Available Online at www.ijcsmc.com

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. 12, Issue. 12, December 2023, pg.46 – 61

Simple and Secure Digital Color Image Steganography

Prof. Ziad Alqadi
Albalqa Applied University, Jordan Amman

DOI: https://doi.org/10.47760/ijcsmc.2023.v12i12.005

Abstract:

A simple and secure method of digital color image steganography method will be introduced, the method will hide a digital color image in another image, the covering image will be any type and with any size (the covering image can be smaller than the image to be hidden, thus the capacity of the covering image will be unlimited.

The proposed method will apply image resizing, the resizing factors will form the private key to protect the hidden image from being hacked, this key will provide a good key space to secure the image, the extracted image will be very sensitive to the selected values of the private key components. A simple way of image bits hiding and extracting operation will be used, the image bit matrix will converted to one column matrix and embedded in the LSBs of the covering bytes using one assignment operation, the LSBs of the stego bytes will extracted using one operation to create a one column matrix, which will be converted to 8 columns matrix to form the image binary matrix.

The method will be implemented and tested using various covering images and various color images to be hidden. The obtained results will be analyzed to prove the quality, speed and sensitivity of the proposed method.

Keywords: steganography, DCI, covering image, stego image, PK, IBM, resizing, quality, speedup, throughput.

Introduction

Digital color image (DCI) [5-10] is an important data type due to the wide range of computer application requiring this data type. DCI may contain secret information, it may be private or secret, and it require protection to prevent any hacking attacks [11-15].

One of the easiest techniques used to secure DCI is image steganography [60-73]. DCI steganography as shown in figure 1 means image hiding before sending it via unsecure data network and extracting after receiving from the data network [16-20].

Figure 1: DCI steganography process

DCI steganography must hide the image in another covering image without affecting much the covering image, the stego image must be closed to the covering image and the quality parameters calculated between the covering and the stego images must satisfy the quality requirements og good stego system listed in table 1 [21-26]:

Table 1: Good stego system quality requirements [55-60]

Quality parameter	Value
Mean square error (MSE)	Low
Peak signal to noise ratio (PSNR)	High
Correlation coefficient (CC)	Close to 1
Number of samples change rate (NSCR)	Close to zero

The most popular method used in data steganography is least significant bit (LSB) method [60-73], this method reserves the LSBs of the covering-stego bytes to hide-extract the bits of the hidden data, The capacity hiding of LSB method is limited to the covering image size and it is equal the covering image size divided by 8 [27-30].
The LSBs of the covering image color bytes are to be replaced by the image to be hidden bits as shown in figure 2 and 3.

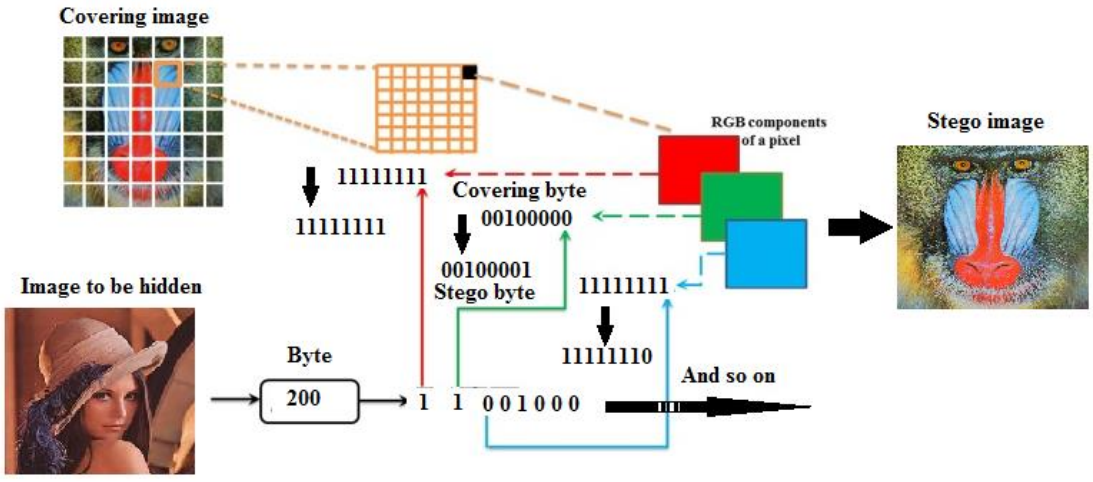

Figure 2: Used LSBs

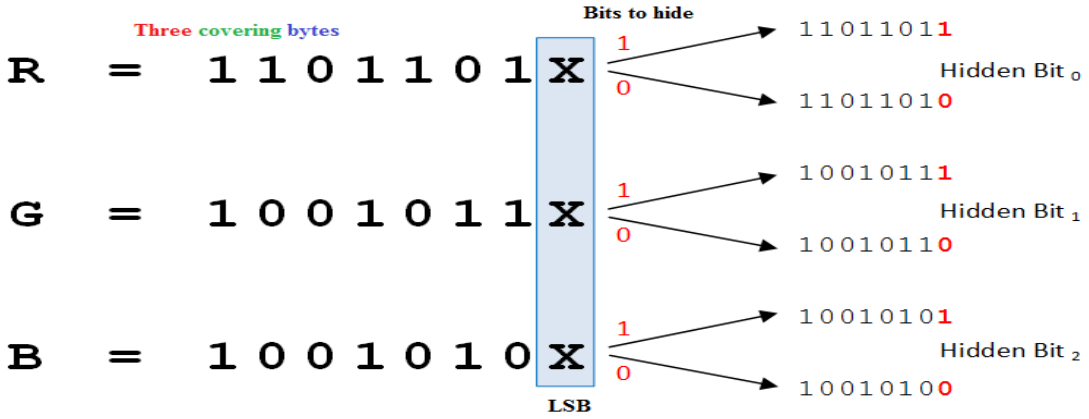

Figure 3: Replacing LSBs by the hidden bits

LSB method assigns a consecutive number of covering bytes to be used for DCI bits hiding, the red byte of the covering bytes is firstly used the green one then the blue byte, the covering bytes are to be converted to binary, the LSBs of these binary number are used for data bits hiding-extracting as shown in figure 4 [31-40].

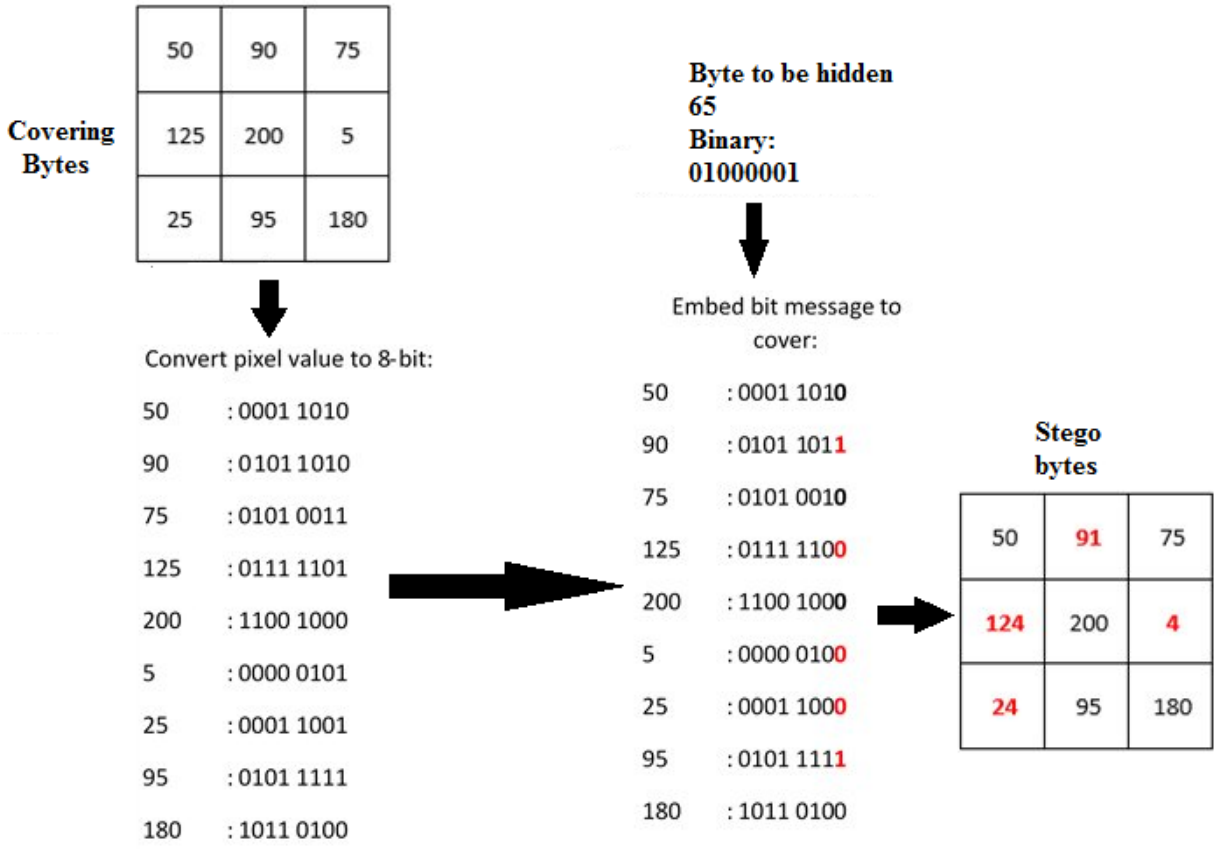

Figure 4: LSB method data hiding

The proposed of this research paper is to introduce a new method of DCI hiding-extracting, which will provide the following enhancement [41-50]:

- Making the hiding capacity unlimited, by resizing the covering image, the size of the DCI to be hidden may be greater than the size of the covering image [51-55].
- Covering image may have any size and any type (gray image or color image).
- The extracting and hiding functions will be simplified, the process of DCI bits hiding will be implemented in batch way by converting the image binary matrix (IBM) to one column matrix, this matrix will replace the LSBs of the covering bytes by performing single assignment operation, the same thing will by applied for the hiding process, the LSBs of the stego bytes will be extracted as one column matrix, then this matrix will be reshaped to 8 columns matrix to form the hidden image IBM. Applying the one operation of hiding and extracting will lead to eliminate the sequence of logical operation used in the hiding and extracting functions used in classical LSB (CLSB) method of image steganography.
- The proposed method will be secure based on using a private key of length equal 192 bits.
- The proposed method will produce a stego image with excellent quality.
- The proposed method will decrease both the hiding and extracting time, it will increase the speed of image steganography, and it will provide a speed up comparing with other existing methods of data steganography.

Many methods based on LSB method [1-4]were introduced, these methods provided a good quality, but the speed of steganography varies from one method to another, the proposed method speed will be compared with CLSB, SLSB, and DSLSB methods, table 2 shows the speed results of these methods:

Table 2: Speed results of some existing methods of data steganography [1-4]

Method	Data length(byte)	HT(second)	ET(second)	HTP(K bytes per second)	ETP(K bytes per second)
CLSB	750	0.062	0.078	5.9767	4.7507
	1000	0.078	0.062	6.3342	7.9689
	1500	0.093	0.109	7.9689	6.7991
Average		0.0777	0.0830	6.7599	6.5062
SLSB	750	2.044	0.073	0.1813	5.0761
	1000	3.338	0.063	0.1480	7.8424
	1500	9.376	0.109	0.0790	6.7991
Average		4.9193	0.0817	0.1361	6.5725
DSLSB	750	0.343	0.078	1.0803	4.7507
	1000	0.592	0.062	0.8346	7.9689
	1500	1.029	0.109	0.7202	6.7991
Average		0.6547	0.0830	0.8784	6.5062

The Proposed Method

The proposed method uses a private key (PK), which contains three components: r n1 and rn2 to define the new dimensions of the resized covering image, and P to define the starting position of the covering-stego bytes. Each component has a double data type, so the address space provided by the PK will be calculated using equation 1, this key space is big enough to resist hacking attacks:

$$\text{Key space} = 2^{3x64} = 2^{192} = 6.277101735386680763835789423207 7x10^{57} \quad (1)$$

The hiding process of the proposed method will be implemented applying the following tasks:

- Cover image resizing using n1 and n2 values.
- Hiding the secret DCI.
- Resizing the stego bytes back to its original size [32-38].

The extracting process of the proposed method will be implemented applying the following tasks:

- Stego image resizing using n1 and n2 values.
- Extracting the secret DCI.

Color image resizing is a simple operation; figure 5 illustrate an example of implementing this operation:

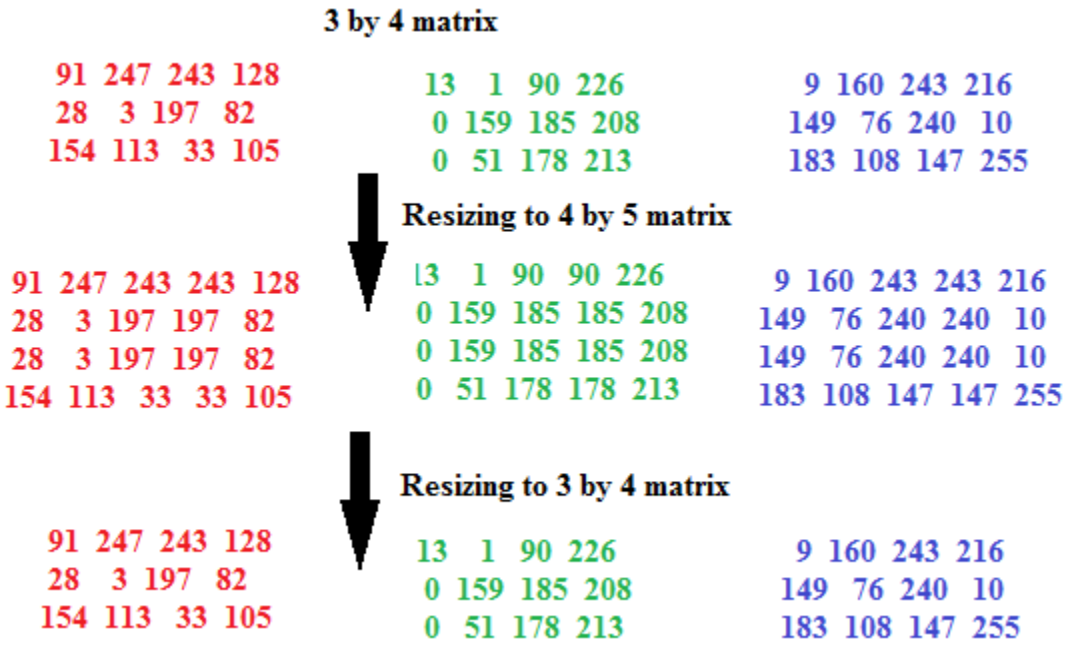

Figure 5: Image resizing example

Using the values of n1 and n2 we can resize the covering image by expanding the image size, and thus expanding the covering image capacity, after hiding DCI the stego image must be resized to its original size. Expanding the image size and reducing the image size by using resizing operations will not affect the covering image, the reduced image will be the same as the source image, this is can be seen in the following example. Figures 6, 7 and 8 show that the reduced image is the same as the source image (the quality parameters calculated between them prove that these two images are the same).

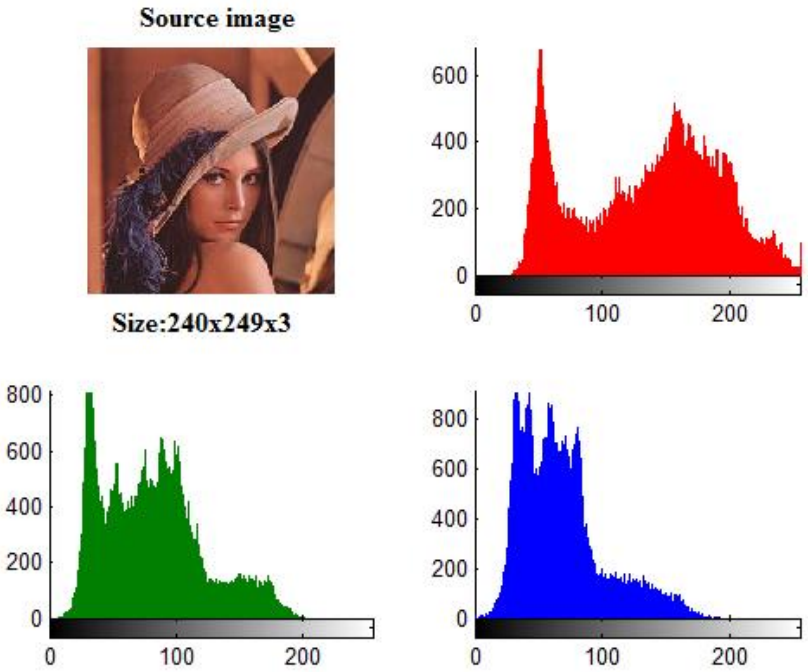

Figure 6: Source image example

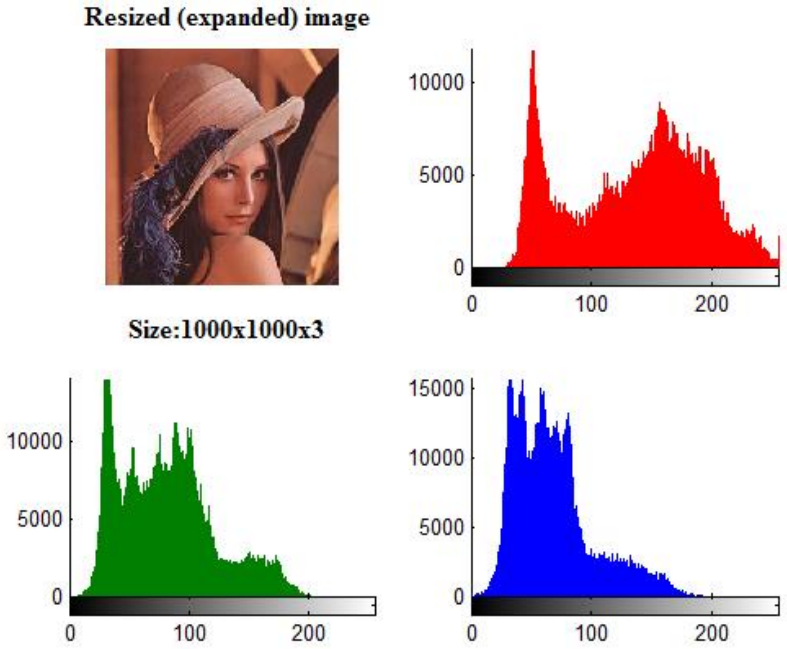

Figure 7: Expanded image

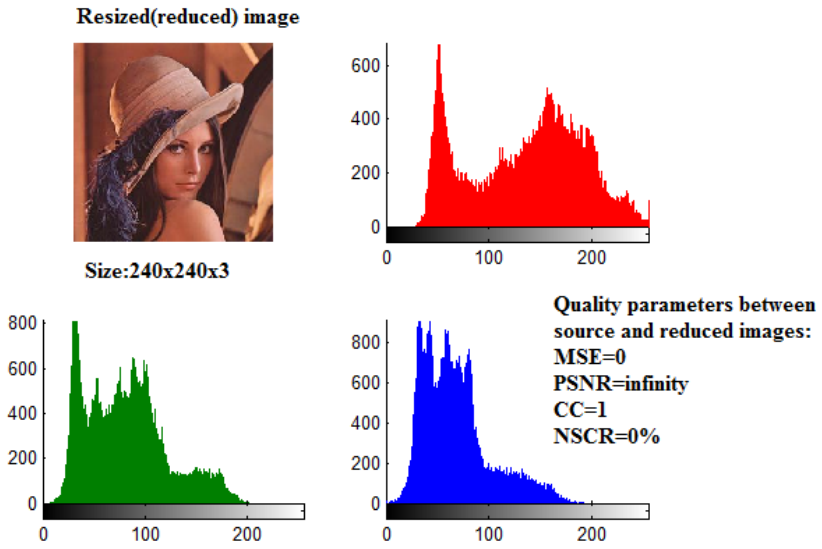

Figure 8: Reduced image

The hiding function of the proposed method can be implemented applying the following steps:

Step 1:

Data preparation:

1) Get the PK.
2) Read the covering image, get the image size, resize the image, get the resized image size.
3) Get the DCI to be hidden, get the image size.
4) Calculate the starting position of the covering bytes.

This step can be implemented by executing the following sequence of mat lab operations:

```
rn1=3000;rn2=3000;P=0.1;
c1=imread('C:\Users\win 7\Desktop\Lena.jpg');
[cn1 cn2 cn3]=size(c1);
c2=imresize(c1,[rn1,rn2]);
[nn1 nn2 nn3]=size(c2);L2=nn1*nn2*nn3;
a1=imread('C:\Users\win 7\Desktop\st_images\4.2.03.tiff');
[n1 n2 n3]=size(a1);L1=n1*n2*n3;
POS=fix(P*L2);
```

Step 2:

DCI hiding:

1) Reshape the secret image to one row matrix.
2) Reshape the covering image to one row matrix.
3) Convert the secret image row matrix to binary to get image binary matrix (IBM);
4) Reshape IBM to one column matrix to get RIBM.
5) Get the covering bytes.
6) Convert the covering bytes to binary.
7) Let the LSBs of the covering bytes equal RIBM to get the stego bytes binary version.
8) Convert the stego bytes to decimal.
9) Return the stego bytes back to the image row matrix.

This step can be implemented by executing the following sequence of mat lab operations:


```
a2=reshape(a1,1,L1);
c3=reshape(c2,1,L2);
st=c3;
a3=dec2bin(a2,8);
a4=reshape(a3,L1*8,1);
s1=c3(1,POS+1:POS+L1*8);
s2=dec2bin(s1,8);
s2(:,8)=a4;
s3=bin2dec(s2)';
st(1,POS+1:POS+L1*8)=s3;
```

Step 3:

Producing stego image:

1) Reshape the stego image row matrix to 3D matrix.
2) Resize the stego image back to original size.

This step can be implemented by executing the following sequence of mat lab operations:

```
stego1=reshape(st,nn1,nn2,nn3);
stego=imresize(stego1,[cn1 cn2]);
```

The extracting function can be implemented applying the following steps:

Step 1:

Data preparation:

1) Get the PK.
2) Resize the stego image and get the image size.
3) Calculate the starting position of the stego bytes.

This step can be implemented by executing the following sequence of mat lab operations:

```
rn1=3000;rn2=3000;P=0.1;
stego2=imresize(stego1,[rn1 rn2]);
LS=prod(size(stego2);
POS=fix(LS*P);
```

Step 2:

DCI extraction:

1) Reshape the stego image to one row matrix.
2) Get the stego bytes.
3) Convert the stego bytes to binary.
4) Get the LSBs from the binary version of the stego bytes to create a one column matrix.
5) Reshape the one column matrix to 8 column matrix to get the DCI IBM.
6) Convert IBM to decimal.
7) Reshape the decimal matrix to DCI size.

This step can be implemented by executing the following sequence of mat lab operations:


```
stego3=reshape(stego2,1,L2);
stb=stego3(1,POS+1:POS+L1*8);
stb1=dec2bin(stb,8);
ei1=stb1(:,8);
ei2=reshape(ei1,L1,8);
ei3=bin2dec(ei2)';
ei4=reshape(ei3,n1,n2,n3);
ei5=uint8(ei4);
```

Implementation and Results Discussion

The proposed method was implemented and tested using various gray and color images, the images were taken from the image data base with the link "https://sipi.usc.edu/database", several approaches of the obtained results analysis were done, below we will follow up these analysis:

1) *Speed analysis*

The proposed method was tested using various messages, the image lena.tiff was selected as a covering image, the following PK was used, the hiding time (HT) in seconds, the extraction time (ET) and the processing time (PT=HT+ET) in seconds were measured, the hiding throughput (HTP) in K bytes per second, the extracting throughput (ETP) in K bytes per second and the processing throughput (PTP) were calculated, and table 3 and 4 show the obtained speed results:

```
Used private key:
rn1=3000;rn2=3000;
P=0.1;
```

Table 3: Obtained times results

Image	Size	HT(second)	ET(second)	PT(second)
5.1.09	256x256	2.1602	0.2973	2.4575
5.1.10	256x256	2.1803	0.2973	2.4776
5.2.08	512x512	7.7833	1.2073	8.9906
5.2.09	512x512	7.5495	1.1523	8.7018
5.3.01	1024x1024	29.5247	4.5847	34.1094
5.3.02	1024x1024	29.4508	4.5970	34.0478
4.2.03	512x512x3	21.9895	3.4146	25.4041
4.2.05	512x512x3	21.9611	3.4321	25.3932
Average		15.3249	2.3728	17.6978

Table 4: Obtained throughputs results

Image	HTP(K bytes per second)	ETP K bytes per second)	PTP K bytes per second)
5.1.09	29.6268	215.3023	26.0431
5.1.10	29.3540	215.2546	25.8314
5.2.08	32.8909	212.0457	28.4742
5.2.09	33.9096	222.1705	29.4193
5.3.01	34.6828	223.3505	30.0210
5.3.02	34.7699	222.7537	30.0754
4.2.03	34.9257	224.9191	30.2314
4.2.05	34.9709	223.7716	30.2444
Average	33.1413	219.9460	28.7925

As shown from tables 3 and 4 the proposed method provided a good speed parameters' values, these results were compared with other methods speed (see table 2), and the proposed method gave a good speed up (speed up of the proposed method equal proposed method throughput divided by other method throughput), it reduced both the hiding and extracting time, and at the same time it increased both the hiding and extracting throughputs, table 5 and 6 show the speed up provided by the proposed method:

Table 5: Speed up of the proposed method in the hiding process

Method	Hiding throughput (K bytes per second)	Speed up of the proposed method
CLSB	6.7599	4.9026
SLSB	0.1361	243.5070
DSLSB	0.8784	37.7292
Proposed method	33.1413	1.0000

Table 6: Speed up of the proposed method in the extracting process

Method	Extracting throughput (K bytes per second)	Speed up of the proposed method
CLSB	6.5062	33.8056
SLSB	6.5725	33.4646
DSLSB	6.5062	33.8056
Proposed method	219.9460	1.0000

2) Stego image quality analysis

The stego image must be closed to the covering image, the quality of the stego image can be visually tested by comparing by eyes the covering image with the stego image, they must be closed, and also the covering image histograms must be closed to the stego image histograms. To prove this fact the image 4.2.03.tiff was hidden in the image lena.tiff using the above mentioned PK, and figures 9, 10 and 11 show the obtained images:

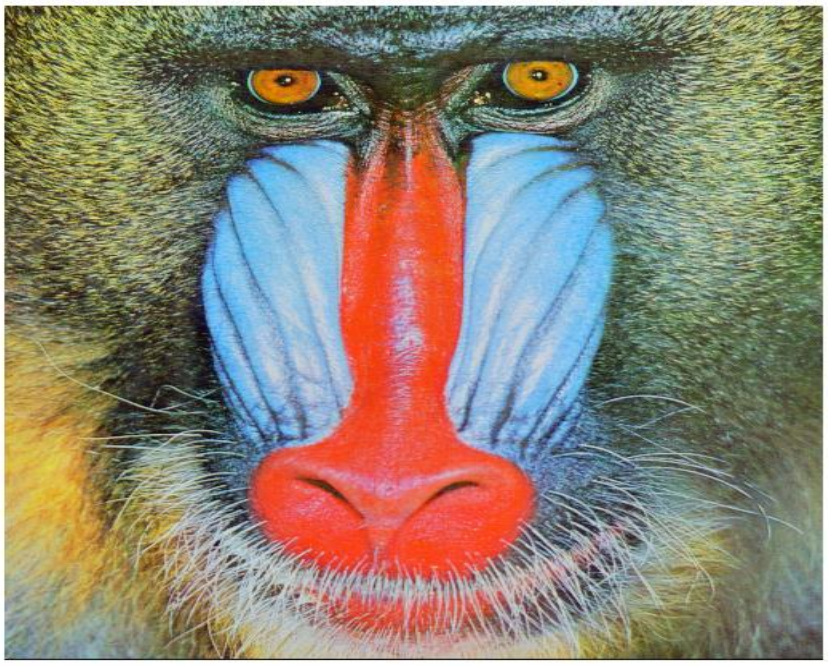

Figure 9: Hidden secret image

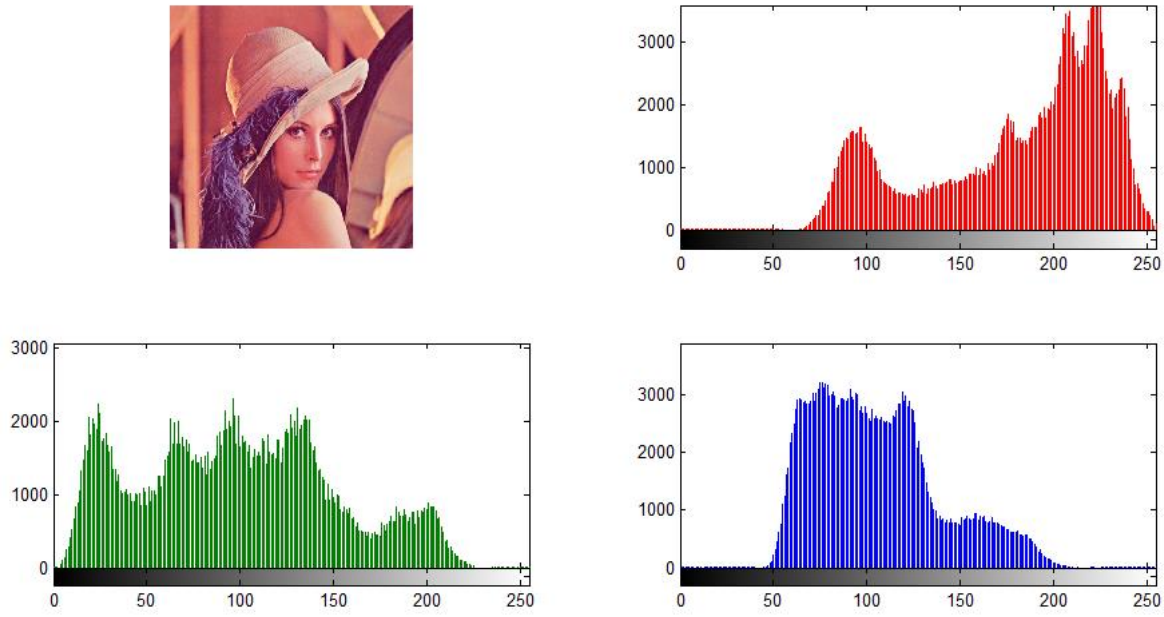

Figure 10: Covering image and histograms

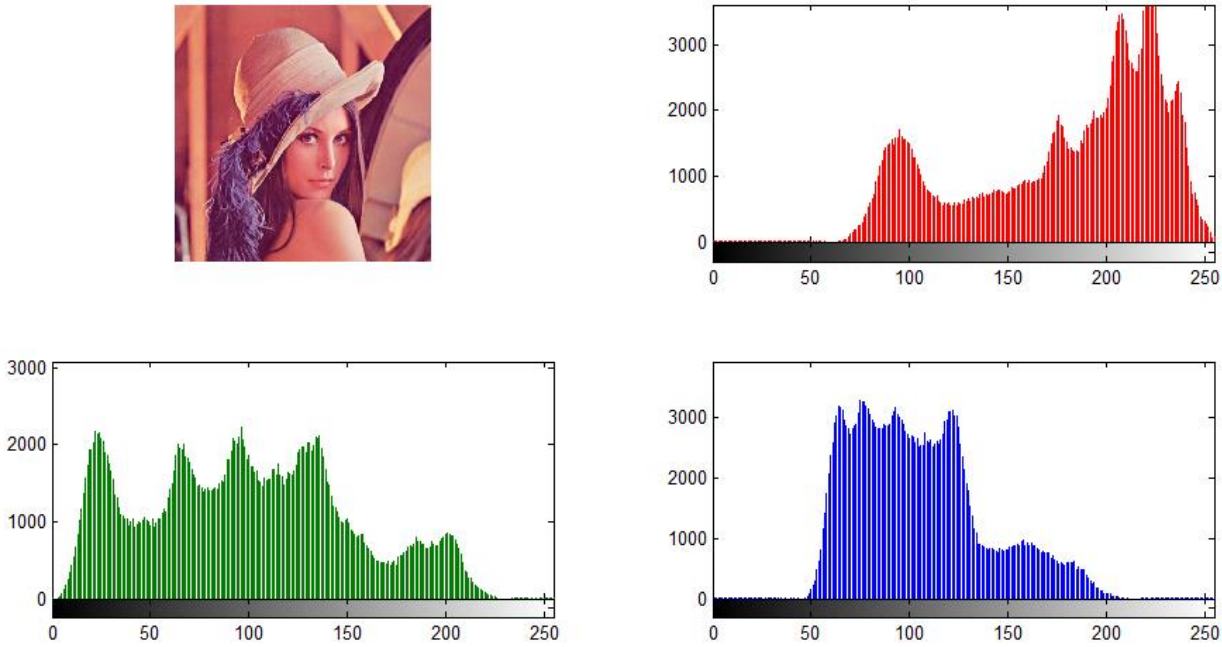

Figure 11: Stego image and histograms

Examining the covering and the stego images by eyes we can see that they are much closed.
Some images from the image data base were selected, each of them was hidden in the covering image ‘lena.tiff; the quality parameters between the covering and the stego images were calculated, the obtained values of these parameters shown in table 6 prove that the proposed method provides a stego images with good quality and it satisfies the quality requirements of good stego system.

Hidden image	MSE	PSNR	CC	NSCR(%)
5.1.09	0.0098	157.0462	1	0.9832
5.1.10	0.0099	156.9758	1	0.9902
5.2.08	0.0390	143.2764	1	3.8964
5.2.09	0.0385	143.3959	1	3.8501
5.3.01	0.1541	129.5296	0.9999	15.4057
5.3.02	0.1555	129.4387	0.9999	15.5463
Remarks	Low	High	Closed to 1	Low
Satisfies the quality requirements				

3) Sensitivity analysis

The Hiding and extracting functions must use the same PKs, any minor changes in the PK in the extraction function will be considered as a hacking attempt by producing damaged extracted DCI, and to show this fact the image 4.2.03.tiff was hidden in the covering image lena.tiff using PK1, the hidden image was extracted using each of the following PKs, figure 12 shows that changing the PK in the extracting function produced a damaged extracted image, and this proves the sensitivity of the proposed method.

PK1:
rn1=3000;rn2=3000;
P=0.1;
PK2:
rn1=2999;rn2=3000;
P=0.1;
PK3:
rn1=3000;rn2=3010;
P=0.1;
PK4:
rn1=3000;rn2=3000;
P=0.01;

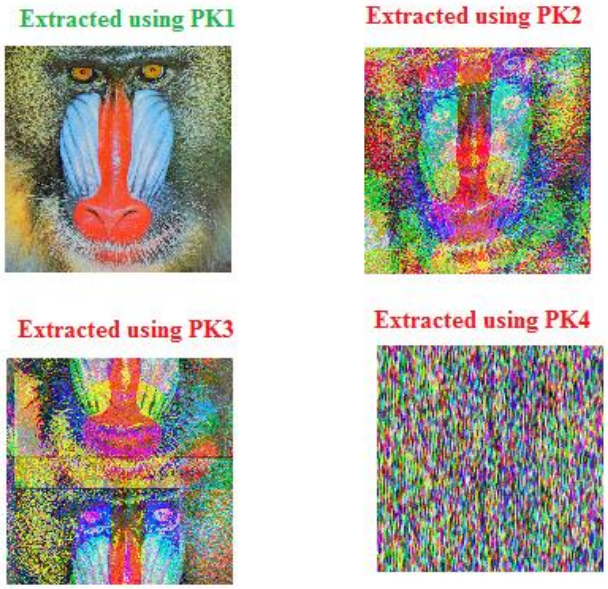

Figure 12: Extracted images

Conclusion

A simple method of color image steganography was proposed, the method used a simple resizing operation and a batch bits hiding and extracting operation to apply digital image steganography, the covering image and the secret image can be any image (gray or color) with any size, the secret image size was not limited to the covering image size, the size of the secret image can be greater than the size of the covering image. The method used a 192 bits private key, this key provided a strong enough key space to protect the image from being hacked, the extracted image was very sensitive to the selected values of the private key in the extracting phase.

The proposed method was implemented using various images, the obtained speed results proved that the proposed method reduced both the hiding and extracting times, the proposed method comparing with other existing methods of data steganography provided a significant speed up by increasing the throughputs of image hiding and image extracting. The proposed method provided an excellent quality parameters, the stego image was always closed to the covering image.

References

[1]. 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.

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

[3]. 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 .

[4]. 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.

[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]. 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.

[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-Jazar (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]. 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.

[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.

[39]. 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.

[40]. 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.

[41]. 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.

[42]. 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.

[43]. 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.

[44]. 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.

[45]. 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).

[46]. 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)

[47]. 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)

[48]. 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)

[49]. 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)

[50]. 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)

[51]. 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)

[52]. 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.

[53]. 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.

[54]. 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.

[55]. 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.

[56]. 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.

[57]. 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.

[58]. 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.

[59]. 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.

[60]. 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.

[61]. 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.

[62]. 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.

[63]. 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.

[64]. 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.

[65]. 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.

[66]. 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.

[67]. 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.

[68]. 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.

[69]. 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

[70]. 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.

[71]. 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.

[72]. 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.

[73]. 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.

