Available Online at www.ijcsmc.com/journal

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. 8, August 2022, pg.9 – 21

Bits Substitution to Secure LSB Method of Data Steganography

Prof. Ziad Alqadi

Albalqa Applied University
Faculty of Engineering Technology
Jordan Amman

DOI: https://doi.org/10.47760/ijcsmc.2022.v11i08.002

Abstract

Least significant bit of data hiding is one of the most popular used methods in data steganography, this method is simple and efficient, but it is not secure.

In this research paper a modified LSB method version will be proposed, this version added a private key as an input of data hiding and data extracting. The private key will contain 8 components which provide a necessary key space to protect the hidden message. The PK key will be used to perform the required substitution and arrangement of the binary version of the secret message.

The proposed method will be tested for quality and performance to prove that the proposed method keeps the performance of the LSB method without changes. Several images will be used as a covering images and a recommendation will be suggested to keep the method efficient.

Keywords: Steganography, covering image, stego image, secret message, PK, substitution, MSE, PSNR.

Introduction

Steganography is the art of hiding information among other less visible information to prevent eavesdropping by concealing its existence in the first place[1-11]. This research focuses on investigating enhanced LSB method of hiding information during modern digital communication. Initially, the focus will be on achieving steganography as a whole, before applying steganography to text information [15-21]. This specific field was chosen because of limited research in this area, and the text is ubiquitous in documents, open source and the Internet. The research will include the strengths and weaknesses of LSB method and suggest solutions and alternative means. In order to complete this extensive research from conference proceedings and journals related to steganography was investigated to identify the basic techniques that could be applied. The importance of this information lies in

presenting a single document that brings together basic methods that can be applied on the basis of current research. In this research paper, the steganography method was used to build a system that hides text information inside the image, and the application creates a (stego image) that contains the text and confidential data and is password-protected for more security [22-30]. The main objective of the research is to design an application to hide information that provides good security strength. It provides a higher degree of security that enables the protection of the image (stego) that contains the message from attacks by people who are not authorized to view confidential information. The accuracy and clarity of the image will not change much when the message is included in an image using LSB method, a substitution sequence will be used to create a PK key, this will provide the LSB method with the required security to protect the embedded secrete message [30-41].

Data steganography as shown in figure 1 is the process of hiding secret data into another data. Big size color image is usually used as a covering media. One of the most popular methods of data steganography is LSB method [12-18]. This method uses 8 bytes from the covering image to hide one character of the secret message. The binary version of the character is to be inserted in the LSBs of the set of 8 bytes of the covering image as shown in figure 2.

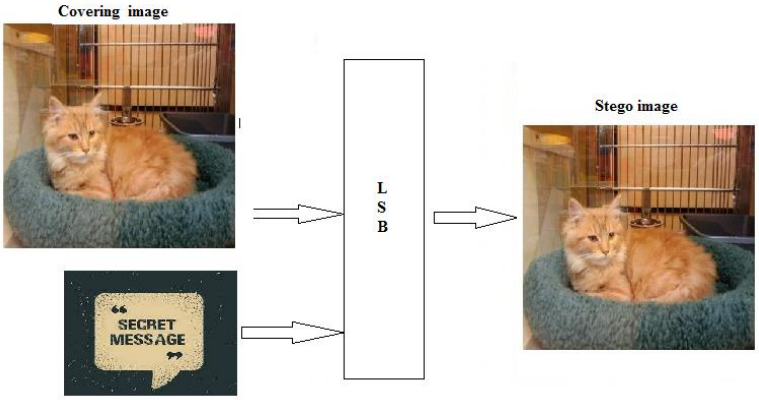

Figure 1: Data steganography process

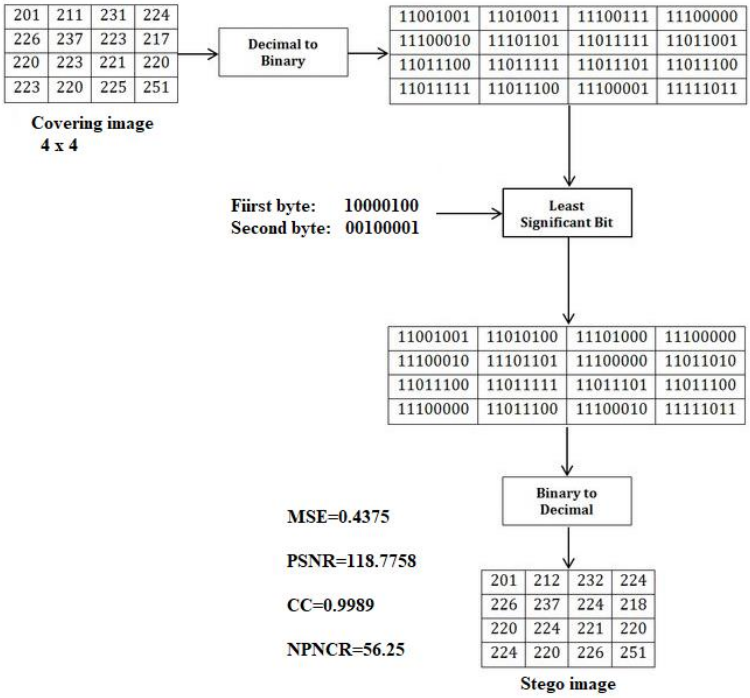

Figure 2: LSB operations

LSB method of data steganography is a simple method of data hiding and extracting, and it has the following features [19-30]:

- The pixel in the carrier image is slightly affected by the process of hiding the secret message, as the pixel value changes within the range -1 and +1 (see table 1), which is a very small value that cannot be noticed with the naked eye, and by this the MSE between the carrier and stego images will be small, while the PSNR and CC between them will be high [31-40].

Table 1: Effects of bit hiding

Message bit	Carrier bit	Stego bit	Changes
0	0	0	No change
0	1	0	Subtract 1
1	0	1	Add 1
1	1	1	No change

- The capacity of LSB method equal the carrier image size divided by 8.
- LSB method is not secure, the message can be easily extracted of the hacker has a good programming experience [25-32].

The objectives of the proposed method are to protect the hidden message from being hacked by a adding a security issues to LSB method. A PK must be used, this key will contain information about the substitution sequence of data hiding and extracting process.

The Proposed Method

The proposed method is based on LSB method of data steganography; it uses a PK to secure the hidden message.
The message binary matrix for LSB method as shown in figure 3 is a 2D matrix (one column for each character and 8 rows (8 bits for the character binary number)), this matrix must be transposed to get a new 2D matrix (8 columns for the binary numbers and one row for each character).

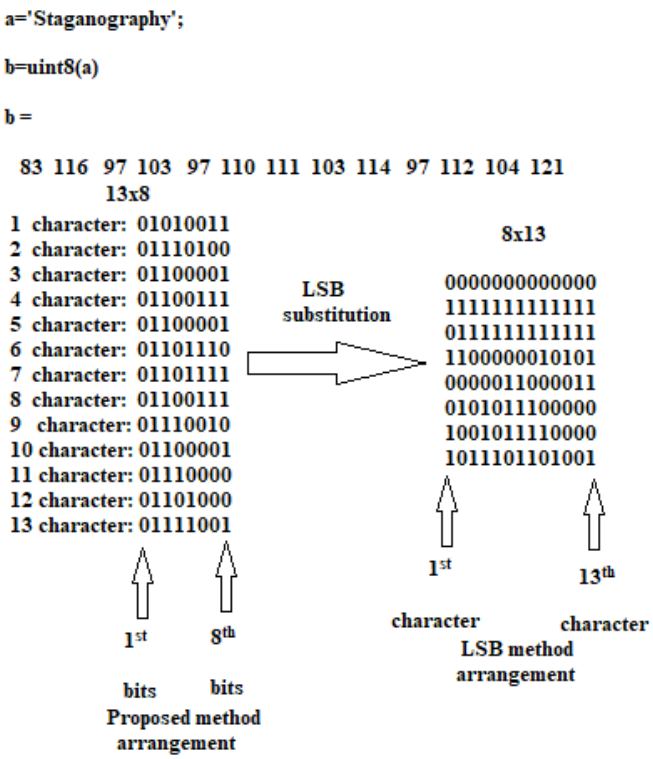

Figure 3: Message bits' arrangement

The proposed method will use a transpose binary matrix to apply message hiding and extracting as shown in figure 4, the matrix must be reshaped to one column matrix, this column matrix will replace the LSB in the covering image binary matrix. The order of the column in the message binary matrix must be determine by the continents of the PK as shown in figure 5.

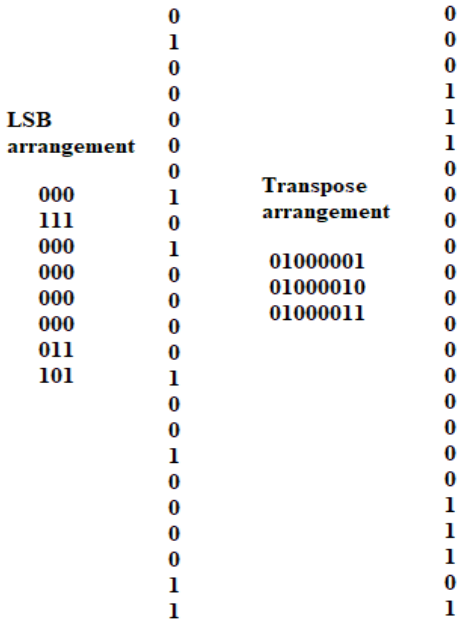

Figure 4: Using the transpose message binary matrix

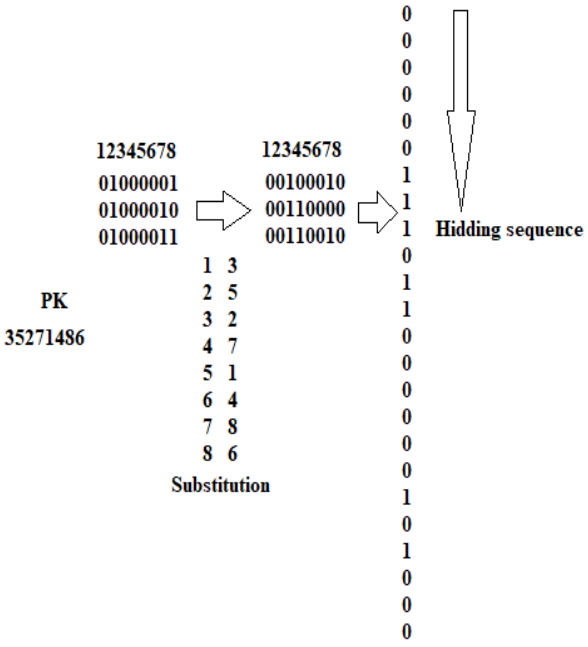

Figure 5: Using PK for column substitution

According to the results of substitution the resulting binary matrix is to be reshaped to 1 column matrix, and the column will define the sequence of the hidden bits as shown in figure 6

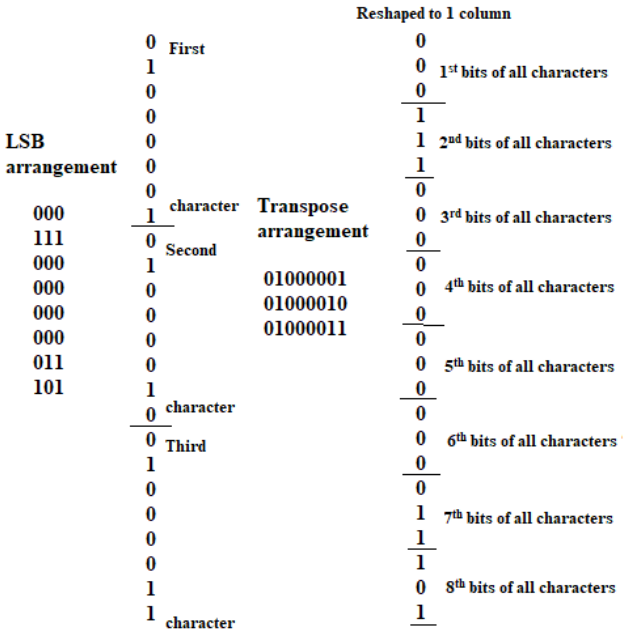

Figure 6: Hiding bits' sequence

The PK contains 8 components, each of them varies from 1 to 8, so the key will provide a number of combinations equal to 8^8=16,777,216, and tis key space will be sufficient to protect the hidden secret message.

The proposed method data hiding phase can be implemented applying the following algorithm:

Inputs

Message, covering image, PK

Output

Stego image

Process

1- *Get the message*

2- *Get the message length (L)*

3- *Change the message to decimal*

4- *Change the decimal message to binary*

5- *Get the transpose message binary matrix*

6- *Get the PK*

7- *Rearrange the transpose matrix based on the PK contents*

8- *Reshape the transpose matrix to one column array*

9- *Reshape the covering image into one column array*

10- *Convert the image array into binary*

11- *Let the LSB of the first L*8 equal message array*

12- *Convert the image array back to decimal*

13- *Reshape the image column to 3D matrix*

The following code can be used to apply message hiding:

```
in=imread('C:\Users\Dr.Tayseer\Desktop\drziad\MAVAV\a12.jpg');
[n1 n2 n3]=size(in);ss=n1*n2*n3;
m='Ziad Alqadi Albalqa Amman Jordan Steganography';
L=length(m);
a=reshape(in,[1,n1*n2*n3]);
tic
m1=uint8(m);
m22=dec2bin(m1,8);
m2(:,1)=m22(:,3);
m2(:,2)=m22(:,5);
m2(:,3)=m22(:,2);
m2(:,4)=m22(:,7);
m2(:,5)=m22(:,1);
m2(:,6)=m22(:,4);
m2(:,7)=m22(:,8);
m2(:,8)=m22(:,6);
a1=a(1,1:L*8);
a2=dec2bin(a1,8);
m3=reshape(m2,[L*8,1]);
a2(:,8)=m3;
a3=bin2dec(a2)';
a(1,1:L*8)=a3;
a4=reshape(a,[n1 n2 n3]);
ht=toc;
```

The extracting phase can be implemented applying the following algorithm:

Input

Stego image, PK

Output

Secret message

Process

1- *Get the stego image*

2- *Get the image size*

3- *Reshape the image into one row*

4- *Get the message length (L)*

5- *From the image extract a part with length equal L*8*

6- *Convert the image part to binary*

7- *From the binary image select column 8*

8- *Reshape the obtained column to transpose matrix*

9- *Get the PK*

10- *Rearrange the matrix according to the PK contents*

11- *Convert the matrix to decimal to get the ASCII characters*

12- *Convert the decimal message to character*

The following code can be used to apply message extracting:

```
%Extracting
tic
a5=reshape(a4,[1,n1*n2*n3]);
a6=a5(1,1:L*8);
a7=dec2bin(a6,8);
m45=a7(:,8);
m44=reshape(m45,[L 8]);
m4(:,1)=m44(:,5);
m4(:,2)=m44(:,3);
m4(:,3)=m44(:,1);
m4(:,4)=m44(:,6);
m4(:,5)=m44(:,2);
m4(:,6)=m44(:,8);
m4(:,7)=m44(:,4);
m4(:,8)=m44(:,7);
m5=reshape(m4,[L,8]);
m6=bin2dec(m5)';
m7=char(m6)
et=toc;
```

Implementation and Experimental Results

The proposed method was implemented using various in lengths messages and various in sizes carrying color images. The main objective of the hiding process it to get a stego image which is very closed to the covering image, the changes must not be noticed by human eyes, here we can visually check the differences between the covering and the stego images, figures 7 and 8 show a sample outputs of hiding a 5000 characters' message in a color image with size equal 6119256 bytes.

Using images with smaller sizes will negatively affect the quality of the stego image, figures 9 and 10 show the sample outputs of hiding the same message in a covering image with size equal 150975 bytes

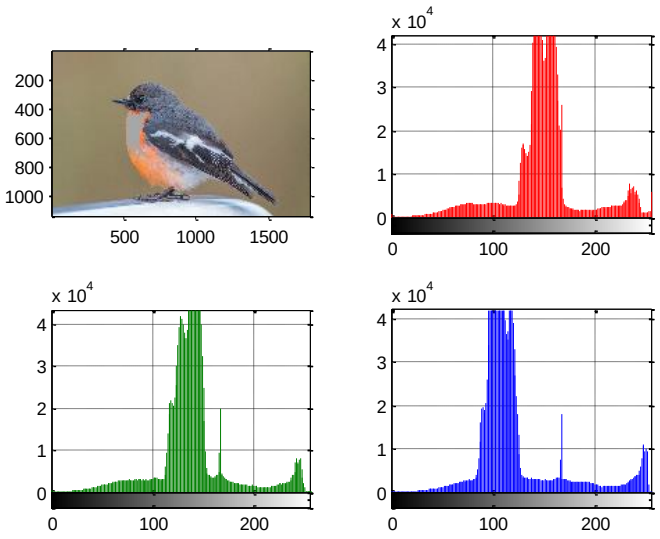

Figure 7: Covering image with size = 6119256 bytes

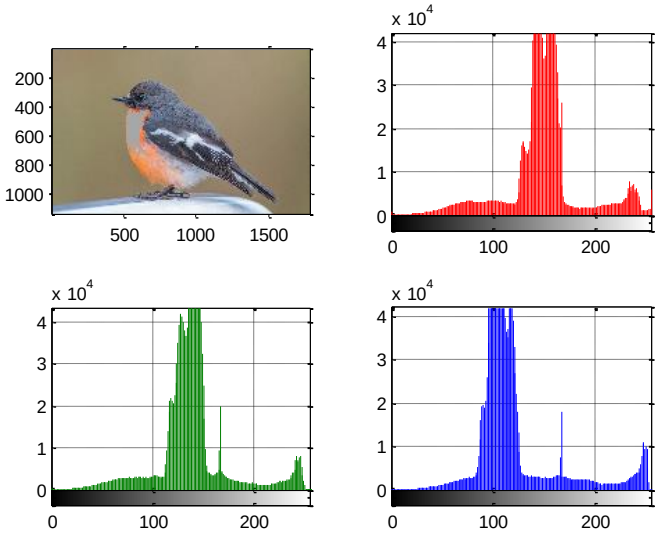

Figure 8: Big stego image

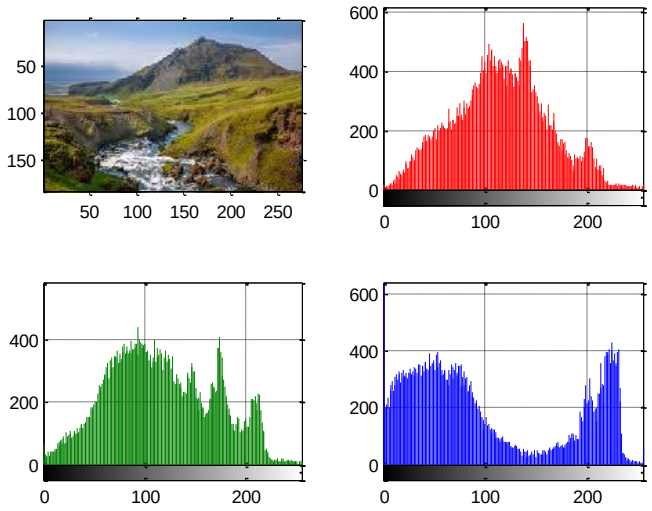

Figure 9: Covering image with size = 150975 bytes

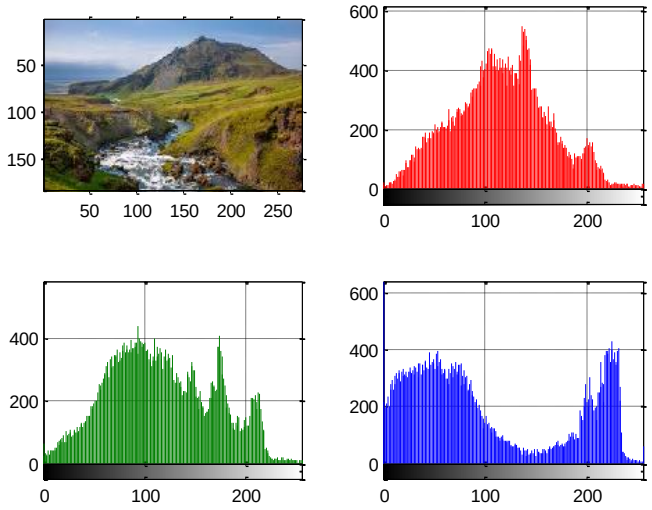

Figure 10: Smaller stego image

The quality of the stego image can be measured by MSE, PSNR, CC and NSCR.

The quality of the stego image must be very high, so MSE must be very low and PSNR must be very high

MSE and PSNR can be calculated using equations 1 and 2:

$$PSNR = 10 \log_{10} \frac{MAX^2}{MSE} \text{dB}, \quad \textbf{(1)}$$

$$MSE = \frac{1}{N}\sum_{i=1}^{N}(x_i - y_i)^2, \quad \textbf{(2)}$$

Where: MAX is the maximum possible value of the color matrix (In our case the maximum value is 255), *N* is the total number of samples (pixels), xi and yi are the corresponding sample values of the plain and encrypted files.

If we select a covering image with big size we can maximize the quality of the stego image by decreasing MSE and increasing PSNR, Using the big image shown in figure 7 as a covering image we can obtain MSE with value 0.0033 and PSNR with value equal 167.9678 (using a message with length=5000 characters).

The proposed method is very efficient, table 2 shows the averages of the performance parameters:

Table 2: Performance results

Parameter	Value
Hiding time (second)	0.1703
Extracting time (second)	0.0424
Hiding throughput(K bytes per second)	28.6773
Extracting throughput(K bytes per second)	115.1827

Conclusion

A simple and efficient modification of LSB method of data steganography was proposed. The modified LSB method protects the hiding secret message by using a PK which provided a suitable key space to increase the security level of the LSB method. The quality of the stego images was examined and it was shown that the proposed method gave an excellent quality, the quality can be enhanced when using a bigger in size covering image, and this will not negatively affect the performance of the proposed method.

The proposed method is very flexible, it can use any type of images as a covering image (color or gray images), the selected type of image does not require any modification in the method algorithm, also the PK can be easily change without changing the algorithm.

The proposed method was very efficient even if we use big images or big messages, the obtained throughputs for data hiding and extracting were acceptable.

References

[1] Afjal H. Sarower; Rashed Karim; Maruf Hassan, An Image Steganography Algorithm using LSB Replacement through XOR Substitution, Computer Science:2019 International Conference on Information and Communications Technology (ICOIACT), DOI:10.1109/icoiact46704.2019.8938486.

[2] Maya Abood, An efficient image cryptography using hash-LSB steganography with RC4 and pixel shuffling encryption algorithms, Computer Science, Mathematics 2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT) 2017.

[3] Saher Manaseer, Asmaa Aljawawdeh and Dua Alsoudi, A New Image Steganography Depending On Reference & LSB, International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 9 (2017) pp. 1950-1955.

[4] 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).

[5] Kaur, G., &Kochhar, A. A steganography implementation based on LSB & DCT. International Journal for Science and Emerging Technologies with Latest Trends, 4(1), pp.35-41, (2012).

[6] Thenmozhi, M. J., &Menakadevi, T. A New Secure Image Steganography Using Lsb And Spiht Based Compression Method. International Journal of Engineering, 16(17), (2016).

[7] Shabnam, S., &Hemachandran, K. LSB based Steganography using Bit masking method on RGB planes. (IJCSIT) International Journal of Computer Science and Information Technologies, 7 (3) , pp.1169- 1173, (2016) .

[8] Datta, B. , Mukherjee, U. , &Bandyopadhyay, S. LSB Layer Independent Robust Steganography using Binary Addition. International Conference on Computational Modeling and Security (CMS 2016), Elsevier Pub, (2016).

[9] Pandit, A. S., Khope, S. R., & Student, F. Review on Image Steganography. International Journal of Engineering Science, 6115, (2016).

[10] Artz, D. Digital steganography: hiding data within data. IEEE Internet computing, 5(3), 75-80, (2001).

[11] Al-Shatnawi, A. M. A new method in image steganography with improved image quality. Applied Mathematical Sciences, 6(79), 3907-3915, (2012).

[12] Gupta, S., Goyal, A., &Bhushan, B. Information hiding using least significant bit steganography and cryptography. International Journal of Modern Education and Computer Science, 4(6), pp.27, (2012).

[13] Mandal, J. K., & Das, D. Color image steganography based on pixel value differencing in spatial domain. International journal of information sciences and techniques, 2(4), (2012).

[14] Rashad J. Rasras1, Mutaz Rasmi Abu Sara2, Ziad A. AlQadi3, 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 ,2019, https://doi.org/10.30534/ijatcse/2019/64832019

[15] Ziad A. Alqadi, Majed O. Al-Dwairi, Amjad A. Abu Jazar and Rushdi Abu Zneit, 2010, Optimized True-RGB color Image Processing, World Applied Sciences Journal8 (10): 1175-1182, ISSN 1818-4952.

[16] Waheeb, A. and Ziad AlQadi, 2009. Gray image reconstruction, Eur. J. Sci. Res., 27: 167-173.

[17] Akram A. Moustafa and Ziad A. Alqadi, Color Image Reconstruction Using A New R'G'I Model, Journal of Computer Science 5 (4): 250-254, 2009 ISSN 1549-3636.https://doi.org/10.3844/jcs.2009.250.254

[18] Musbah J. Aqel, Ziad ALQadi, Ammar Ahmed Abdullah, RGB Color Image Encryption-Decryption Using Image Segmentation and Matrix Multiplication, International Journal of Engineering & Technology, 7(3.13) (2018) 104-107.https://doi.org/10.14419/ijet.v7i3.13.16334

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

[20] Khaled Matrouk, Abdullah Al- Hasanat, HaithamAlasha'ary, Ziad Al-Qadi, Hasan Al-Shalabi, Analysis of Matrix Multiplication Computational Methods, European Journal of Scientific Research, ISSN 1450-216X / 1450-202X Vol.121 No.3, 2014, pp.258-266.

[21] Ziad A.A. Alqadi, Musbah Aqel, and Ibrahiem M. M. ElEmary, Performance Analysis and Evaluation ofParallel Matrix Multiplication Algorithms, World Applied Sciences Journal 5 (2): 211-214, 2008.

[22] Z Alqadi, A Abu-Jazzar, Analysis of program methods used in optimizing matrix multiplication, Journal of Engineering, 2005.

[23] Musbah J. Aqel , Ziad A. Alqadi, Ibraheim M. El Emary, Analysis of Stream Cipher Security Algorithm, Journal of Information and Computing Science Vol. 2,No. 4, 2007, pp. 288-298.

[24] 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.

[25] 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.

[26] 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.

[27] 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

[28] 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

[29] 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.

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

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

[32] 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.

[33] M. Abu-Faraj, and Z. Alqadi, "Image Encryption using Variable Length Blocks and Variable Length Private Key," International Journal of Computer Science and Mobile Computing (IJCSMC), vol. 11, Iss. 3, pp. 138-151, 2022.

[34] M. Abu-Faraj, A. Al-Hyari, and Z. Alqadi, "A Dual Approach for Audio Cryptography," Journal of Southwest Jiaotong University, vol. 57, no. 1, pp. 24-33, 2022.

[35] 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.

[36] M. Abu-Faraj, K. Aldebei, and Z. Alqadi, "Simple, Efficient, Highly Secure, and Multiple Pur- posed Method on Data Cryptography," Traitement du Signal, vol. 39, no. 1, pp. 173-178, 2022.

[37] M. Abu-Faraj, Khaled Aldebe, and Z. Alqadi, "Deep Machine Learning to Enhance ANN Performance: Fingerprint Classifier Case Study," Journal of Southwest Jiaotong University, vol. 56, no. 6 , pp. 685-694, 2021.

[38] M. Abu-Faraj, Z. Alqadi, and K. Aldebei, "Comparative Analysis of Fingerprint Features Ex- Traction Methods," Journal of Hunan University Natural Sciences, vol. 48, iss. 12, pp. 177-182, 2021.

[39] M. Abu-Faraj, and Z. Alqadi, "Improving the Efficiency and Scalability of Standard Meth- ods for Data Cryptography," International Journal of Computer Science and Network Security (IJCSNS), vol. 21, no.12, pp. 451-458, 2021.

[40] Dr. Amjad Hindi, Dr. Majed Omar Dwairi, Prof. Ziad Alqadi, Analysis of Procedures used to build an Optimal Fingerprint Recognition System, International Journal of Computer Science and Mobile Computing, vol. 9, issue 2, pp. 21 – 37, 2020.

[41] Aws AlQaisi, Mokhled Tarawneh, Ziad A. Alqadi, Ahmad A. Sharadqah, Analysis of Color Image Features Extraction using Texture Methods, TELKOMNIKA, vol. 17, issue 3, pp. 1220-1225, 2019.

