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. 1, January 2022, pg.182 – 193

Carrier Image Rearrangement to Enhance the Security Level of LSB Method of Data Steganography

Prof. Mohamad K. Abu Zalata; Dr. Mohamad T. Barakat; Prof. Ziad A. Alqadi
Albalqa Applied University**,** Faculty of Engineering Technology**,** Jordan, Amman
DOI: 10.47760/ijcsmc.2022.v11i01.024

Abstract: Least significant bit method is one of the most popular methods of data steganography, this method is very simple and provides good values for MSE and PSNR. LSB method is not secure enough and the embedded secret message can be easily hacked by any person with any programming experience. To enhance the security level of LSB and to protect the secret message from being hacked and addition stage is recommended. This stage adds a necessary protection without affecting the quality parameters and the efficiency of LSB. The protection process is based on using a complex private key, this key is generated by sender depending on the block size and the selected image size and kept in secret to be used by the receiver, the private key can be changed or updated any time, when the needs arise.
Keywords: Steganography, LSB, PK, MSE, PSNR, rearrangement.

1- Introduction

Color digital images are one of the most widespread and widely used types of digital data in many vital applications. This is due to many reasons, the most important of which are [1-5]:

- ✓ Availability of the necessary equipment and supplies to obtain them at no significant cost.
- ✓ Large size, which provides a large environment for data processing.
- ✓ Ease of processing, because it is represented by a three-dimensional matrix that is easy to process and in multiple ways (see figure 1).
- ✓ The possibility of dealing with the matrix of each color separately and the possibility of replacing the colors and rearranging them in a specific way by dividing the image into blocks and re-mixing these blocks (see figure 2) [6-11].

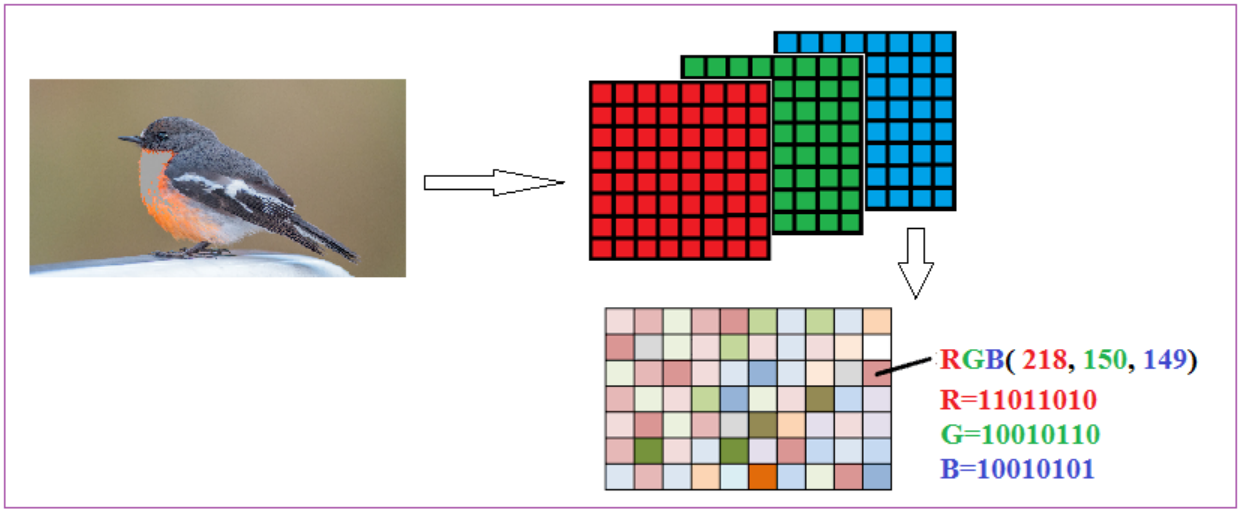

Figure 1: Color image representation

Figure 2: Color image rearrangement

- ✓ The color values in the digital image range between 0 and 255 and these values are identical to the ASCII values that represent the symbols in text messages, which facilitate the processing of text messages using color digital images (see figures 3 and 4) [15-20].

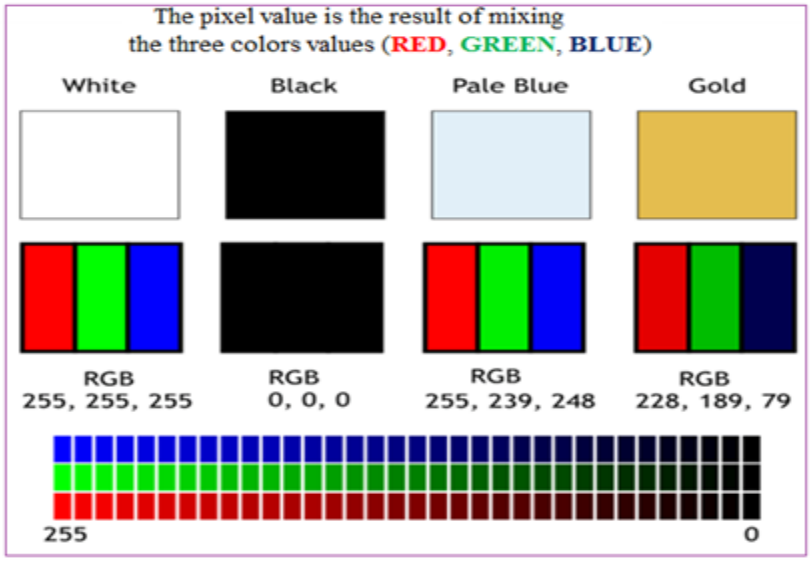

Figure 3: Color pixels' values

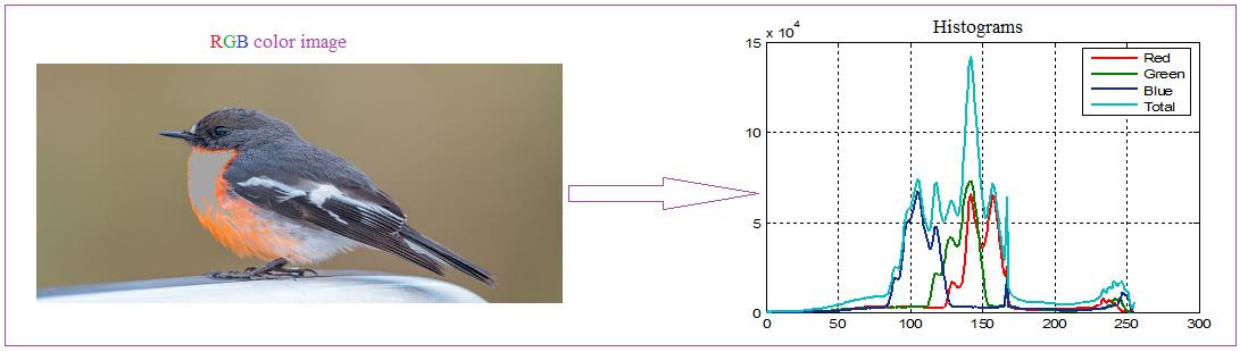

Figure 4: Image and histograms

Color digital images are used in many vital applications, the most important of which is to hide secret text messages, which is known as data steganography[33-38]. Data steganography as shown in figure 5 means hiding secret and private data in a covering color image to produce a stego_image using a selected method of data steganography [21-27].

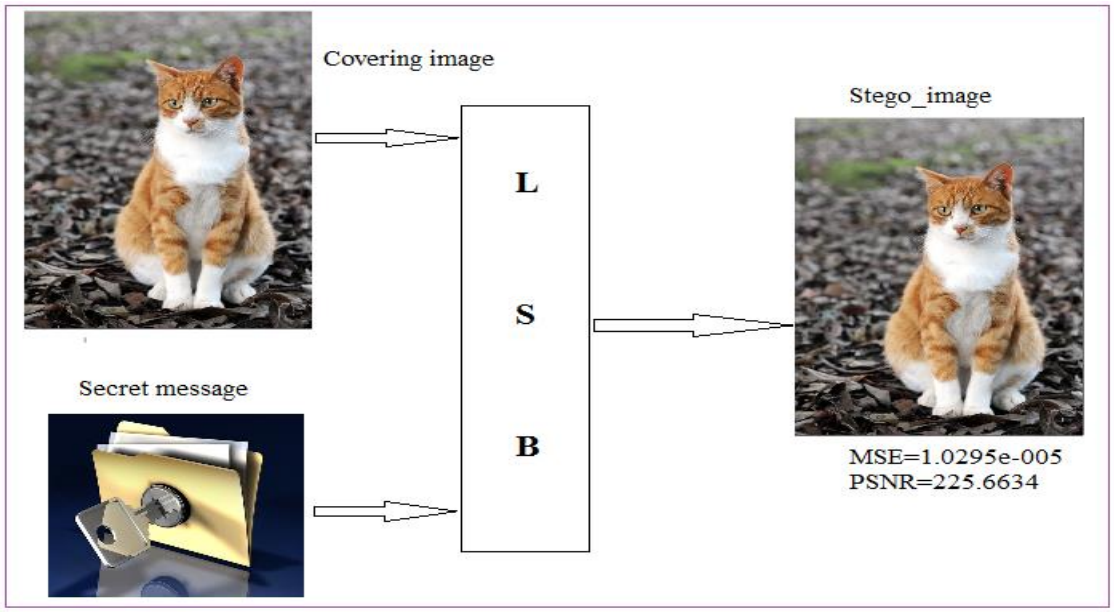

Figure 5: Data steganography process

The process of hiding confidential data in the image should not affect it by making modifications that can be observed with the naked eye, the changes can be measured by the quality parameters MSE (mean square error) and/or PSNR (peak signal to noise ratio), these parameters can be calculated using equations 1 and 2, a good method of data steganography must provide a small value for MSE and a big value of PSNR, this means that a minor change were made after hiding the secret message [28-32].

MSE of x channel

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

Total MSE

$$MSE_t = MSE_R + MSE_G + MSE_B$$

Calculate PSNR

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

2- Related Works

Multiple methods are used to hide messages and confidential data in color digital images, and many of these methods are based on the least significant bit (LSB) method. The LSB method has good advantages that have led to its widespread, including [12], [13], [14]:

- ✓ Ease of programming and implementation.
- ✓ Great hiding ability, where a text message can be hidden in a color image with a size equal to the size of the image divided by eight, because eight bytes of the image are allocated for each byte of the text message.
- ✓ High efficiency because it takes a little time to hide data and a little time to retrieve data from the digital image.
- ✓ A high quality factor for the digital image carrying the text message, where the amount of change in a byte in the stego_image ranges between negative one and positive one (here the MSE between the source image and the stego_image always very small, while the PSNR value very high).

Despite the advantages of the LSB method, it is not secure and does not provide the necessary protection for secret messages hidden in the digital image, as it is easy to penetrate by people with software experience, which leads us to the need to provide the necessary protection for this method.

LSB method can be implemented applying the following steps:

- Convert the holding image and the secret message to binary.
- For each byte of the secret message reserve 8 bytes from the holding image.
- Use least significant bits of the holding bytes to insert the byte of the message as shown in the example illustrated in figure 6.
- Convert back the holding image to decimal to produce the stego_image.

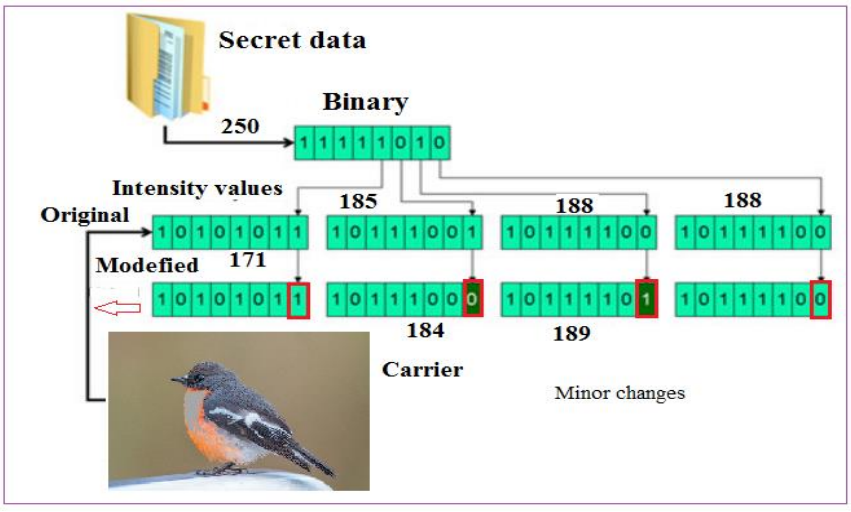

Figure 6: LSB example

3- The Proposed Method

The proposed method is based on LSB data steganography by using a special private (PK), this PK can be created depending on the process of dividing the holding color image into blocks and rearranging these blocks to produce a rearranged holding image. The holding image is to be divided into equal blocks, the number of blocks and the block size is determined by the message sender. The process of rearrangement must be saved to be used as a PK as shown in figure 7 (number of blocks=10):

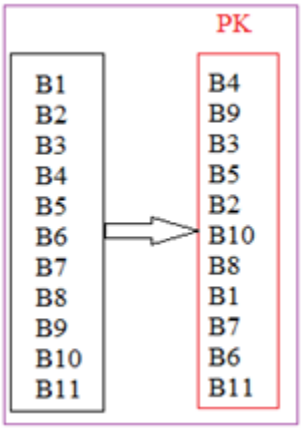

Figure 7: Example of generating PK

The proposed method of data hiding can be implemented as shown in figure 8 applying the following steps:

- Get the carrier image.
- Determine the number of blocks.
- Divide the carrier image into equal blocks (except the last block).
- Rearrange the blocks using a selected sequence to get the holding rearranged image.
- Apply LSB method.
- Rearrange back the image to get the stego_image.

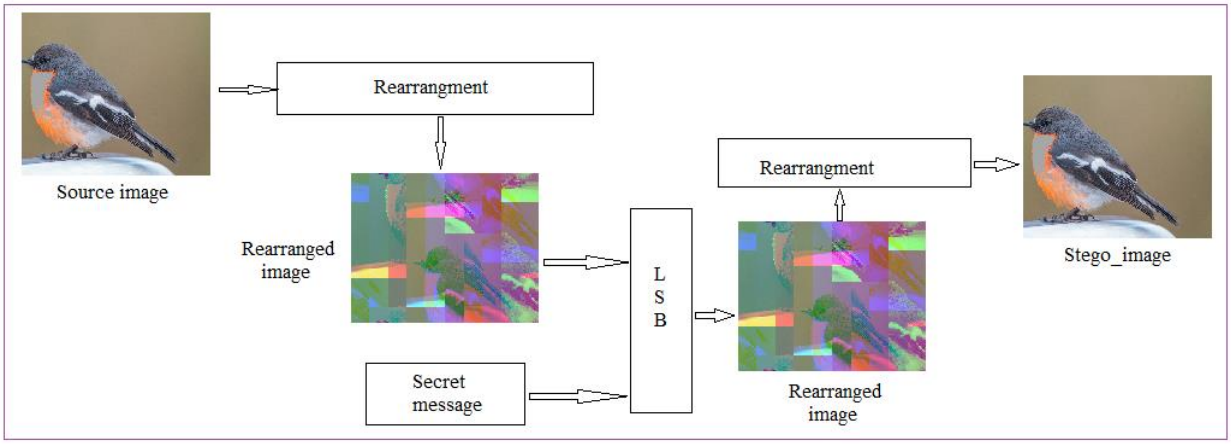

Figure 8: Proposed method hiding process

The process of data extracting can be implemented as shown in figure 9 applying the following steps:

- Get the stego_image.
- Get the PK.
- Rearrange the stego_image using PK.
- Apply LSB data extraction to get the secret message.

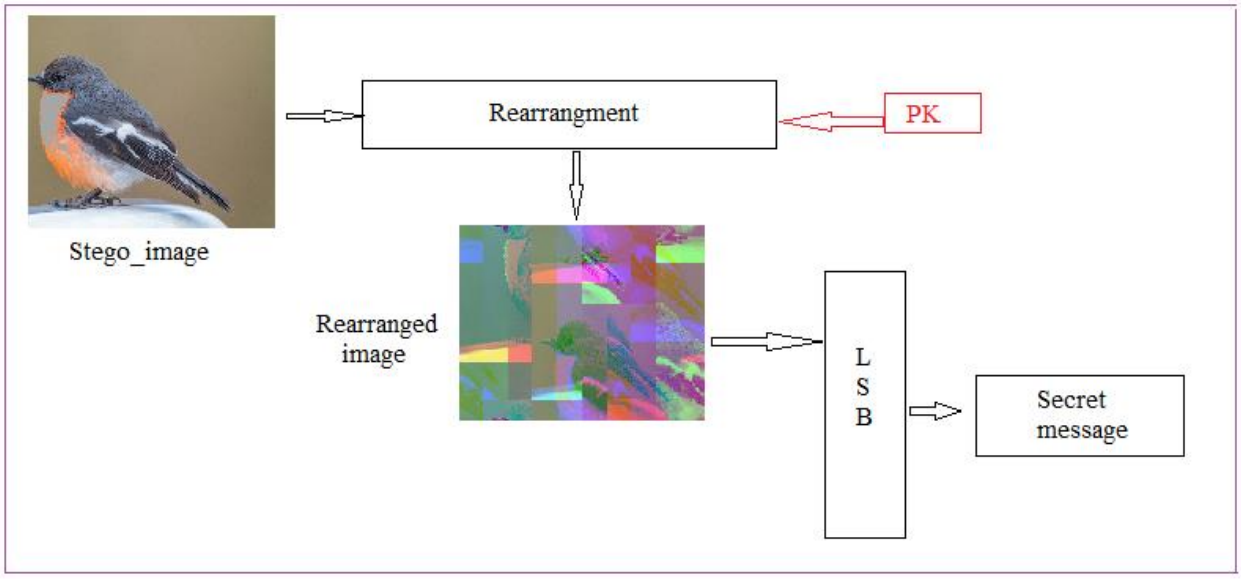

Figure 9: Message extraction process

4- Implementation and Experimental Results

The proposed method was implemented using various images and secret messages, the PK shown in figure 10 was used:

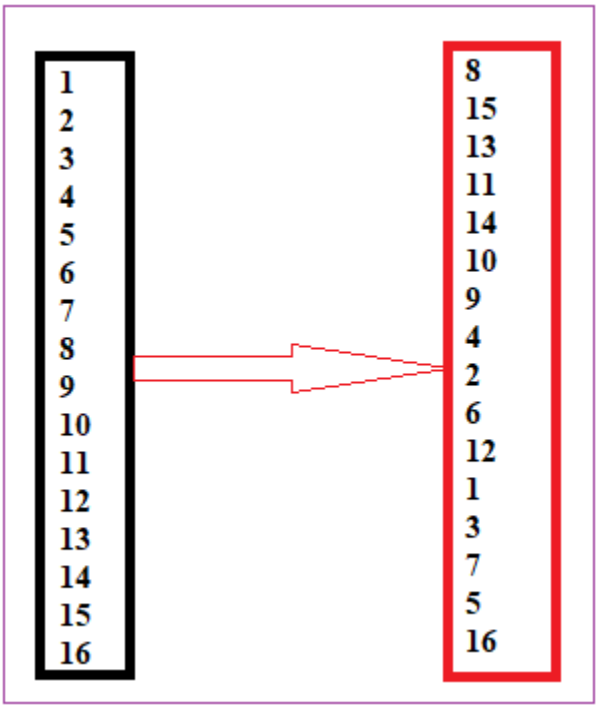

Figure 10: Example of used PK

Figures 11, 12 and 13 show an outputs results of hiding selected message in a covering image.

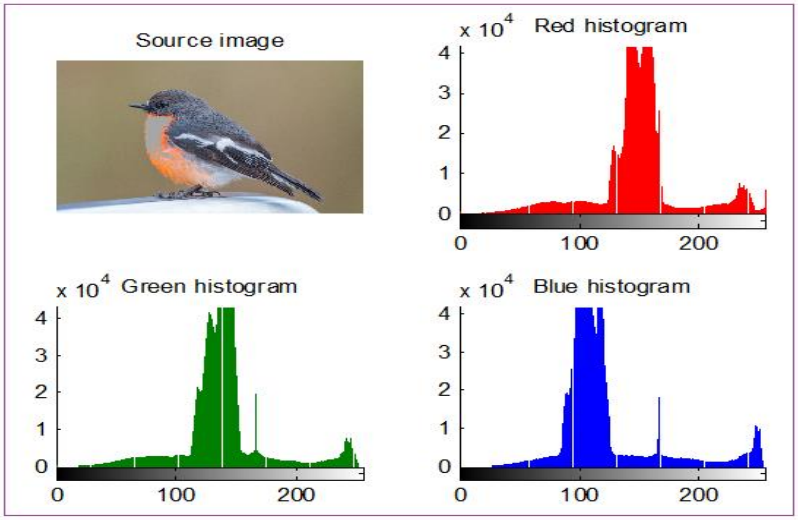

Figure 11: Covering image example

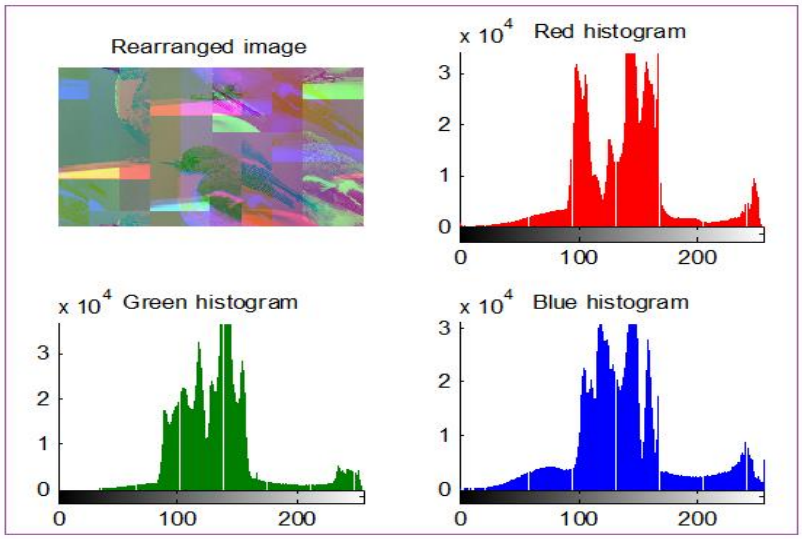

Figure 12: Rearranged image example

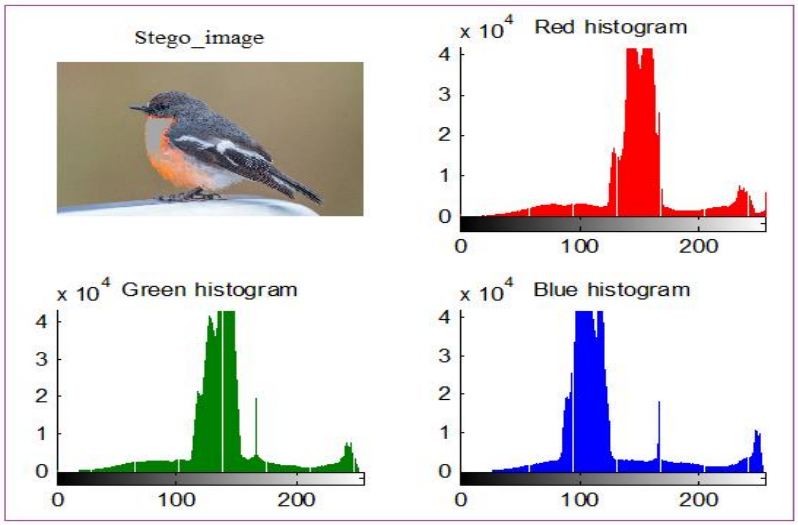

Figure 13: Stego_image example

A message of 20-characters length was treated by the proposed method using various covering images, table 1 shows the obtained experimental results:

Table 1: Hiding 20 characters' message

Image #	Size (byte)	MSE	PSNR	Ordering time (2*t)	Hiding time	Total time
1	150849	4.6360e-004	187.5807	0.0011	0.0302	0.0322
2	77976	8.9771e-004	180.9819	7.8240e-004	0.0175	0.0183
3	518400	1.3503e-004	199.9253	0.0020	0.0903	0.0923
4	5140800	1.3617e-005	222.8675	0.0293	0.8792	0.9303
5	4326210	1.6180e-005	221.1423	0.0460	0.7747	0.8208
6	122265	5.7253e-004	185.4798	0.0008	0.0244	0.0252
7	518400	1.3503e-004	199.9253	0.0020	0.0961	0.0981
8	150975	4.6365e-004	187.5890	0.0011	0.0297	0.0308
9	150975	4.6365e-004	187.5890	0.0013	0.0354	0.0367
10	151353	4.6249e-004	187.6140	0.0009	0.0300	0.0309
11	1890000	3.7037e-005	212.8612	0.0089	0.3185	0.3274
12	6119256	1.1439e-005	224.6098	0.0673	1.0182	1.0855

Short messages were hidden in image 12 (big size image), table 2 shows the obtained experimental results:

Table 2: Short messages hiding using image 12 as a covering image

Message length(byte)	MSE	PSNR	Hiding time
10	6.5367e-006	230.2060	1.0364
20	1.3891e-005	222.6683	1.0379
30	1.9774e-005	219.1369	1.0386
40	2.5493e-005	216.5962	1.0475
50	3.2357e-005	214.2121	1.0538
60	4.0691e-005	211.9203	1.0694
70	4.6411e-005	210.6050	1.0716
80	5.0006e-005	209.8589	1.0767
90	5.6870e-005	208.5728	1.0769
100	6.8309e-005	206.7400	1.0951
120	7.5173e-005	205.7825	1.1303

The same messages were hidden in image 2 (small size image), table 3 shows the obtained experimental results:

Table 3: Short messages hiding using image 2 as a covering image

Message length(byte)	MSE	PSNR	Hiding time
10	5.3863e-004	186.0901	0.0178
20	0.0011	179.1587	0.0178
30	0.0016	175.5089	0.0181
40	0.0020	172.7778	0.0185
50	0.0024	170.9441	0.0188
60	0.0029	169.1734	0.0190
70	0.0038	166.4290	0.0191
80	0.0042	165.5367	0.0192
90	0.0047	164.4132	0.0193
100	0.0052	163.4033	0.0193
120	0.0061	161.8970	0.0195

Long messages were hidden in image 12 (big size image), table 4 shows the obtained experimental results:

Table 4: Long messages hiding using image 12 as a covering image

Message length(K byte)	MSE	PSNR	Hiding time
1	6.7426e-004	183.8441	1.1116
10	0.0067	160.8996	1.1279
20	0.0134	153.9482	1.1282
30	0.0201	149.8930	1.1286
40	0.0268	147.0120	1.1577
50	0.0335	144.7873	1.1589
60	0.0402	142.9630	1.1620
70	0.0469	141.4299	1.1733
80	0.0535	140.1083	1.1803
90	0.0603	138.9056	1.1806
100	0.0669	137.8690	1.1818

The same messages were hidden in image 2 (small size image), table 5 shows the obtained experimental results:

Table 5: Long messages hiding using image 2 as a covering image

Message length(K byte)	MSE	PSNR	Hiding time
1	0.0526	140.2843	0.0185
10	0.0762	136.5638	0.0215
20	0.0781	136.3212	0.0264
30	0.0770	136.4584	0.0287
40	0.0757	136.6347	0.0336
50	0.0763	136.5571	0.0364
60	0.0748	136.7488	0.0431
70	0.0754	136.6686	0.0433
80	0.0754	136.6737	0.0454
90	0.0761	136.5857	0.0488
100	0.0769	136.4784	0.0495

5- Results Analysis

The proposed method uses a rearranged covering image to hide a secret message and to produce a stego_image, the rearrangement process is implemented based on a PK generated by the sender and used by the receiver, this PK key will protect the secret message and will make the process of LSB hacking difficult. The PK can be kept in secret and can be updated any time when the needs arise. The proposed method kept the advantages of LSB method of data steganography without any changes.

To improve the quality parameters (Improving MSE and PSNR values) it is recommended to use a carrier image with big size (see table 1), the quality parameters and the efficiency will depend on the selected image size as shown in figures 14, 15 and 16.

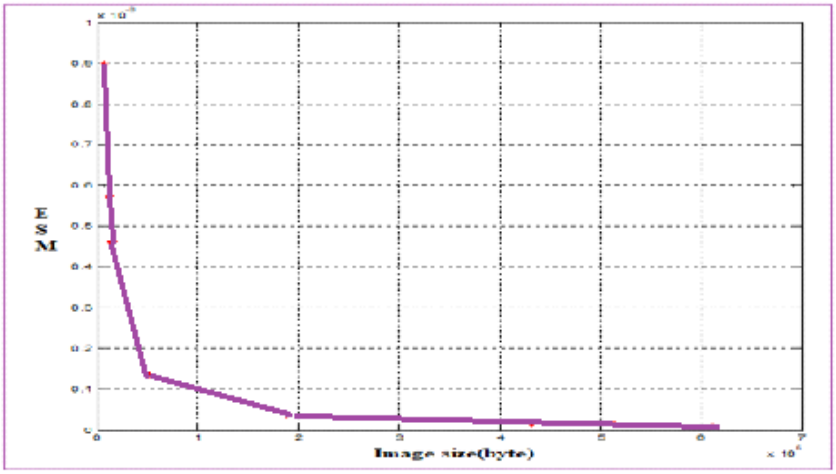

Figure 14: Relationship between image size and MSE

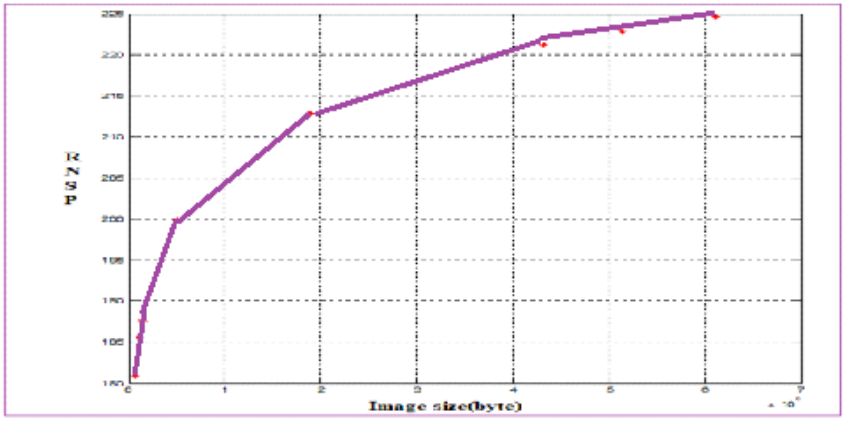

Figure 15: Relationship between image size and PSNR

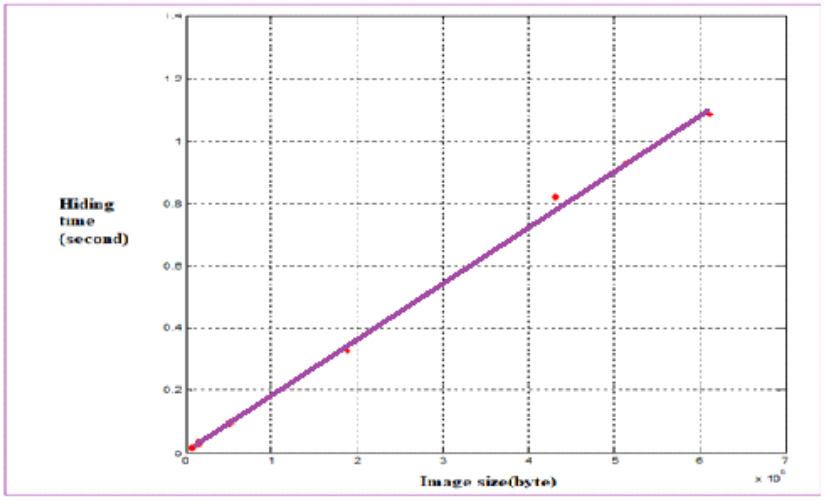

Figure 16: Relationship between image size and Hiding time

Using big size images optimize the values of quality parameters, keeping the proposed method efficient.

6- Conclusion

A method of enhancing LSB security level was proposed. The adding secret message protection is based on using a complex PK to rearrange the carrier image and to produce the stego_image. The PK is to be created by the sender and kept in secret, this PK can be updated or changed depending on the block size and the selected carrier image.
Adding protection stage to LSB does not negatively affect the quality parameters MSE and PSNR, the added time for rearrangement is very small and does not negatively affect LSB efficiency, keeping the proposed method efficient. Based on the obtained experimental results it is recommended to use carrier image with big size, this will optimize the quality parameters (MSE and PSNR) values.

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, 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.

[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. 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.

[30].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.

[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.

