28178750

Table 6: Efficiency parameters using big in size covering image (image1 2)

Message number	Proposed method		LSB method	
	Hiding time(second)	Extracting time(second)	Hiding time(second)	Extracting time(second)
1	0.0820	0.0090	0.2530	0.0820
2	0.0770	0.0080	0.2600	0.0860
3	0.0780	0.0080	0.3610	0.0890
4	0.0760	0.0080	0.2490	0.0810
5	0.0770	0.0080	0.2500	0.0810
6	0.0770	0.0080	0.2510	0.0790
7	0.0770	0.0080	0.2510	0.0810
8	0.0790	0.0080	0.2620	0.0810
Average	0.0779	0.0081	0.2671	0.0825

The proposed method uses any bit plate (from 1 to 8) to hide the secret message, a 100-character message was treated using the proposed method by varying the bit plate (from 1 (LSB) to 8 (MSB)), image 12 was selected as a covering image, figure 13 shows an output example of using bit plate 8, while table 7 shows the obtained results

Table 7: Results varying bit plate and using image 12 as a covering image

Bit plate	MSE	PSNR	Hiding time	Extracting time
1 (LSB)	6.5531e-005	207.1552	0.0780	0.0080
2	2.6082e-004	193.3422	0.0780	0.0090
3	9.7528e-004	180.1531	0.0830	0.0090
4	0.0033	167.8854	0.0840	0.0100
5	0.0179	151.0284	0.0810	0.0120
6	0.0654	138.0930	0.0770	0.0090
7	0.2611	124.2557	0.0800	0.0090
8 (MSB)	1.0978	109.8926	0.0770	0.0090

Figure 13: Sample output using bit plate 8

From table 7 we can see that MSE will increase when increasing the bit plate, and PSNR will decrease when increasing the bit plate, but for all bit plate the results of MSE and PSNR will be acceptable specially if we use a covering image with big size, figure 14 shows how the values of MSE and PSNR will be affected when increasing the bit plate.

Figure 14: Effects of increasing bit plate

For long messages it is better to select a covering image with big size, this will improve the value of MSE and PSNR, table 8 shows the results of hiding 800_character message using various in sizes images:

Table 8: Result of hiding long message; Message size=800

Image number	MSE	PSNR	Hiding time	Extracting time
1	0.0210	149.4729	0.0090	0.0120
2	0.0412	142.7110	0.0070	0.0120
3	0.0061	161.8555	0.0130	0.0130
4	6.3512e-004	184.4423	0.0670	0.0120
5	7.2673e-004	183.0948	0.0580	0.0120
6	0.0267	147.0515	0.0080	0.0120
7	0.0061	161.7765	0.0130	0.0120
8	0.0213	149.3150	0.0080	0.0130
9	0.0212	149.3399	0.0070	0.0130
10	0.0211	149.4055	0.0080	0.0120
11	0.0017	174.6465	0.0290	0.0120
12	5.2098e-004	186.4233	0.0800	0.0140

Various in lengths messages were processed using the proposed method, Image 12 was selected as a covering image, the obtained results are shown in table 9

Table 9: Hiding various messages results

Message length	MSE	PSNR	Hiding time	Extracting time
100	6.5531e-005	207.1552	0.0730	0.0090
200	1.3351e-004	200.0384	0.0740	0.0090
400	2.5591e-004	193.5320	0.0770	0.0110
800	5.2098e-004	186.4233	0.0790	0.0130
1600	0.0011	179.3997	0.0790	0.0210
3200	0.0021	172.5815	0.0820	0.0250
6400	0.0042	165.4505	0.0880	0.0530
12800	0.0084	158.6296	0.1090	0.0800

25600	0.0167	151.7546	0.1200	0.1500
51200	0.0334	144.8028	0.1670	0.2890

A message of 51200 characters was treated using the proposed method, image 12 was selected as a covering image, the obtained MSE and PSNR values were acceptable even if we use bit plate 8 (MSB) for data hiding, figures 15 and 16 show the obtained stego_images.

Increasing the message length will negatively affect the values of hiding time, extracting time, MSE and PSN, to minimize the negative effects we can use a covering image with big size. Figure 17 shows the relationship between the message length and other performance parameters, from this figure we can see that the performance parameters values are meet the requirement even if use long message for data hiding.

Figure 15: Stego_image using bit plate 1 (LSB)

Figure 16: Stego_image using bit plate 8 (MSB)

Figure 17: Relationship between message length and performance parameters

Conclusion

A simple operations were used to enhance the process of data steganography using LSB method. These operation were used to implement the proposed method, the obtained results show the enhancement achieved by implementing the proposed method, the value of MSE were decreased, the PSNR values were increased and the hiding and extracting times were decreased. The proposed method adds a protection issues to LSB method base on a simple way of message encoding and decoding. The proposed method uses any bit plate for data hiding and it was shown that even if we use bit plate 8 (MSB) the obtained performance parameters values were acceptable. The proposed method gave excellent results even if we use long messages and it is recommended to use cover image with big size to keep the values of the performance parameters acceptable.

References

- [1]. 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.
- [2]. 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.
- [3]. 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.
- [4]. ZA Alqadi, Musbah Aqel, Ibrahim MM El Emary, Performance analysis and evaluation of parallel matrix multiplication algorithms, World Applied Sciences Journal, vol. 5, issue 2, pp. 211-214, 2008.
- [5]. 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.
- [6]. 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.
- [7]. 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.
- [8]. Waheeb, A. and Ziad AlQadi, Gray image reconstruction. Eur. J. Sci. Res., 27: 167-173, 2009.
- [9]. 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.

- [10].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.
- [11].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, Vol. 96. No. 13, pp. 4081-4091, 2018.
- [12].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.
- [13].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.
- [14].M. Juneja, P. S. Sandhu, An improved LSB based Steganography with enhanced Security and Embedding/Extraction, 3rd International Conference on Intelligent Computational Systems, Hong Kong China, January 26-27, 2013.
- [15].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.
- [16].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.
- [17].Z.A. Alqadi, A. Abu-Jazzar (2005), Analysis of Program Methods Used for Optimizing Matrix Multiplication, Journal of Engineering, vol. 15 n. 1, pp. 73-78.
- [18].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.
- [19].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.
- [20].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.
- [21].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.
- [22].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, March- 2019, pg. 76-90.
- [23].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.
- [24].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.
- [25].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.
- [26].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.
- [27].Jamil Al-Azzeh, Bilal Zahran, Ziad Alqadi, Belal Ayyoub, Muhammed Mesleh; A Novel Based on Image Blocking Method to Encrypt-Decrypt Color; INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION VOL 3, (2019)
- [28].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.
- [29].J. AL-AZZEH, B. ZAHARAN, 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.
- [30].J. AL-AZZEH, B. ZAHARAN, Z. ALQADI," Salt and Pepper Noise: Effects and Removal", International Journal on Informatics Visualization, Vol.2. No 4, 2018.pp: 252-256.
- [31].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.
- [32].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.
- [33].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.
- [34].Dr. Mohamad Barakat Prof. Ziad Alqadi, Highly Secure Method for Secret Data Transmission, International Journal of Scientific Engineering and Science, vol. 6, issue 1, pp. 49-55, 2022.
- [35].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.

- [36].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.
- [37].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.
- [38].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.