

MESSAGE BITS SUBSTITUTION TO SECURE LSB METHOD**Prof. Ziad Alqadi**Albalqa Applied University
Faculty of Engineering Technology**ABSTRACT**

A secure LSB method of message steganography will be introduced, this method will use a private key of 256 bits length, this length will provide the required key space to protect the hidden message from being hacked, the private key will be used to select the position of the covering-stego bytes and to generate a secret indices key, which will be used for message blocks of bits substitution. The presented method will use simple procedures for key generation, message substitution, message hiding and message extracting. The message binary column matrix will be divided into equal blocks, the block size will be variable and it will be determined by the message sender, blocking will be used to minimize the key generation time especially when the message is very long. The presented method will use a simple chaotic logistic map model to generate the required for message substitution indices key.

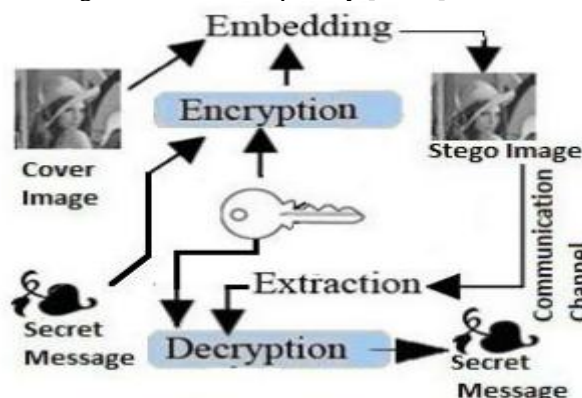
The presented method will be implemented using various covering images and various messages, the obtained results will be analyzed by applying speed, quality and security analysis to show that the presented method will satisfy the requirements of good stego method.

Keywords:

Message steganography, Message column binary matrix, block, substitution, PK, CLMM, IK.

INTRODUCTION

The idea of hiding secret digital data has been used for centuries [1-5], but with the increasing use of digital transmitted files and the development of communication technologies today, the computer has become a part of every aspect of society [6-10]. The rate of data circulation has increased dramatically, as data is transmitted and processed automatically on a large scale. This requires careful storage and transfer of digital data [11-14]. There are many reasons for protecting secret and private digital data, including protecting the economy, avoiding corruption, or ensuring the protection of citizens. It has become necessary to develop new techniques for data hiding [15-18]. Data hiding is a general term for two types of techniques. The first type is used to protect data from observers and attackers, and is called cloaking. The second type is used to justify intellectual property rights or to damage trust, and is called digital encryption. Figure 1 illustrates the block diagram of stego system, and it is important to note that data hiding is divided into different areas [19-21]. A cover media is used to hide any message intended for delivery to a specific person or group of people. In this case, the goal is to prevent that message from being read by any other person. Another major use of data hiding is to protect the copyright of the owner. It is used to confirm the rights of access and privacy [22-27].

*Figure 1: Stego system diagram*

The objective of this paper research is to present a message stego method, which will meet the following [28-33]:

- Providing a stego image with high quality, the quality parameters measured between the covering image and the stego image will satisfy the quality requirements listed in table 1:

Table 1: Stego image quality requirements [34-38]

Quality parameter	Value
Mean square error (MSE)	Low
Peak signal to noise ratio(PSNR)	High
Correlation coefficient(r)	Closed to 1

- Providing an extracted message with excellent quality, the MSE between the source message and the extracted one will be zero, the PSNR will be infinite, while r will be 1.
- Providing a high level of security, the hidden message will be protected by using a private key of 256 bits length [39-42].
- Providing a high speed of message hiding and message extracting, the presented method will minimize both the hiding and extracting times by using a simple bits replacement operation [43-48].
- Simplicity, the presented method will use simple operations for bits replacement and for secret key generation, it will not require any complex operations of logical and arithmetic operations used in other methods of message steganography [49-53].
- Flexibility, the presented method will allow the user to change the PK by changing the block size and the chaotic parameters.

Related works

Classical least significant bit (CLSB) and LSB2 methods are the most popular methods used for message steganography, a lot of methods were based on these methods [1-10], these methods have the following features, and some of them required enhancement, these features include[53-60]:

- LSB method uses the LSBs of the covering bytes to hide the message bits, while LSB2 method uses the two LSBs of the covering bytes to hide the message bits (see figures 2 and 3) [61-70].

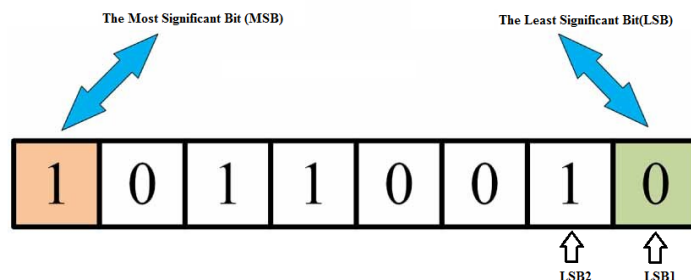


Figure 2: Used LSBs for message hiding

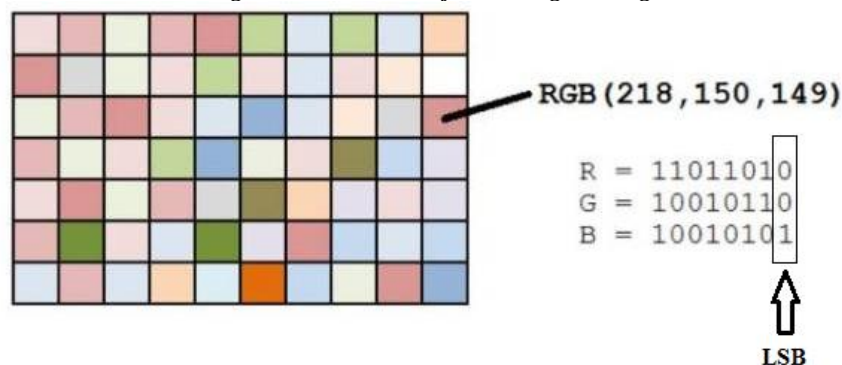


Figure 3: Color pixel LSBs

CLSB and LSB2 methods use consecutive covering bytes to hide the message character (see figures 4 and 5); this will require performing a sequence of logical operations to hide the message character [61-70]. The presented message bit substitution method (MBS_LSB) in this paper will not require

consecutive bytes to hide the message character, it will hide the character in scattered bytes, this can be done by reshaping the message binary matrix into one row matrix, and this matrix will be used to replace the required LSBs of the binary values of the covering bytes. The process of hiding does not require hiding the character in successive bytes, but the task is to implement the hiding process and retrieve the message correctly, this will simplify the process of message bits hiding and extracting.

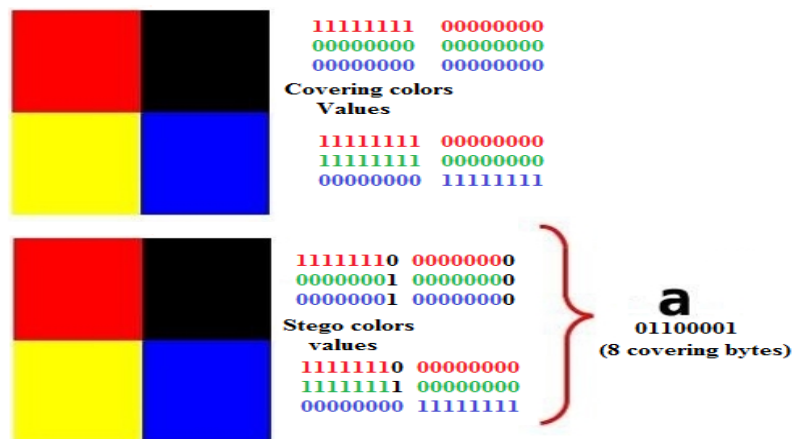


Figure 4: CLSB method hiding process

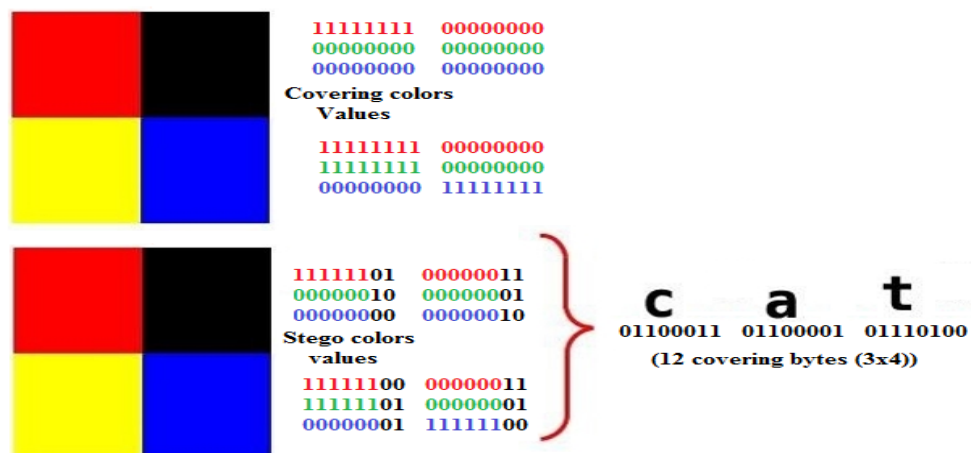


Figure 5: LSB2 method hiding process

- CLSB and LSB2 methods are not secure, knowing that the stego image is holding a message it will be easy to hack the hidden message. The presented MBS_LSB method will use a complicated private key (PK) to protect the hidden message from being hacked.
- CLSB and LSB2 methods are not fast enough, the presented MBS_LSB method will enhance the speed of message steganography, and it will provide a good speed up comparing with CLSB based method.

The presented MBS_LSB method

To protect the hidden message from being hacked the presented MBS_LSB method uses a complicated PK with length equal 256 bits, figure 6 shows a sample used PK:

```
P=100;           %starting position of the covering_stego bytes
NB=3;            %number of blocks
r=3.77;x=0.11;   %chaotic logistic parameters
```

Figure 6: PK example

iJETRM

International Journal of Engineering Technology Research & Management

Published By:

<https://www.ijetrm.com/>

The PK will be used to apply the following tasks:

- Selecting the starting position of the covering-stego bytes.
- Calculating the block size of the message binary column matrix, by dividing the matrix size by the selected value of the number of blocks (NB).
- Generating the secret indices key (IK) by using the chaotic logistic parameters values (r and x) and by running a chaotic logistic map model (CLMM), this model will generate a chaotic logistic data set (CLDS), this set will be sorted to form the required IK.

The values of NB, r and x will be used to generate the CLDS; this task will be simple and figure 7 shows the simple sequence of operations required to generate the IK.

```
P=100;  
NB=3;  
r=3.77;x=0.11;  
for i=1:NB  
    x=x*r*(1-x);  
    CLDS(i)=x;  
end  
[clds IK]=sort(CLDS);
```

Figure 7: IK generation process

The generated IK will be used to substitute the message bits before message hiding in the hiding phase and after message extracting in the extracting phase.

The MBS_LSB method hiding algorithm will be implemented applying the following steps:

Step 1: Get the covering image, get the secret message, and get the PK.

Step 2: Get the image size (S), and get the message length (L).

Step 3: Calculate BS.

Step 4: Run a CLMM to generate IK.

Step 5: Message preparation:

- Convert the message to decimal, and then convert the decimal to binary.
- Reshape the binary matrix of the message to one column matrix as shown in figure 8.
- Use IK to substitute the message column matrix.

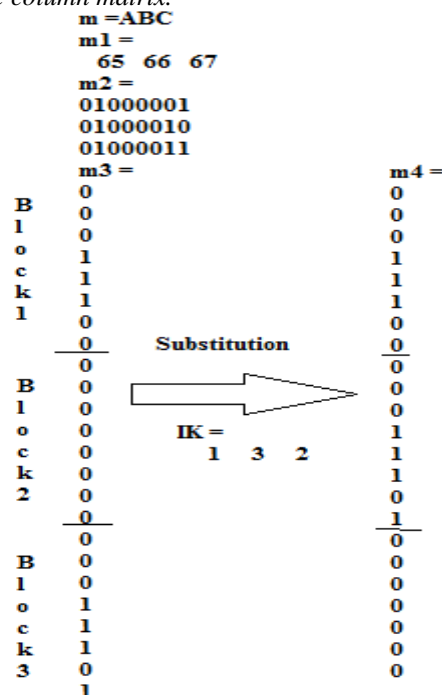


Figure 8: Message preparation

iJETRM

International Journal of Engineering Technology Research & Management

Published By:

<https://www.ijetrm.com/>

Step 6: Message hiding:

- Reshape the covering image matrix to one row matrix.
- Get the covering byte from the position P with length equal $L*8$ when using LSBs.
- Convert the covering bytes to binary (see figure 9).
- Replace all LSBs of the coveringh bytes with message column matrix.
- Convert the obtained covering bytes to decimal.
- Return back the covering bytes to the image row matrix.
- Reshape back the image row matrix to 3D matrix to get the stego image.


```

cb =
200 200 200 200 200 197 197 197 197 197 197 197 197 200 199 199 198 198 197 196 196 197 197 197

cbb =
11001000
11001000
11001000
11001000
11001000
11001001
11001001
11000101
11000101
11000101
11000100
11000100
11000100
11000100
11000101
11000101
11000101
11000101
11000101
11001000
11000111
11000111
11000110
11000110
11000110
11000110
11000101
11000100
11000100
11000100
11000100
11000101
11000101
11000100
11000100

Replacing LSBs with m4

```



```

cbd =
200 200 200 201 201 197 196 196 196 196 196 196 197 197 201 198 199 198 198 196 196 196 196 196 196

```

Figure 9: Replacing LSBs of the covering bytes with message column matrix

Message column binary matrix will be substituted based on the contents of the generated IK, this matrix will be divided into blocks, and the blocks will be rearranged using IK as shown in figure 10:

```

m4=m3;
fori=1:NB
    cc=IK(i);
    m4((i-1)*BS+1:(i-1)*BS+BS)=m3((cc-1)*BS+1:(cc-1)*BS+BS);
end

```

Figure 10: Message one column binary matrix substitution

The MBS_LSB method extracting algorithm will be implemented applying the following steps:

- Step 1: Get the stego image, and get the PK.
- Step 2: Reshape the image matrix to one row matrix.
- Step 3: From the position P get the stego bytes with length equal $L \times 8$.
- Step 3: Convert the stego bytes to binary.
- Step 4: From the binary matrix of the stego bytes get the all LSBs.
- Step 5: Use IK to substitute the obtained one column matrix.
- Step 6: Reshape the resulting matrix to 8 columns matrix to get the message binary matrix.
- Step 7: Convert the message binary matrix to decimal.
- Step 8: Convert the decimal results to characters to get the secret hidden message.

Message column binary matrix will be substituted based on the contents of the generated IK, this matrix will be divided into blocks, and the blocks will be rearranged using IK as shown in figure 11:

```

mm4=mm3;
for i=1:NB
    c=IK(i);
    mm4((c-1)*BS+1:(c-1)*BS+BS)=mm3((i-1)*BS+1:(i-1)*BS+BS);
end

```

*Figure 11: Message one column binary matrix substitution in the extracting phase***MBS_LSB implementation**

The presented MBS_LSB method was implemented using various messages and various covering images, the quality of the stego image was always good, the value of MSE measured between the covering image and the stego image was always low, while the value of PSNR was always high, figures 11 and 12 show how the stego images were closed to the covering images when hiding short and long messages:

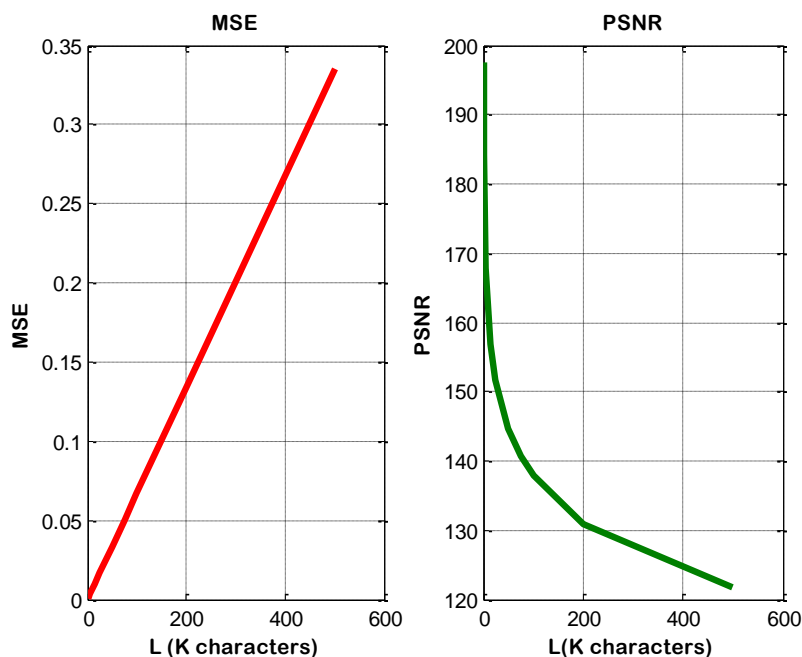
*Figure 11: Stego image holding 100 characters**Figure 11: Stego image holding 4 K characters*

A color image with 6119256 bytes was selected as a covering image and it was used to hold different in sizes messages, the PK shown in figure 12 was used, and table 2 shows the obtained quality parameters:

P=100; NB=150;**r=3.77;x=0.11;****Figure 12: Used PK****Table 2: Obtained quality parameters**

Message size (K bytes)	MSE	PSNR	r
0.25	0.00016947	197.6539	1.000
0.5	0.00032471	191.1510	1.000
1	0.00065596	184.1193	1.000
5	0.0033	167.8320	1.000
15	0.0101	156.7996	1.000
25	0.0168	151.6986	1.000
50	0.0335	144.7941	1.000
75	0.0502	140.7499	1.000
100	0.0669	137.8635	0.999
200	0.1339	130.9326	0.999
500	0.3347	121.7715	0.998

From table 2 it is shown that even if the message was too long the quality of the stego image was good, the value of MSE increased slowly when increasing the message length, while the PSNR value decreased slowly when increasing the message length (see figure 13), the obtained r values point to the fact that the stego image was very close to the covering image.

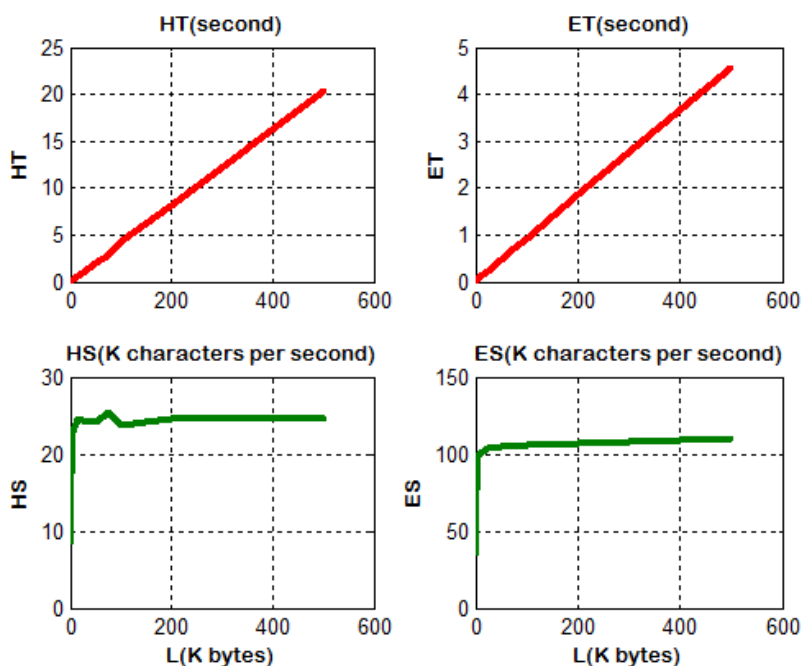
**Figure 13: MSE and PSNR vs message length**

The speed of the presented MBS_LSB method was tested, the previous messages were processed again, the hiding time (HT) and the extracting time (ET) in seconds were calculated, and the hiding speed (HS) and the extracting speed (ES) in K bytes per seconds were also calculated and table 3 shows the obtained speed parameters:

Table 3: Obtained speed parameters

Message length (K characters)	HT(second)	ET(second)	HS(K characters per second)	ES(K characters per second)
0.25	0.0290	0.0070	8.6207	35.7143
0.5	0.0380	0.0080	13.1579	62.5000
1	0.0570	0.0130	17.5439	76.9231
5	0.2180	0.0500	22.9358	100.0000
15	0.6120	0.1470	24.5098	102.0408
25	1.0250	0.2400	24.3902	104.1667
50	2.0730	0.4780	24.1196	104.6025
75	2.9460	0.7180	25.4582	104.4568
100	4.2210	0.9420	23.6911	106.1571
200	8.1370	1.8750	24.5791	106.6667
500	20.3110	4.5480	24.6172	109.9384
Average	3.6061	0.8205	21.2385	92.1060

From table 3 we can see that the presented MBS_LSB method provided a good speed, the hiding speed average was equal 21.2385 K bytes per second, while the extracting speed average was equal 92.1060 K bytes per second, the hiding and extracting times have a linear relationship with the message length, while the speed grew when increasing the message length and it remained stable for long messages as shown in figure 14.

**Figure 14: Speed parameters vs message length**

The presented MBS_LSB speed was compared with other existing methods speed, and table 4 shows the results of comparisons:

Table 4: Methods speed parameters comparisons

Presented MBS_LSB			
L(byte)	750	1000	1500
HT(second)	0.0450	0.0560	0.0780
ET(second)	0.0100	0.0130	0.0170
TT(second)	0.0550	0.0690	0.0950
Average	0.0730		
SSLSB[66-69]			

L(byte)	750	1000	1500
HT(second)	2.044	3.338	9.376
ET(second)	0.073	0.063	0.109
TT(second)	2.1170	3.4010	9.4850
Average	5.0010		
DSLSB[66-69]			
L(byte)	750	1000	1500
HT(second)	0.343	0.592	1.029
ET(second)	0.078	0.062	0.109
TT(second)	0.4210	0.6540	1.1380
Average	0.7377		

From table 4 it is shown that the presented MBS_LSB method enhanced the speed of message steganography and it speed up the process of message steganography comparing with other existing methods as shown in table 5.

Table 5: Speed up of MBS_LSB method

Method	TT	Speed up of SLSB_LSB2 (using LSB version)
SLSB	9.4850	129.9315
DSLSB	1.1380	15.5890
Presented MBS_LSB	0.0730	1.0000
Speed up=other method time divided by proposed method time		

The presented MBS_LSB method provided a high level of security, it protected the hidden message from being hacked, the method used a PK with length equal 256 bits, this length provided a huge key space capable to resist hacking attacks, the key space was calculated using equation 1:

$$\text{Key space} = 2^{256} = 1.1579208923731619542357098500869 \times 10^{77} \text{ Combinations} \quad (1)$$

The extracted message was very sensitive to the selected values of the PK, any minor changes in the PK in the extracting phase was considered as a hacking attempt by extracting a damaged message, and to show this fact the message "Secret message steganography using MBS_LSB method" was hidden in a covering image using the PK shown in figure 15, the hidden message was extracted by applying some changes in the PK, the results shown in table 4 show that the method is very sensitive to the selected values of the PK:

P=100;
NB=5;
r=3.77;x=0.11;

Figure 15: Used PK for sensitivity test

Table 4: Method sensitivity

Changes in the PK	Extracted message
No changes	Secret message steganography using MBS_LSB method
P=101	ecret message steganography using MBS_LSB methnd\$
NB=6	š±»:¶6"» hKRLONDCAQcQJwc]_aiedMiuucyhiAm9-%,
r1=3.66;x1=0.16]J~nG-fnzLt~ LEDNFI\Lt~FIT}en-'D~.=]<\$YH

CONCLUSION

A simple, efficient and secure MBS_LSB method was presented; this method used a simple LSBs replacement operation to apply message bits hiding, the message bits were hidden in shuffled covering bytes. The presented

method used a long PK, this key was used to protect the hidden message, and it was used to select the starting position of the covering-stego bytes and to generate the secret indices keys, which was used to substitute the message bits before message hiding and after message extracting. The presented method used a simple chaotic logistic map model to generate the required secret indices key. The message binary bits were divided into blocks, the block size was variable and it was selected by the user, blocking was used to minimize the substitution time. The PK had a 156 bits length, this length was good enough to provide a key space capable to resist hacking attacks and the extracted message was very sensitive to the selected values of the PK. The presented method was implemented using various images and various messages, the obtained results were analyzed by applying quality, speed and security analysis, and the results of analysis showed that the presented method satisfied the quality speed and security requirements of good stego method, the presented method enhanced the performance of the existing CLSB method.

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.
- [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 . <https://doi.org/10.1109/ICIS.2016.7550955>.
- [7]Wu D-C, Tsai W-H. A steganographic method for images by pixel value differencing. Pattern Recognition. Lett. 24, 1613–1626. 2003 [https://doi.org/10.1016/S0167-8655\(02\)00402-6](https://doi.org/10.1016/S0167-8655(02)00402-6).
- [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. <https://doi.org/10.1109/ICRCICN.2016.7813674>.
- [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, 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, 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.
- [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 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 Emery, 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)

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

[66]Kaur, R. Dhir, & G. Sikka,“A new image steganography based on first component alteration technique”, International Journal of Computer Science and Information Security (IJCSIS), 6, pp.53-56, 2009.<http://arxiv.org/ftp/arxiv/papers/1001/1001.1972.pdf>.

[67] Alvaro Martin, Guillermo Sapiro, &Gadiel Seroussi,“Is Steganography Natural”, IEEE Transactions on Image Processing, 14(12), pp.2040-2050, 2005.doi: 10.1109/TIP.2005.859370 .

[68] Bhattacharyya, A. Roy, P. Roy, & T. Kim, "Receiver compatible data hiding in color image", International Journal of Advanced Science and Technology, 6, pp.15-24, 2009.<http://www.sersc.org/journals/IJAST/vol6/2.pdf> .

[69] Namer Ali Aletawi; Mansour A. Abu Sameha; Prof. Ziad Alqadi, Modified LSB2 Steganography Method to Secure the Embedded Secret Message, IJCSMC, Vol. 11, Issue. 8, August 2022, pg.22 – 44.

[70] Pleacher, D. (n.d.), Calculating password entropy. Retrieved February 16, 2023, from <https://www.pleacher.com/mp/mplessons/algebra/entropy.html>Potter, 8, 2023.