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. 4, April 2023, pg.110 – 124

Securing Message Steganography by using Modified LSB Method

Prof. Ziad Alqadi; Mohammad Al-Raqqad
Albalqa Applied University, Jordan Amman

DOI: https://doi.org/10.47760/ijcsmc.2023.v12i04.010

Abstract:
Message steganography is one of the popular methods used to protect secret message. In this research paper a modified LSB method of message steganography will be introduced. The introduced method will use a complicated private key to protect the message from being hacked, the key will provide an excellent key space capable to resist hacking attacks, it will contain 6 values with a double data type. The private key will be used to divide the covering image into segments and divide the secret message into partitions; each message partition will be hidden in one image segment. The hiding and extracting processes will be implemented in a patch way, by inserting the binary version of the message partition in burst way and extracting the binary version of the message partition also in burst way. The proposed method will keep the quality of the stego image as in LSB method. The efficiency of the proposed method will be closed to the efficiency of LSB method.
The proposed method will be implemented and tested using various images and various covering images, the obtained results will be analyzed to prove the advantages provided by the proposed method.
Keywords: Steganography, LSB, PK, covering image, stego image, image segment, message partition.

Introduction

Steganography [1-5] is the process of hiding secret information in another data which is called a covering data. Steganography is one of the most popular and easiest methods of data protection, most methods based on least significant bit (LSB) and LSB2 are not secure, and it is easy to hack the hidden message [37-43]. Digital color image is the most convenient data which can be used as a covering media for the following reasons [6-15]:

- The color image [50-60] can be easily processed because it is represented by a 3D matrix (one 2D matrix for each color: red, green and blue) as shown in figure 1 [16-20].
- The color image has a huge size capable to hide short and long messages [31-36].
- The pixel values and the character's values are decimal integers and have the same range from 0 to 255, see figure 2 [21-30].
- The clearance of the image can be tested by the image itself and by the image histograms.

- It is easy to convert both the character values and the pixel values to binary to perform the required bits replacement.
- It is easy to reshape the color image to one column or one row matrix.
- It is easy to get a required part (segment) from the image to use it as a covering segment.

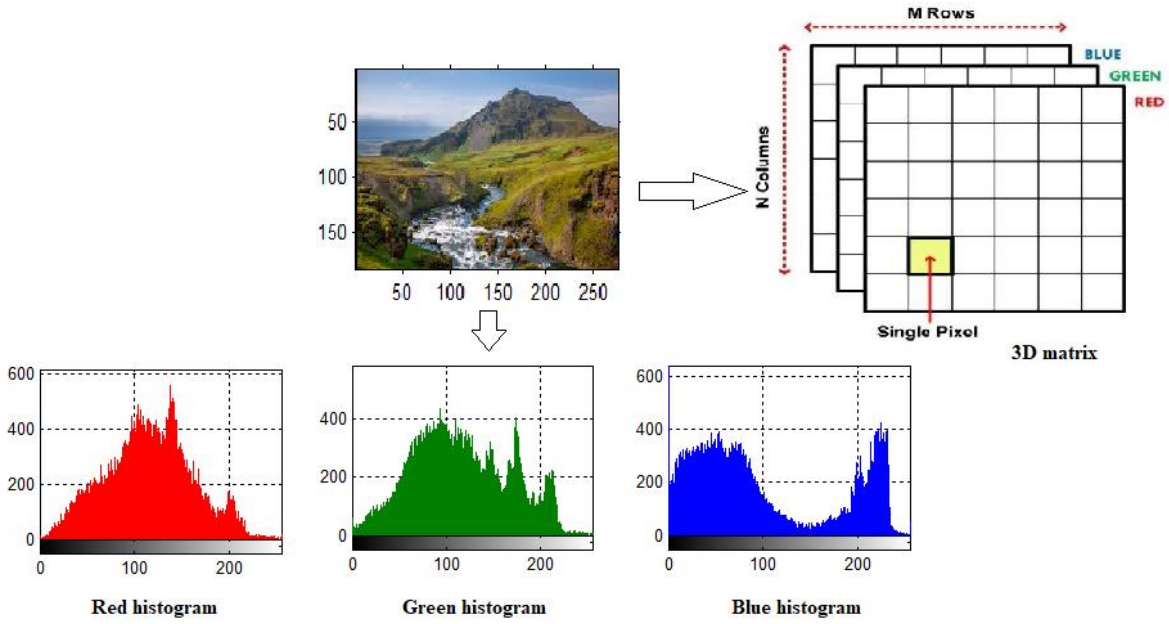

Figure 1: Color image matrices and histograms [43-50]

Color name	RGB triplet	Color
Red	(255, 0, 0)	
Lime	(0, 255, 0)	
Blue	(0, 0, 255)	
White	(255, 255, 255)	
Black	(0, 0, 0)	
Gray	(128, 128, 128)	
Fuchsia	(255, 0, 255)	
Yellow	(255, 255, 0)	
Aqua	(0, 255, 255)	
Silver	(192, 192, 192)	
Maroon	(128, 0, 0)	
Olive	(128, 128, 0)	
Green	(0, 128, 0)	
Teal	(0, 128, 128)	
Navy	(0, 0, 128)	
Purple	(128, 0, 128)	

Figure 2: Color pixels' values [43-50]

Data steganography system contains as shown in figure 3: Covering image (CI), stego image (SI), secret message (SM) and a private key (PK) to add a security issue to protect the message from being hacked [1-10].

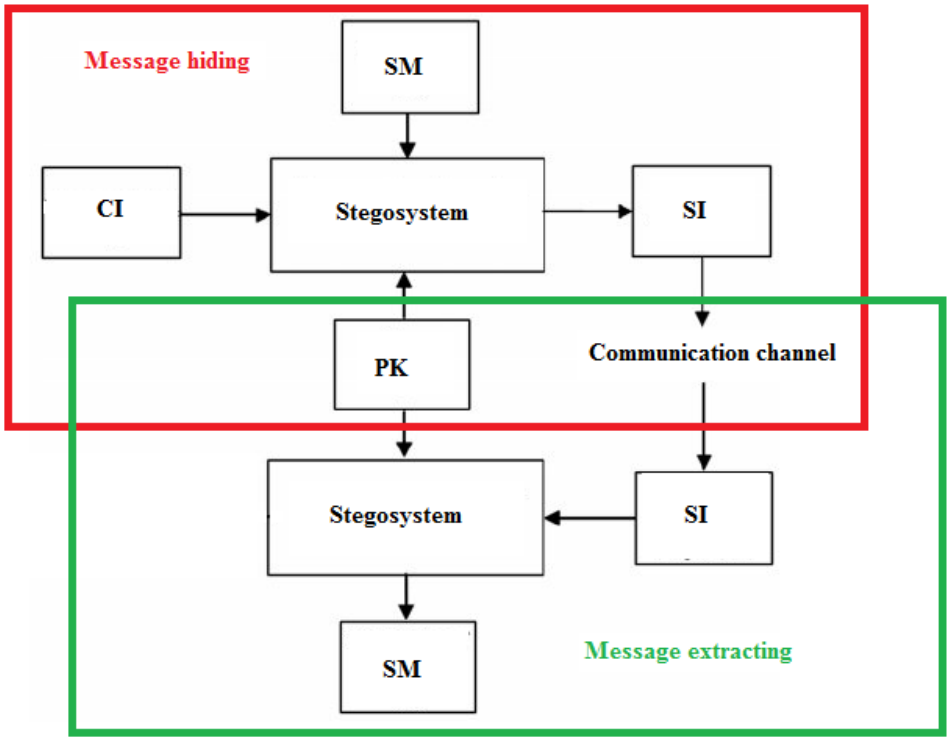

Figure 3: Stego system components

LSB method uses the least significant bits (see figure 4) to be replaced by the message bits, this will add a minor changes to the pixel value, these changes cannot be noticed and the stego image will be always closed to the covering image (the changes are -1, 0 or +1 see figure 5) [1-10].

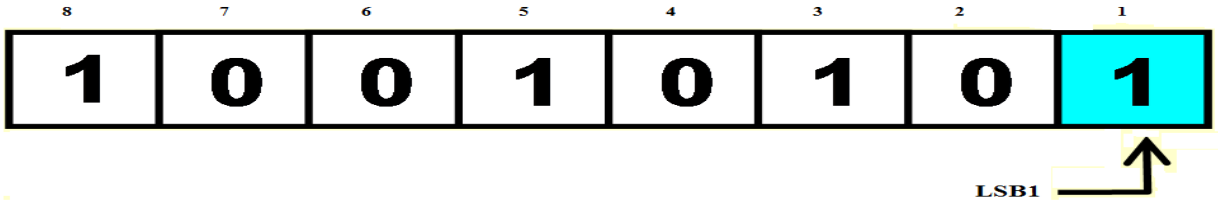

Figure 4: Used LSB bit

Figure 5: Minor changes when using LSB bit

LSB method has a hiding capacity equal the image size divided by 8, each character to be hidden requires 8 bytes from the covering image, and the bytes must are consecutive, this method can be implemented applying the following steps:

Hiding phase:

(See figure 6)

Step 1:

Get the covering image, retrieve the image size, and reshape the image to one column matrix.

Step 2:

Convert the image column matrix to binary.

Step 3:

Get the message, retrieve the message length (L), convert the message to decimal.

Step 4:

Convert the decimal matrix to binary.

Step 5:

Reserve 8 bytes from the binary image and use the LSBs to hide the character byte bits.

Step 6:

Convert the image matrix to decimal.

Step 7:

Reshape back the image matrix to get the stego image.

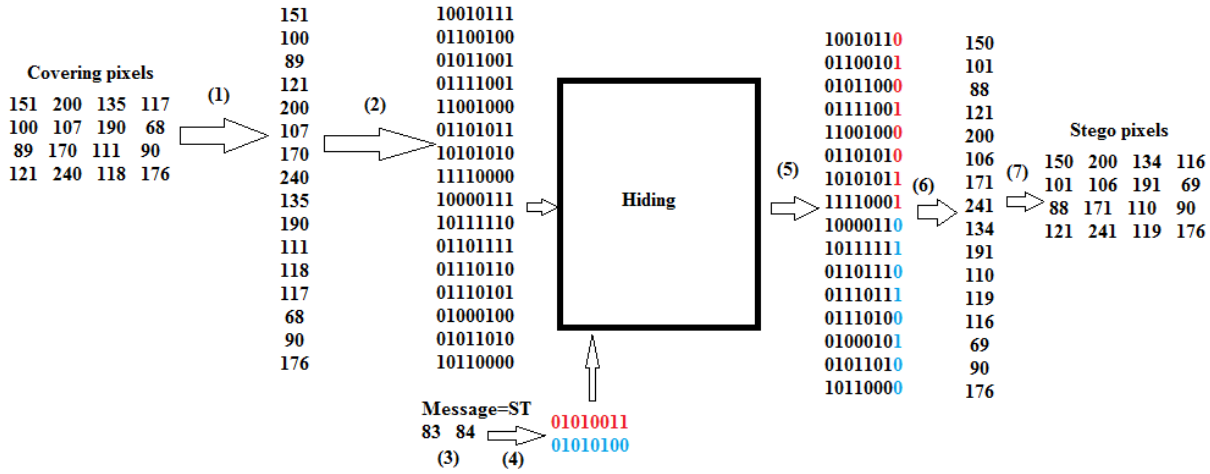

Figure 6: LSB method hiding

Extracting phase

(See figure 7)

Step 1:

Get the stego image, retrieve the image size and reshape the image matrix to one column matrix.

Step 2:

Convert the column matrix to binary.

Step 3:

From the binary matrix extract the LSBs of the 8 consecutive bytes to form the binary version of the character, repeat this step L times.

Step 4:

Convert the character's binary matrix to decimal, then to characters to get the secret message.

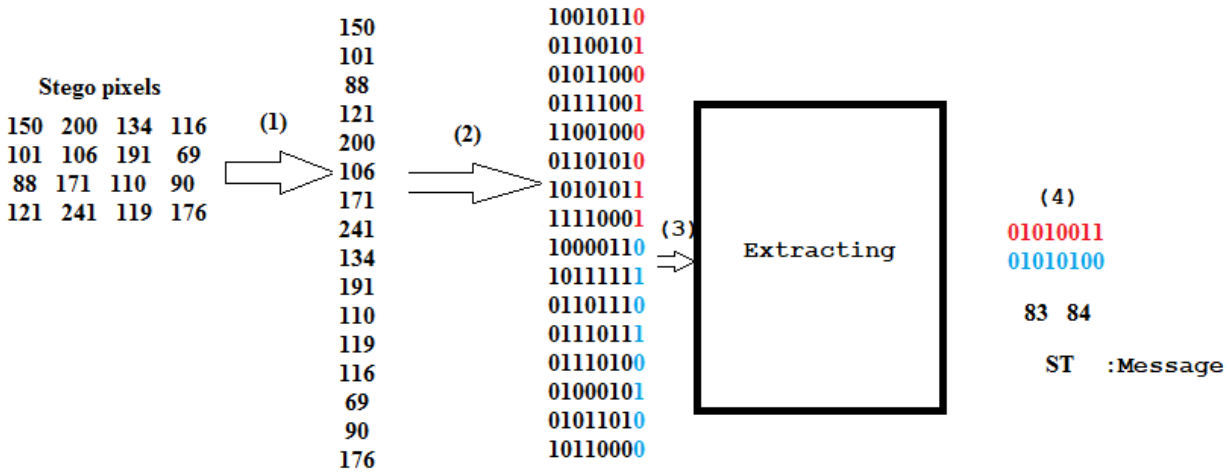

Figure 7: LSB method message extraction

The Proposed Method

The proposed method is based on LSB method by adding the following modifications:

1) Private key:

The proposed method uses a complicated private key (PK), which contains as shown in table 1 six values, each of them has a double data type:

Table 1: PK structure

Image segments fractions		
S1	S2	S3
Message partitions fraction		
P1	P2	P3
Example		
0.197	0.265	0.298
0.321	0.178	0.275

The PK is used to divide the covering image into segments (4 segments) and to divide the message into partitions (4 partitions), each image segment will hold one message partition, the sizes of the segments are different and so the partitions sizes. The covering image may be divided row wise or column wise, below is an example of dividing a covering image and a secret message using the following PK (see figures 8 and 9):

PK:
S1=0.27;S2=0.159;S3=0.345;
P1=0.16;P2=0.22;P3=0.21;

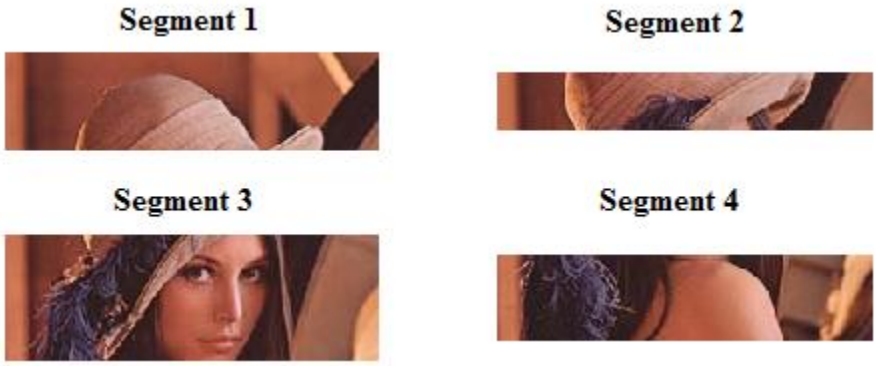

Figure 8: Image "lena.jpg" segments

Source message:
Securing secret message using modified LSB method of data steganography
MP1 =
Securing se
MP2 =
cret message us
MP3 =
ing modified L
MP4 =
SB method of data steganography

Figure 9: Message partitions

2) Patch hiding and extracting

The message binary version is to be reshaped into one column matrix and inserted in the LSBs of the image binary version using one operation, also the extracted LSBs from the stego image (column matrix) is to be reshaped to 8 column matrix to form the binary version of the message, figure 10 and 11 show how to apply hiding and extracting operations using patch method.

Patch method will minimize the number of operations required to apply message hiding and message extracting, this will simplify these operations and will reduce the hiding and extracting times, thus the performance of message steganography will be improved.

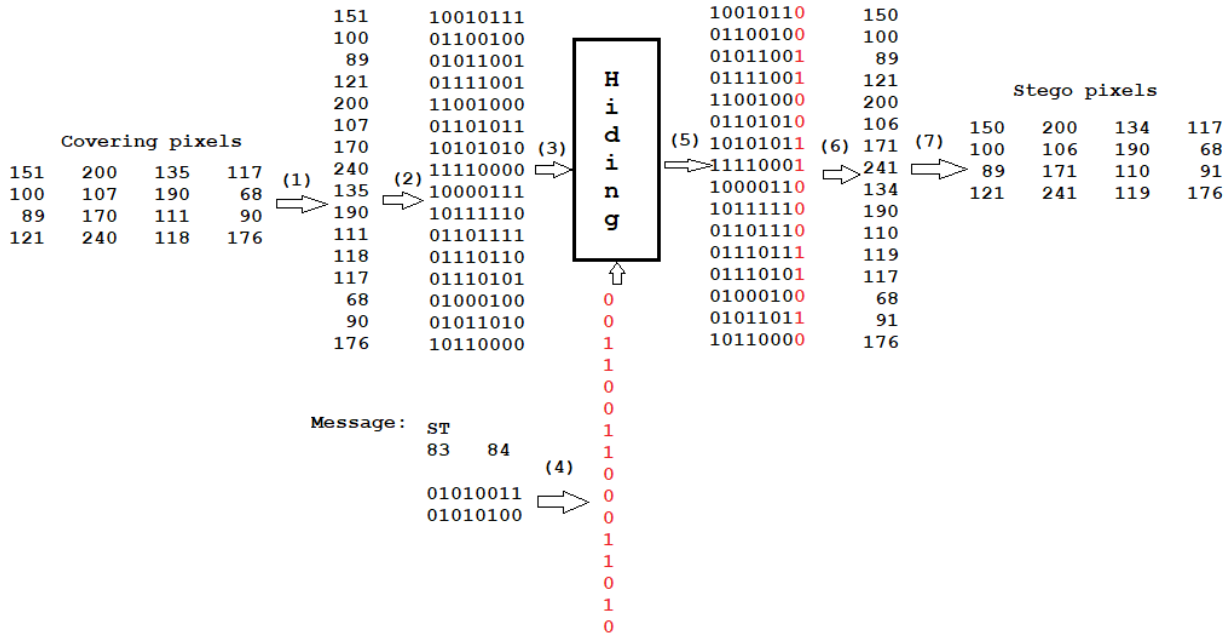

Figure 10: Hiding using patch method

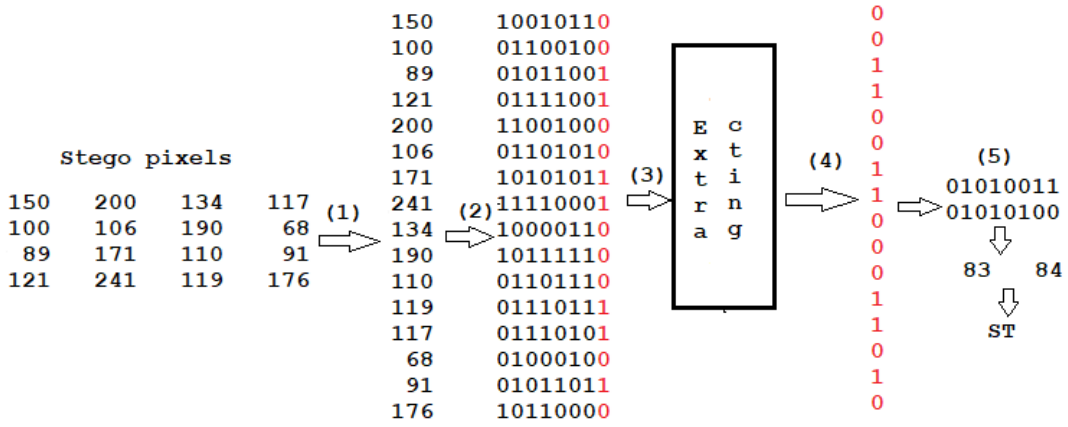

Figure 11: Extracting using patching

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

Step 1:

Data preparation: get the image, retrieve the image size, get the message, retrieve the message length, this step can be implemented by executing the following mat lab instructions:

```
a=imread('C:\Users\win 7\Desktop\Lena.jpg');
[n1 n2 n3]=size(a);s=n1*n2*n3;
mes='Securing secret message using modified LSB method of data steganography';
L=length(mes);
```

Step 2:

Get the private key (PK), this step can be implemented by executing the following mat lab instructions:
(Her position where to start hiding and extracting was added), this step can be implemented by executing the following mat lab instructions:

```
S1=0.27;S2=0.159;S3=0.345;
P1=0.16;P2=0.22;P3=0.21;
```

Step3:

Image dividing into segments and message dividing into partitions: use the PK to calculate the size of each image segment, and the length of each partition length, extract each segment and extract each partition, this step can be implemented by executing the following mat lab instructions:

```
S1R=fix(S1*n1);
S2R=fix(S2*n1);
S3R=fix(S3*n1);
S4R=n1-S1R-S2R-S3R;
P1L=fix(L*P1);
P2L=fix(L*P2);
P3L=fix(L*P3);
P4L=L-P1L-P2L-P3L;
MP1=mes(1,1:P1L);
MP2=mes(1,P1L+1:P1L+P2L);
MP3=mes(1,P1L+P2L+1:P1L+P2L+P3L);
MP4=mes(1,P1L+P2L+P3L+1:L);
L1=length(MP1);L2=length(MP2);
L3=length(MP3);L4=length(MP4);
POS=L1;
i1=a(1:S1R,1:n2,:);[i1n1 i1n2 i1n3]=size(i1);
i2=a(S1R+1:S1R+S2R,1:n2,:);[i2n1 i2n2 i2n3]=size(i2);
i3=a(S1R+S2R+1:S1R+S2R+S3R,1:n2,:);[i3n1 i3n2 i3n3]=size(i3);
i4=a(S1R+S2R+S3R+1:n1,1:n2,:);[i4n1 i4n2 i4n3]=size(i4);
```


Step 4:

Hide each partition in the associated segment, use POS as a starting point of data hiding, this step can be implemented as shown in figure 10, and it can be implemented by executing the following mat lab instructions:

```
%First partition:
MD1=uint8(MP1);
MB1=dec2bin(MD1,8);
MB12=reshape(MB1,L1*8,1);
si1=reshape(i1,1,i1n1* i1n2* i1n3);
S1B=dec2bin(si1,8);
S1B(POS+1:POS+L1*8,8)=MB12;
S1D=bin2dec(S1B)';
st1=reshape(S1D,[i1n1,i1n2 i1n3]);
%second partition:
MD2=uint8(MP2);
MB2=dec2bin(MD2,8);
MB22=reshape(MB2,L2*8,1);
si2=reshape(i2,1,i2n1* i2n2* i2n3);
S2B=dec2bin(si2,8);
S2B(POS+1:POS+L2*8,8)=MB22;
S2D=bin2dec(S2B)';
st2=reshape(S2D,[i2n1,i2n2 i2n3]);
%third partition:
MD3=uint8(MP3);
MB3=dec2bin(MD3,8);
MB32=reshape(MB3,L3*8,1);
si3=reshape(i3,1,i3n1* i3n2* i3n3);
S3B=dec2bin(si3,8);
S3B(POS+1:POS+L3*8,8)=MB32;
S3D=bin2dec(S3B)';
st3=reshape(S3D,[i3n1,i3n2 i3n3]);
%fourth partition:
MD4=uint8(MP4);
MB4=dec2bin(MD4,8);
MB42=reshape(MB4,L4*8,1);
si4=reshape(i4,1,i4n1* i4n2* i4n3);
S4B=dec2bin(si4,8);
S4B(POS+1:POS+L4*8,8)=MB42;
S4D=bin2dec(S4B)';
st4=reshape(S4D,[i4n1,i4n2 i4n3]);
```

Step 5:

Combine the stego segment in one image to get the stego image, this step can be implemented by executing the following mat lab instructions:

```
sa(1:S1R,1:n2,:)=st1;
sa(S1R+1:S1R+S2R,1:n2,:)=st2;
sa(S1R+S2R+1:S1R+S2R+S3R,1:n2,:)=st3;
sa(S1R+S2R+S3R+1:n1,1:n2,:)=st4;
sa=uint8(sa);
```


The extracting process can be implemented applying the following steps:
Step 1:
Get the stego image and retrieve the image size, this step can be implemented by executing the following mat lab instructions:

```
load sa
load L; message length
[n1 n2 n3]=size(sa);s=n1*n2*n3;
```

Step 2:
Get the PK, this step can be implemented by executing the following mat lab instructions:
(Her position where to start hiding and extracting was added), this step can be implemented by executing the following mat lab instructions:

```
S1=0.27;S2=0.159;S3=0.345;
P1=0.16;P2=0.22;P3=0.21;
```

Step 3:
Image dividing into segments and message dividing into partitions: use the PK to calculate the size of each image segment, and the length of each partition length, extract each segment and extract each partition, this step can be implemented by executing the following mat lab instructions:

```
S1R=fix(S1*n1);
S2R=fix(S2*n1);
S3R=fix(S3*n1);
S4R=n1-S1R-S2R-S3R;
P1L=fix(L*P1);
P2L=fix(L*P2);
P3L=fix(L*P3);
P4L=L-P1L-P2L-P3L;
POS=P1L;
si1=sa(1:S1R,1:n2,:);[i1n1 i1n2 i1n3]=size(si1);
si2=sa(S1R+1:S1R+S2R,1:n2,:);[i2n1 i2n2 i2n3]=size(si2);
si3=sa(S1R+S2R+1:S1R+S2R+S3R,1:n2,:);[i3n1 i3n2 i3n3]=size(si3);
si4=sa(S1R+S2R+S3R+1:n1,1:n2,:);[i4n1 i4n2 i4n3]=size(si4);
si1r=reshape(si1,1,i1n1* i1n2* i1n3);
```

Step 4:
Message partitions extraction: for each message partition apply extraction as shown in figure 11; this step can be implemented by executing the following mat lab instructions:


```
%extract partition 1:
ss1=si1r(1,POS+1:POS+P1L*8);
ss1b=dec2bin(ss1,8);
em1=ss1b(:,8);
em11=reshape(em1,P1L,8);
em1e=bin2dec(em11)';
 %extract partition 1:
si2r=reshape(si2,1,i2n1* i2n2* i2n3);
ss2=si2r(1,POS+1:POS+P2L*8);
ss2b=dec2bin(ss2,8);
em2=ss2b(:,8);
em21=reshape(em2,P2L,8);
em2e=bin2dec(em21)';

%extract partition 3:
si3r=reshape(si3,1,i3n1* i3n2* i3n3);
ss3=si3r(1,POS+1:POS+P3L*8);
ss3b=dec2bin(ss3,8);
em3=ss3b(:,8);
em31=reshape(em3,P3L,8);
em3e=bin2dec(em31)';
 %extract partition 4:
si4r=reshape(si4,1,i4n1* i4n2* i4n3);
ss4=si4r(1,POS+1:POS+P4L*8);
ss4b=dec2bin(ss4,8);
em4=ss4b(:,8);
em41=reshape(em4,P4L,8);
em4e=bin2dec(em41)';
```

Step 5:

Combine the extracted partitions in one partition to get the secret message, this step can be implemented by executing the following mat lab instructions:

```
emes=[em1e em2e em3e em4e];
sms=char(emes)
```

Implementation and Results Discussion

The proposed method was implemented using various messages and various covering images, the images were taken from the http:// sipi.usc.edu/database/ that is also known as the USC-SIPI Image Database to analyze the utility and the do-ability of our proposed gray and RGB images cryptography scheme. All the related experiments and simulations have been performed in MATLAB environment.

The proposed method was tested for sensitivity, the hiding function and the extraction function must use the same PK, any changes in the PK during the extraction phase will be considered as a hacking attempt by extracting a damages unreadable message. To prove the method sensitivity the message "Securing secret message using modified LSB method of data steganography" was hidden in the image 'lena.jpg' using PK1, table 2 shows the extracted messages using other PKs:


```
PK1:
S1=0.27;S2=0.159;S3=0.345;
P1=0.16;P2=0.22;P3=0.21;
PK2:
S1=0.17;S2=0.159;S3=0.345;
P1=0.16;P2=0.22;P3=0.21;
PK3:
S1=0.27;S2=0.21;S3=0.345;
P1=0.16;P2=0.22;P3=0.21;
PK4:
S1=0.27;S2=0.21;S3=0.345;
P1=0.26;P2=0.22;P3=0.21;
```

Table 2: Extracting using various PKs

Used PK	Extracted message
PK1	Securing secret message using modified LSB method of data steganography
LSB	=gM'»o¹-¡«£□%)+)+-'+!+¡©§¡□□ÈÊHÂ□JÄÊÌÆÊÚ□âùÞÒ13□ _8D□□6Q/;□>²¹:□*;□□®
PK2	C@KÊ□ÀÅÀÆÏCX□cx^P2zXb□ð□□□ÿ□®2□¾;»□°□»¿□¾□ËÊ}½XÑ^ÕØÕÐÑ□]UURD\ZB@@AQMD□
PK3	□CZ□□H□□□□□□□9;9□9#+!;¥-¢□ ¯«éëmç£oáïíãëë□ÅÍÏÅECÉÅKLDKÚVa{]□8²Ë(V8F□Å}□5
PK4	□□□¼¾¼<+9>,²®«¥§)²f`gDL□FjÔÒÊ□□□□¶3´2°□"□□□□;¸µ□9»224¶gæ¨ål l+4!j#Op5e'

From table 2 we can see that using LSB method to extract the message will extract a damaged message, also any minor changes in the PK (PK1) will produce a damaged previous message was hidden using various covering images and using PK1, mean square error (MSE) [50-55], peak signal to noise ratio (PSNR), correlation coefficient (CC) and number of pixels change ratio (NPCR) were calculated between the covering images and the stego images [56-63], table 3 show the obtained results:

Table 3: Quality parameters between covering and stego images

Covering image	MSE	PSNR	CCr, CCg, CCb	NPCR %
House.tiff	0.00034205	190.6308	1, 1, 1	0.0342
2.2.01.tiff	0.000099182	201.4622	1, 1, 1	0.0099
2.2.21.tiff	0.000085831	203.3273	1, 1, 1	0.0086
4.2.07.tiff	0.00038783	187.9107	1, 1, 1	0.0388
Lena,jpg	0.0015	175.7790	1, 1, 1	0.1510
Remarks	Low	High	Excellent	Low

From table 3 we can see that the stego images are very closed to the covering ones, bedding the message keeps the quality of the stego image high, this can be visually tested by locking to the images and their histogram as shown in figures 12 and 13, the stego image is much closed to the covering image:

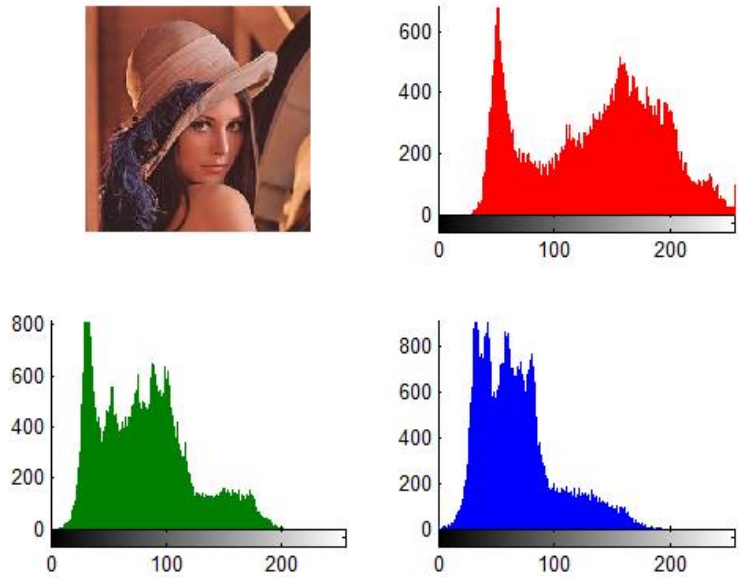

Figure 12: Covering image and histograms (example)

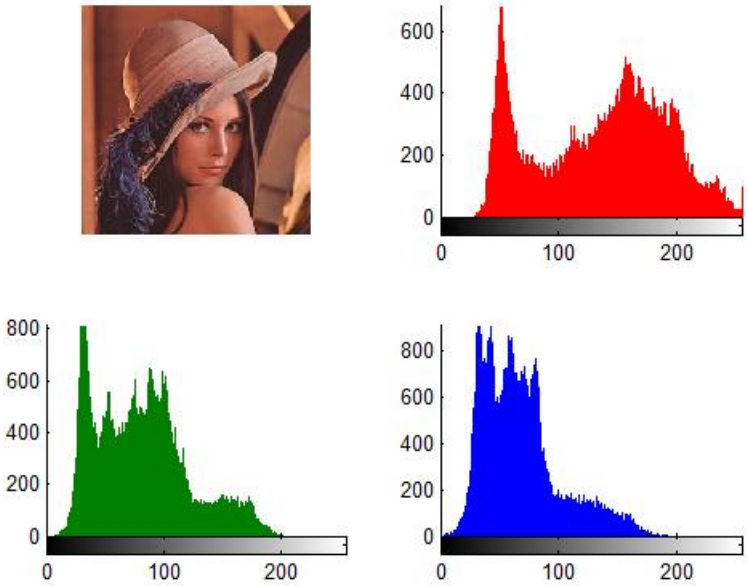

Figure 13: Stego image and histograms

The speed of the proposed method was tested, several messages were selected, the hiding time and the extracting times were measured, the throughput (Bytes processed per second=message size divided by the time), table 4 shows the speed parameters of processing various messages:

Table 4: Speed results

Covering image	Size (byte)	Hiding time (second)	Extracting time(second)	Hiding throughput (bytes per second)	Extracting throughput (bytes per second)
Message length= 2845 characters					
House.tiff	786432	3.7480	0.0530	759.0715	53679
2.2.01.tiff	3145728	15.3010	0.0640	185.9356	44453
2.2.21.tiff	3145728	15.2510	0.0560	186.5451	50804

4.2.07.tiff	786432	3.7240	0.0500	763.9635	56900
Lena,jpg	172800	0.8250	0.0510	3448.5	55784
Message length= 8535 characters					
House.tiff	786432	3.7920	0.1080	2250.8	79028
2.2.01.tiff	3145728	15.1180	0.1110	564.5588	76892
2.2.21.tiff	3145728	15.6590	0.1140	545.0540	74868
4.2.07.tiff	786432	3.7920	0.1080	2250.8	79028
Lena,jpg	172800	0.8230	0.1430	10371	59685

And as we can see from the table above, the time for message hiding increases with the increase in the size of the carrier image, and accordingly, we recommend using carrier images of a small size to hide short secret messages, so as to reduce the time required to process the image by dividing it into segments, for larger messages we can select larger images to keep the throughput os steganography acceptable.

Conclusion

A secure method based on LSB method of secret messages cryptography was introduced. The method provided a high level of security by using a complicated PK, this key contains 6 values, each of them had a double data type, and thus the key space will be very large and capable to resist hacking attacks. The extracted message was very sensitive to the selected PK, adding minor changes to the PK in the extraction phase was considered as a hacking attempt by extracting a damaged unreadable message. The PK was used to divide the covering-stego images into segments with variable lengths and to divided the secret message into partitions with different lengths, each message partition was embedded into the associated segment. It was easy to change the PK and the covering image without the needs to modify the method operations. The qualities of the stego images were tested and it was shown that the stego image was always closed to the covering image and the obtained quality parameters values were always excellent and acceptable. The proposed method gave a good performance and it was recommended to use covering images with small sizes to increase the speed of message steganography.

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]. EE. KisikChang, J. Changho, & L. Sangjin,"High Quality Perceptual Steganographic Techniques", Springer. 2939, pp.518-531, 2004.doi: 10.1007/978-3-540-24624-4_42, http://www.springerlink.com/content/c6guuj5xnyy4wj3c/

[5]. C. Kessler,"Steganography: Hiding Data within Data" An edited version of this paper with the title "Hiding Data in Data", Windows & .NET Magazine, 2001. [Online] Available: http://www.garykessler.net/library/steganography.html (October 4,2011)

[6]. Gandharba Swain, &S.K.lenka,"Steganography-Using a Double Substitution Cipher", International Journal of Wireless Communications and Networking. 2(1), pp.35-39, 2010. ISSN: 0975-7163. http://www.serialspublications.com/journals1.asp?jid=436&jtype

[7]. Hideki Noda, MichiharuNimi, &Eiji Kawaguchi,"High- performance JPEG steganography using Quantization index modulation in DCT domain", Pattern Recognition Letters, 27, pp.455-46, 2006.http://ds.lib.kyutech.ac.jp/dspace/bitstream/10228/450/1/repository6.pdf

[8]. Kathryn,"A Java Steganography Tool", 2005.http://diit.sourceforge.net/files/Proposal.pdf

[9]. Motameni, M.Norouzi, M.Jahandar, & A. Hatami,"Labeling method in Steganography", Proceedings of world academy of science, engineering and technology, 24, pp.349-354, 2007. ISSN 1307-6884. http://www.waset.org/journals/waset/v30/v30-66.pdf

[10]. Mohammed A.F Al Husainy, "Message Segmentation to Enhance the Security of LSB Image Steganography", International Journal of Advanced Computer Science and Applications, 3(3): 57-62, 2012.http://www.ijacsa.thesai.org

[11]. Mohammed A.F Al Husainy, "Developed Segmented LSB Image Steganography", International Science and Technology Conference (ISTEC 2012), Dubai, December 13-15, 2012. http://www.iste-c.net

[12]. 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.

[13]. 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

[14]. 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.

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

[16]. 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

[17]. 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

[18]. 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.

[19]. 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.

[20]. 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.

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

[22]. 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.

[23]. 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.

[24]. 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.

[25]. 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.

[26]. 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

[27]. 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

[28]. 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.

[29]. 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

[30]. 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

[31]. 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

[32]. 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.

[33]. 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.

[34]. 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.

[35]. 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.

[36]. 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.

[37]. 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.

[38]. 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.

[39]. Abdullah N. Olimat, Ali F. Al-Shawabkeh, Ziad A. Al-Qadi, Nijad A. Al-Najdawi, Forecasting the influence of the guided flame on the combustibility of timber species using artificial intelligence, Case Studies in Thermal Engineering, Volume 38, 2022, 102379, ISSN 2214-157X, https://doi.org/10.1016/j.csite.2022.102379.

[40]. 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.

[41]. 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.

[42]. 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.

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

[44]. 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.

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

[46]. J. Vilkamo and T. Bäckström, "Time-Frequency Processing: Methods and Tools," in Parametric Time-Frequency Domain Spatial Audio, V. Pulkki, S. Delikaris-Manias, and A. Politis, Eds. Wiley, 2017, pp. 3–24.

[47]. K Matrouk, A Al-Hasanat, H Alasha'ary, Ziad Al-Qadi, H Al-Shalabi, Speech fingerprint to identify isolated word person, World Applied Sciences Journal, 31 (10), 1767-1771, 2014.

[48]. Ziad alqadi, Analysis of stream cipher security algorithm, Journal of Information and Computing Science, vol. 2, issue 4, pp. 288-298, 2007.

[49]. 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, issue 1, pp. 86-93, 2019.

[50]. Musbah J Aqel, Ziad ALQadi, Ammar Ahmed Abdullah, RGB Color Image Encryption-Decryption Using Image Segmentation and Matrix Multiplication, International Journal of Engineering and Technology, vol. 7. Issue 3.13, pp. 104-107. 2018.

[51]. Jihad Nadir, Ashraf Abu Ein, Ziad Alqadi, A Technique to Encrypt-decrypt Stereo Wave File, International Journal of Computer and Information Technology, vol. 5, issue 5, pp. 465-470, 2016.

[52]. Saleh Khawatreh, Belal Ayyoub, Ashraf Abu-Ein, Ziad Alqadi, A Novel Methodology to Extract Voice Signal Features, International Journal of Computer Applications, vol. 975, pp. 8887, 2018.

[53]. 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 9, pp. 4092-4098, 2019.

[54]. Aws Al-Qaisi, Saleh A Khawatreh, Ahmad A Sharadqah, Ziad A Alqadi, Wave File Features Extraction Using Reduced LBP, International Journal of Electrical and Computer Engineering, vol. 8. Issue 5, pp. 2780-2787, 2018.

[55]. 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.

[56]. Ashraf Abu-Ein, Ziad AA Alqadi, Jihad Nader, A TECHNIQUE OF HIDING SECRETE TEXT IN WAVE FILE, International Journal of Computer Applications, 2016.

[57]. Ismail Shayeb, Ziad Alqadi, Jihad Nader, Analysis of digital voice features extraction methods, International Journal of Educational Research and Development, vol. 1, issue 4, pp. 49-55, 2019.

[58]. Jihad Nader Ahmad Sharadqh, Ziad Al-Qadi, Bilal Zahran, Experimental Investigation of Wave File Compression-Decompression, International Journal of Computer Science and Information Security, vol. 14m issue 10, pp. 774-780, 2016.

[59]. 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.

[60]. Majed O Al-Dwairi, A Hendi, Z AlQadi, an efficient and highly secure technique to encrypt-decrypt color images, Engineering, Technology &Applied Science Research, vol. 9, issue 3, pp. 4165-4168, 2019.

[61]. Amjad Y Hendi, Majed O Dwairi, Ziad A Al-Qadi, Mohamed S Soliman, a novel simple and highly secure method for data encryption-decryption, International Journal of Communication Networks and Information Security, vol. 11, issue 1, pp, 232-238, 2019

[62]. Prof. Ziad Alqadi, Dr. Mohammad S. Khrisat, Dr. Amjad Hindi, Dr. Majed Omar Dwairi, USING SPEECH SIGNAL HISTOGRAM TOCREATE SIGNAL FEATURES, International Journal of Engineering Technology Research & Management, vol. 4, issue 3, pp. 144-153, 2020.

[63]. 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.

