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. 5, May 2023, pg.32 – 53

Complex CLMM Private Keys to Secure Digital Color Images

Prof. Ziad AlQadi
Albalqa Applied University, Jordan Amman
DOI: https://doi.org/10.47760/ijcsmc.2023.v12i05.005

Abstract:
Color digital images are one of the most widespread and widely used types of data, and the image can be secret or of a special nature, or it can be a carrier of confidential data, which makes protecting it very important. In this research, a new method for protecting color digital images will be presented, and the ease of implementing this method and its suitability for any digital image will be shown. The proposed method will provide a high degree of security and provide a high degree of protection for the digital image through the use of a complex private key based on chaotic logistic map model, six chaotic key will be used to form six integer keys, and these keys will be resized to match the dimensions of each color channel. The proposed method will use two rounds of data cryptography; each round will require three private keys, one for each color. Different variations of CLMM will be used to generate 1D and 2D chaotic keys, the results of using 1D chaotic keys will be compared with the results of using 2D chaotic keys and some recommendations will be raised. The proposed method will be implemented, different types of results analysis's (Quality analysis, sensitivity analysis, and throughput analysis) to improve the enhancement provided by yje proposed method comparing with other existing methods.

Keywords: CLMM, 1D chaotic, 2D chaotic key, private key, cryptography, MSE, PSNR, CC, throughput.

Introduction
Color digital images [13-15] are one of the most widely used and widely used types of data. And the digital image may be secret or personal of a special nature, or it may be carrying confidential data, which requires protecting it from the process of penetration by intruders, by data thieves, or by any unauthorized party [60-70].
Digital color image is presented by a three-dimensional matrix (a two-dimensional matrix for each of the three colors: red, green and blue), as shown in figure 1, each color matrix can be extracted and treated alone, the processed color matrices can be combined to form the processed color image [16-21].

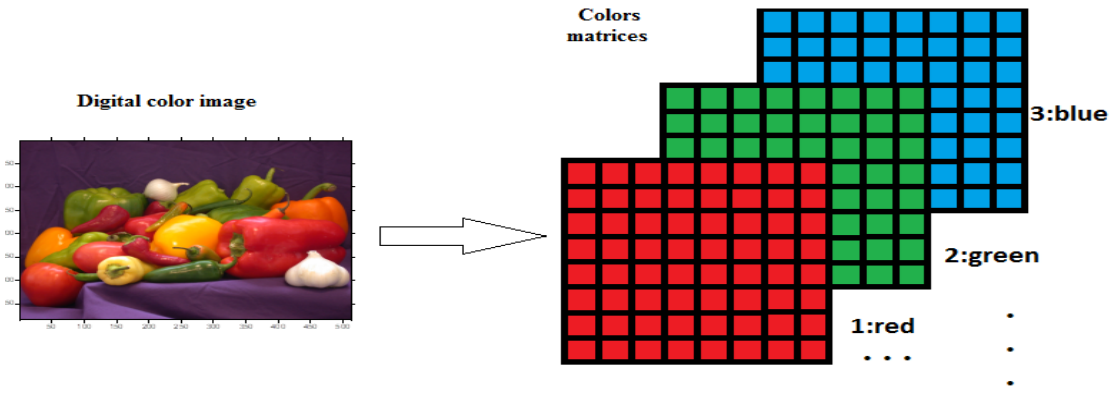

Figure 1: Color image representation

One of the popular methods of protecting images is image cryptography. Image cryptography means encryption the image before sending and decrypting it after receiving. Encryption and decryption usually done using secret (PK) (see figure 2), this key must provide a huge key space to prevent the process of key guessing or hacking [21-30].

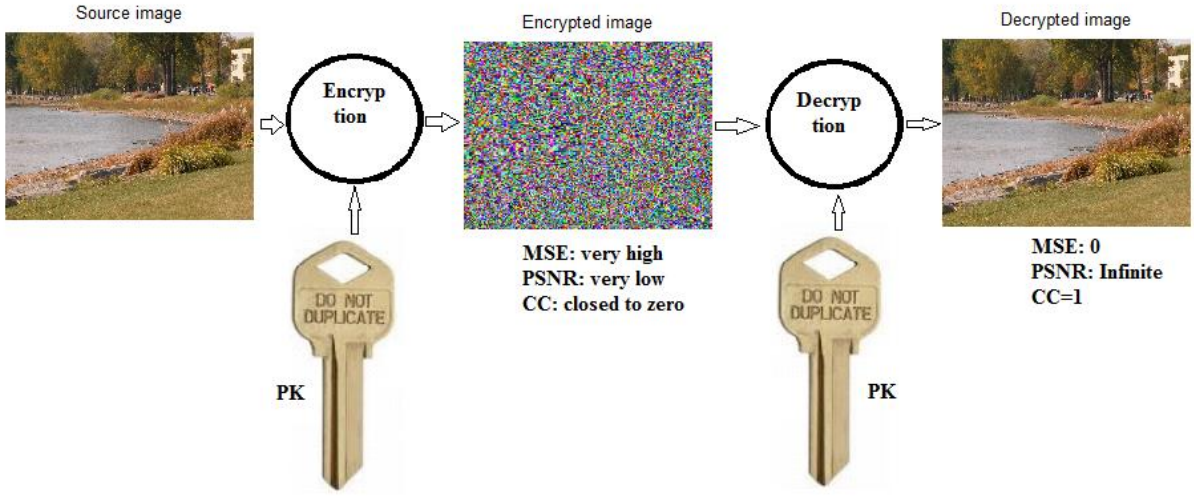

Figure 2: Color image cryptography process

A good method of cryptography must satisfy the following [17-20]:

- Simplicity: easy to use, and it must suit any image with any size.
- Security: The PK must provide a huge key spaces to prevent key guessing or hacking, also the PK must be sensitive to any minor changes in the PK components, any change in the PK components in the decryption phase must be considered as a hacking attempt by producing a corrupted, damaged decrypted data.
- Efficiency: minimizing the encryption-decryption times, thus maximizing the process of cryptography throughput (bytes encrypted-decrypted per second) [41-50].
- Quality: The method must give good values for quality parameters measured between the source image and the encrypted one after processing the encryption phase, and between the source image and the decrypted one after processing the decryption phase [31-40]. The quality parameters used in this research are: Mean square error (MSE), peak signal to noise ratio (PSNR), and correlation coefficient (CC), these parameters can be calculated using equations 1, 2, and 3 [16].

MSE of x channel

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

Total MSE

$$MSE_t = MSE_R + MSE_G + MSE_B$$

Calculate PSNR

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

$$\mathbf{cc} = \frac{\sum (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum (x_i - \bar{x})^2 \sum (y_i - \bar{y})^2}} \quad (3)$$

Where:

cc = **correlation coefficient**

x_i = **values of first message**

$\bar{x}$ = **mean of x**

y_i = **values of second message**

$\bar{y}$ = **mean of y**

The encryption phase must totally destroy the image [51-60], while the decryption phase must recover the original image, this can be proved by the calculated values of the quality parameters. In the encryption phase the value of MSE must be very high, the value of PSNR must be very low, and CC must be closed to zero. In the decryption phase MSE must be zero, PSNR must be infinite, and CC must be equal 1.

Related Work

Data protection is a very important matter [61-70], which prompted many researchers to provide various methods of encryption with varying values in efficiency. Some methods were based on the standards DES, AES, 3DES and BF, these methods are good for small in size data, when the data size increased (as an image), these methods became inefficient, and table 1 shows the throughputs of these standard methods [1]:

Table 1: Throughput of standard methods

	DES	3DES	AES	BF
Throughput(byte per second)	835	292	491	1038

In [2] the authors made performance comparisons between chaotic and non-chaotic methods of data cryptography, the final results of comparisons are shown in table 2.

Table 2 : Cryptography methods performance comparisons [2]

Method	Throughput(K bytes per second)
Non-chaotic approach	170.3906
Chaotic approach	141.2305
Hyper Chaotic approach	636.3379

Some other authors introduced methods which enhanced the throughput, in [8] the authors introduced a method , the throughput was enhanced to reach 169.1 K bytes per second, while in [9] the introduced method enhanced the throughput to reach 710 K bytes per second.

In [3] the authors provided a robust and fast image encryption scheme based on a mixing technique. In [4] the authors provided cosine-transform-based chaotic system for image encryption, while in [5] the authors introduced a novel image encryption algorithm based on polynomial combination of chaotic maps and dynamic function generation. In [6] the authors introduced Multiple-image Encryption Algorithm Based on DNA Encoding and Chaotic System, while in [7] the authors produced a multiple-image encryption with bit-plane decomposition and chaotic maps, these methods provided good quality a have various speeds as shown in table 3

Table 3 : Performance comparisons of method mentioned in [3-7]

Method	Throughput(K bytes per second)
In [3]	888.8867
In [4]	638.4082
In [5]	911.0352
In [6]	360.4102
In [7]	384.9609

The Proposed Method

The proposed method is based on using chaotic logistic map model to generate needed PKs for color image cryptography.

The chaotic logistic map (CLM) function is calculated by equation 4 [10-12]:

$$X_{n+1} = r \cdot X_n \cdot (X_n - 1) \quad (4)$$

Where Xn is the first chaotic logistic parameter that ranges from 0 to 1, r is the second chaotic logistic parameter that ranges from 0 to 4. The behavior of the chaotic logistic map depends on the selecting value of r, so, when r is equal to [3-6]:

- 0 to 1, the chaotic function generates fixed and stable values near to zero.
- 1 to 3, the function generates a fixed and stable values near to (r-1)/r).
- 3 to 3.7, the function generates values with periodic attractor.
- 3.7 to 4, the function acts as a chaotic function.

In the proposed method we will use the ranges: $3.5<r<4$ and $0<x<1$.

CLMM can be used to generate 1D chaotic key, this key can be easily converted to integer key and can be resized to any image dimensions, figure 3 shows the sequence of operations required to use CLMM to generate a PK:


```
R=200;r1=3.9;x1=0.025;  % CLMM parameters
for i=1:R
    x1=r1*x1*(1-x1);
    k12(i)=x1;          %CLMM key
end
k1=uint8(255*k12);   %Integer key
key=imresize(k1,[n1 n2])  % n1 and n2 are color channel dimensions
```

Figure 3: Key generation process

Figure 4 shows example outputs of implementing CLMM:

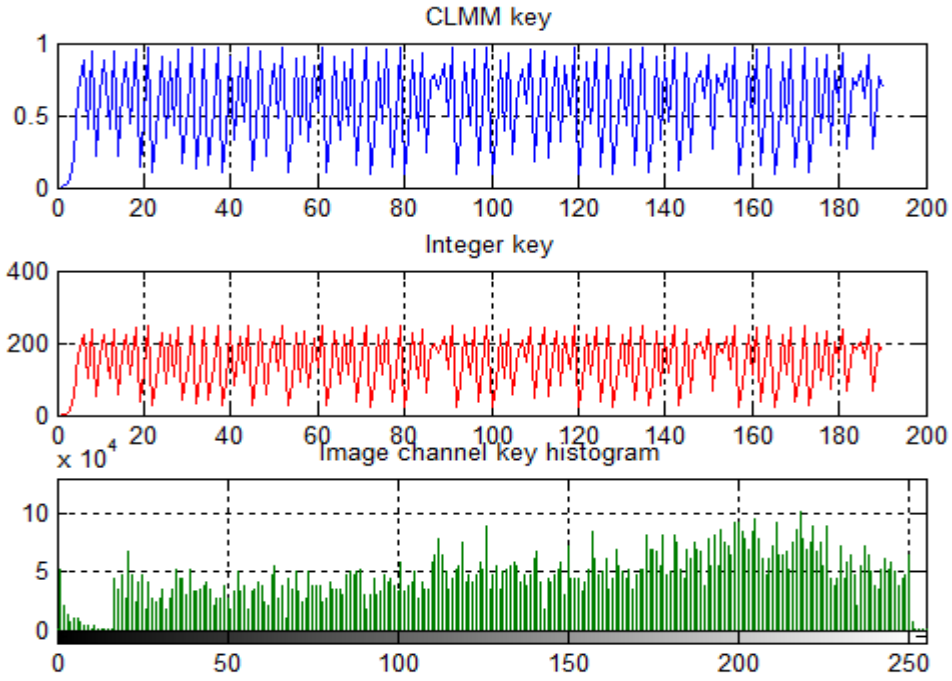

Figure 4: Example of using 1D CLMM key

For performance analysis we will use also CLMM to produce 2D CLMM key, this key can be converted to integer and resized to match the color matrix size, figure 5 shows the sequence of operations required to produce 2D CLMM key, while figures 6 and 7 show sample outputs:

```
R=10;C=12;r1=3.95;x1=0.005;
for i=1:R
   for j=1:C
      x1=r1*x1*(1-x1);
      k15(i,j)=x1;
   end
   x1=x1+0.001;
end
k4=uint8(255*k15)
```

Figure 5: 2D key generation process

0.0197	0.0761	0.2777	0.7923	0.6500	0.8987	0.3597	0.9098	0.3242	0.8654	0.4600	0.9812
0.0692	0.2543	0.7491	0.7424	0.7555	0.7297	0.7791	0.6798	0.8598	0.4762	0.9853	0.0574
0.2171	0.6714	0.8715	0.4424	0.9744	0.0986	0.3510	0.8998	0.3561	0.9057	0.3374	0.8831
0.4049	0.9518	0.1813	0.5864	0.9580	0.1588	0.5276	0.9845	0.0603	0.2240	0.6865	0.8500
0.5007	0.9875	0.0488	0.1832	0.5911	0.9547	0.1709	0.5597	0.9734	0.1021	0.3622	0.9125
0.3121	0.8480	0.5091	0.9872	0.0500	0.1877	0.6022	0.9462	0.2010	0.6343	0.9163	0.3030
0.8358	0.5422	0.9805	0.0757	0.2762	0.7897	0.6560	0.8914	0.3824	0.9329	0.2473	0.7352
0.7671	0.7058	0.8202	0.5824	0.9607	0.1492	0.5015	0.9875	0.0488	0.1833	0.5914	0.9545
0.1679	0.5517	0.9769	0.0890	0.3204	0.8600	0.4754	0.9851	0.0579	0.2155	0.6678	0.8763
0.4252	0.9654	0.1319	0.4522	0.9785	0.0832	0.3013	0.8315	0.5534	0.9762	0.0917	0.3289

Figure 6: 2D CLMM key

5	19	71	202	166	229	92	232	83	221	117	250
18	65	191	189	193	186	199	173	219	121	251	15
55	171	222	113	248	25	90	229	91	231	86	225
103	243	46	150	244	40	135	251	15	57	175	217
128	252	12	47	151	243	44	143	248	26	92	233
80	216	130	252	13	48	154	241	51	162	234	77
213	138	250	19	70	201	167	227	98	238	63	187
196	180	209	149	245	38	128	252	12	47	151	243
43	141	249	23	82	219	121	251	15	55	170	223
108	246	34	115	250	21	77	212	141	249	23	84

Figure 7: 2D integer key

Generating CLMM key requires a processing time (generation time), this time will rapidly increases when increasing the length of CLMM key, so it is recommended to use a medium size of CLMM key to save the total time needed to image cryptography and thus to increase the method throughput, table 4 shows the generation time needed to generate various lengths CLMM key, while figure 8 shows the generation time increasing:

Table 4: CLMM key generation time

Key length(element)	Generation time(second)
100	0.0010
200	0.0013
400	0.0040
600	0.006000
800	0.009000
1000	0.014000
2000	0.050000
4000	0.057000
5000	0.062000
10000	0.104000
50000	1.395000
100000	10.744000

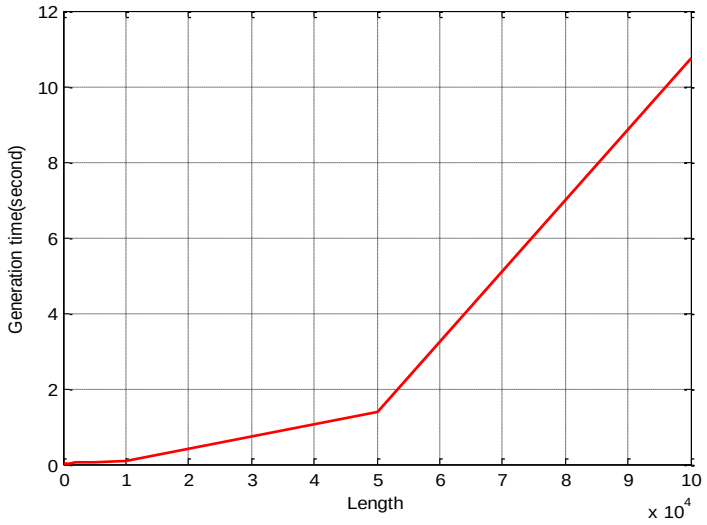

Figure 8: CLMM generation time VS key length

The proposed method will use two rounds of image cryptography; each round requires 3 keys, so the total number of required keys is six. The information required to generate the needed keys is included in the PK, which will have a complicated structure to prevent any hacking attempts, the structure of the first form of PK to generate 1D CLMM keys is shown in figure 9, while the structure of the second form of PK to generate 2D CLMM keys is shown in figure 10.

Round 1								
Key 1			Key 2			Key 3		
R1	r1	x1	R2	r2	x2	R3	r3	x3
Round 2								
Key 4			Key 5			Key 6		
R4	r4	x4	R5	r5	x5	R6	r6	x6

Figure 9: 1D PK structure

Round 1											
Key 1				Key 2				Key 3			
R1	C1	r1	x1	R2	C2	r2	x2	R3	C3	r3	x3
Round 2											
Key 4				Key 5				Key 6			
R4	C4	r4	x4	R5	C5	r5	x5	R6	C6	r6	x6

Figure 10: 2D PK structure

The proposed method includes the following tasks to apply color image encryption-decryption.

1) Using 6 CLMM to generate 6 CLMM keys.
2) Converting keys to integers
3) Resizing the keys to match the color matrix size.
4) Apply XORing each color matrix with the associated key (as shown in figures 11 and 12)

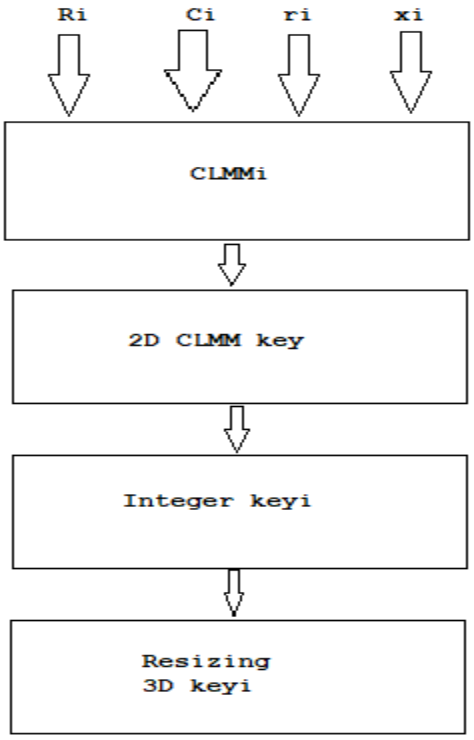

Figure 11: 2D keys generation

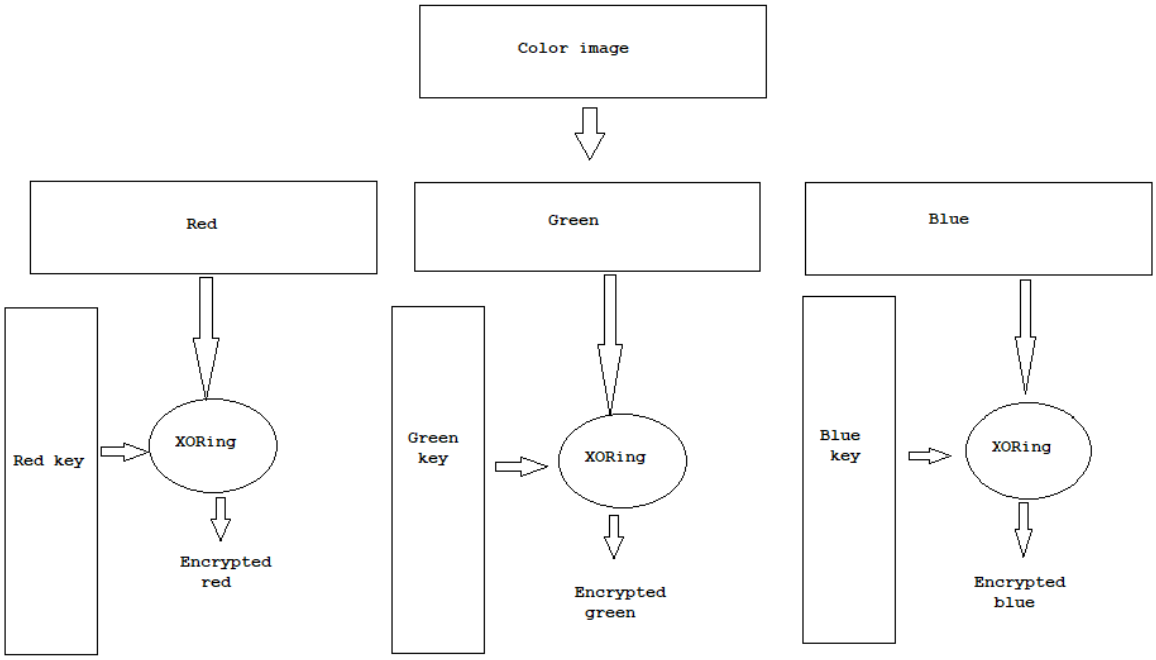

Figure 12: Encryption phase (1 round)

The encryption phase can be implemented applying the following algorithm:

Inputs

Color image to be encrypted, PK

Output

Decrypted color image

Process

1) *Get the color image*
2) *Extract each color channel matrix*
3) *Retrieve color matrix dimensions*
4) *Get the PK*
5) *Apply CLLMs to get 6 CLMM keys.*
6) *Convert the CLMM keys to integer.*
7) *Resize each integer key to match the color matrix size.*
8) *Apply round 1 by XORing each color matrix with the associated key (key1, key 2 and key3)*
9) *Apply round 2 by XORing each of the resulting color matrix obtained in step 8 by the associated key (key 4, key 5 and key 6) to get the encrypted colors.*
10) *Combine the three colors obtained in step 9 in one 3D matrix to get the encrypted color image.*

The decryption phase can be executed using the same sequence, the same PK must be used and the input image is the encrypted image.

Implementation and Results Analysis

The image "sampleMerry_0055_Lasalle.jpg" was encrypted-decrypted using the proposed method, figures 13, 14, and 15 show sample outputs of the implementation:

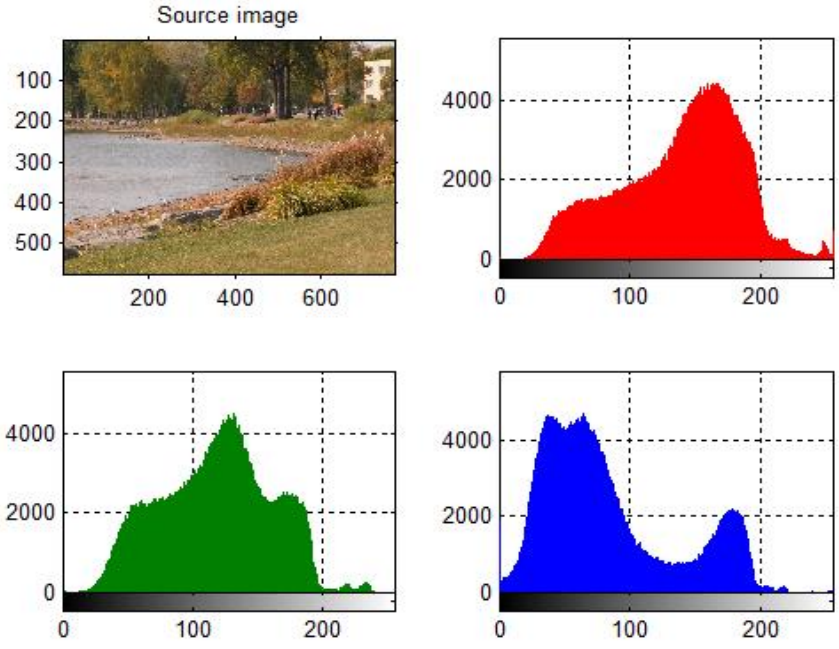

Figure 13: Sample input image (sampleMerry_0055_Lasalle.jpg)

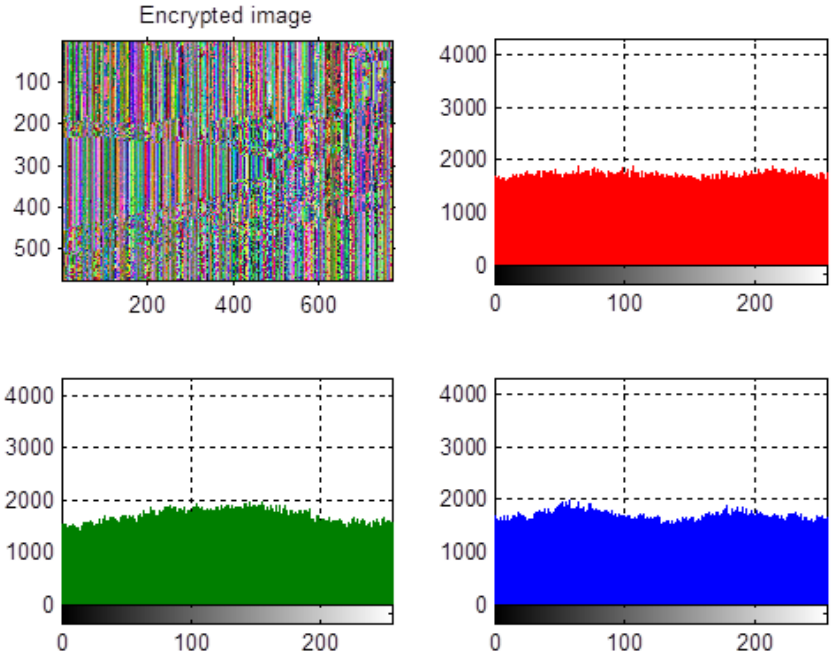

Figure 14: Sample encrypted image

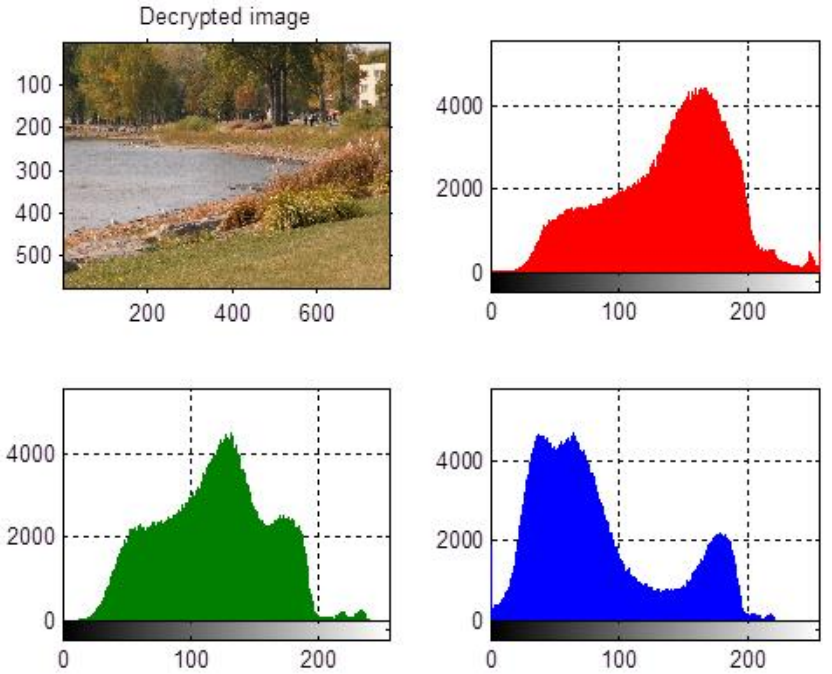

Figure 15: Sample decrypted image

The proposed method will be implemented using the 10 selected images shown in figure 16:

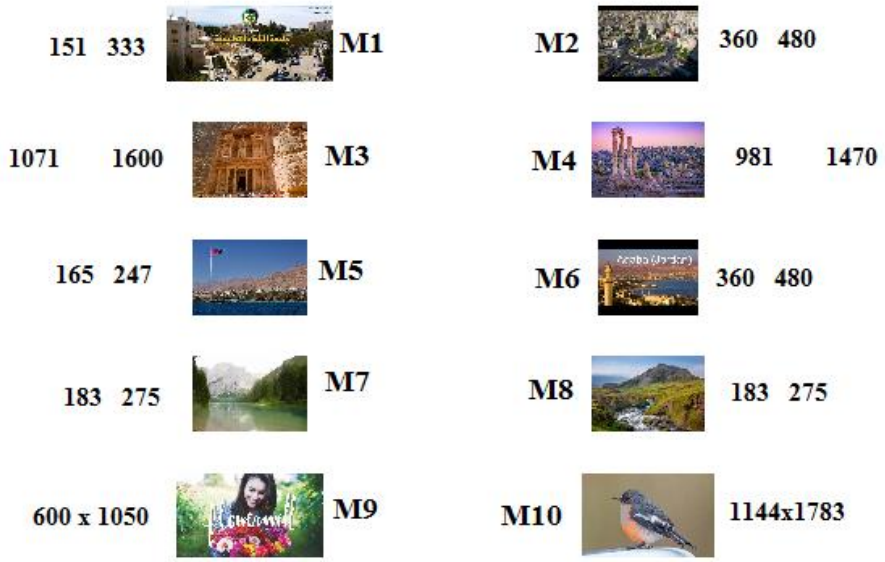

Figure 16: Selected used color images

1) Quality analysis

The selected images were treated using the proposed method, 1D PK shown in I figure 17 was used:

CLMM1	CLMM2	CLMM3
R=190;r1=3.9;x1=.001;	R=180;r1=3.9;x1=.011;	R=200;r1=3.9;x1=.01;
CLMM4	**CLMM5**	**CLMM6**
R=140;r1=3.9;x1=.02;	R=150;r1=3.9;x1=.021;	R=170;r1=3.9;x1=.029;

Figure 17: Used PK to generate 1D key

The calculated quality parameters between the input and the decrypted images were: MSE=0, PSNR=infinite, which means that the decrypted images were identical to the input ones.

Table 5 shows the calculated quality parameters values between the input images and the encrypted images.

Table 5: Quality of the encrypted images (using 1D keys)

Image	MSE	PSNR
1	12364	16.5997
2	10362	18.3660
3	9197.2	19.5587
4	9175.4	19.5825
5	7989.5	20.9665
6	11526	17.3014

7	10536	18.1997
8	8654.3	20.1672
9	11447	17.3708
10	6950.3	22.3599

From table 5 we can see that MSE always high and PSNR always low for any image with any size, this means that the proposed method satisfies the requirements of good image cryptography.

The PK shown in figure 18 was used to encrypt-decrypt the selected images, table 6 shows the obtained quality parameters between the input and encrypted images.

CLMM1

R=70;C=80;r1=3.9;x1=0.025;

CLMM2

R=100;C=100;r1=3.99;x1=0.012;

CLMM3

R=50;C=60;r1=3.97;x1=0.009;

CLMM4

R=45;C=75;r1=3.95;x1=0.005;

CLMM5

R=90;C=100;r1=3.91;x1=0.0092;

CLMM6

R=75;C=90;r1=3.89;x1=0.027;

Figure 18: PK to generate 2D keys

Table 6: Quality of the encrypted images (using 2D keys)

Image	MSE	PSNR
1	12603	16.4083
2	10866	17.8912
3	9502.7	19.2319
4	94097	19.3304
5	8163.3	8163.3
6	11933	16.9549
7	11027	17.7443
8	9329.4	19.4160
9	11328	17.4747
10	6924.3	22.3974

The obtained results shown in table 6 also prove that the proposed method provides a good quality, this can be seen in the sample outputs shown in figures 19, 20 and 21:

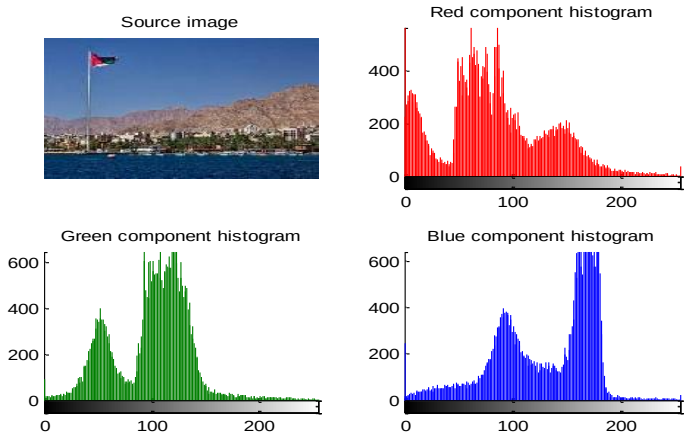

Figure 19: Image 5 example

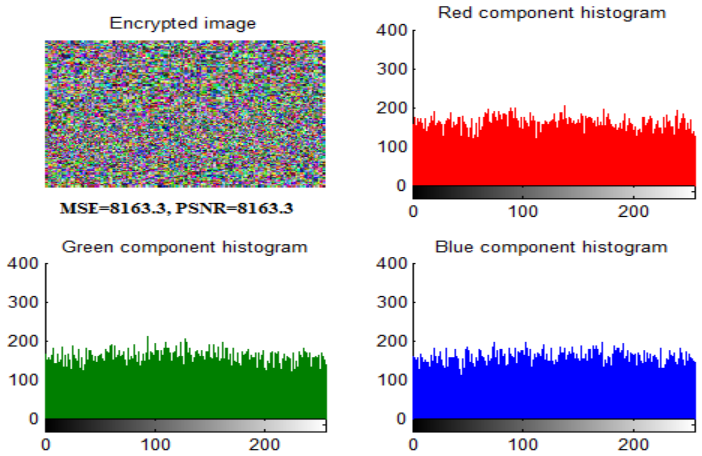

Figure 20: Encrypted image 5 example

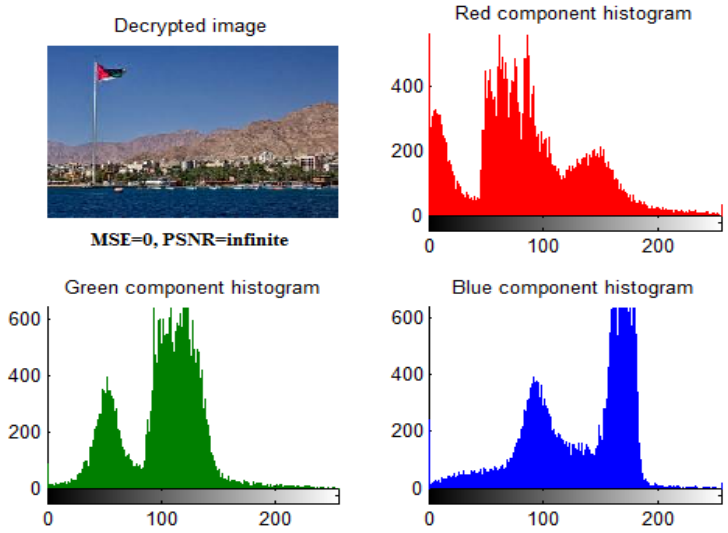

Figure 21: Decrypted image 5 example

2) Statistical analysis

The selected images were treated using the proposed method, first we use the PK shown in figure 17, and then the PK shown in figure 18 was used. In both cases the calculated values of CC between the input images and the decrypted ones were always equal 1, which means that the method after decryption recovers the input image. Tables 7 and 8 shows the calculated values of CC between the input and the encrypted images:

Table 7: Calculated CCs using first PK

Image	CC red	CC green	CC blue
1	0.0263	0.0701	-0.0039
2	0.0369	0.1186	0.0126
3	0.0095	0.0500	0.0146
4	0.0040	0.0764	0.0214
5	0.0231	0.0586	0.0045

6	0.0212	0.0965	0.0101
7	0.0030	0.1167	0.0631
8	0.0435	0.0820	0.0652
9	0.0101	0.0872	0.0516
10	-0.0072	0.0279	0.0042

Table 8: Calculated CCs using second PK

Image	CC red	CC green	CC blue
1	0.0192	0.0178	0.0154
2	0.0126	0.0046	0.0145
3	0.0089	0.00038515	0.0076
4	0.0169	-0.0051	0.0089
5	0.0118	0.0053	0.0101
6	0.0058	0.0081	0.0191
7	0.0217	0.0010	0.0185
8	0.0044	0.0090	0.0112
9	0.0211	0.0104	0.0120
10	0.0032	0.0057	0.0037

Tables 7 and 8 show that CC values always closed to zero (very low), this means that images were fully destructed in the decryption phase, and the proposed method satisfies the requirement of good cryptography.

3) Efficiency analysis

Doing this analysis we calculated the encryption and decryption times provided by the proposed method, then the throughputs were calculated, tables (9 and 10) show the obtained results using 1D and 2D keys:

Table 9: Efficiency parameters (Using 1D key)

Image	Encryption time(second)	Throughput (K byte per second)	Throughput (M byte per second)
1	0.0740	1991.1	1.9444
2	0.0677	7475.0	7.2998
3	0.2058	24393	23.8213
4	0.1805	23401	22.8525
5	0.0575	2075.5	2.0269
6	0.0697	7261.6	7.0914
7	0.0552	2672.5	2.6099
8	0.0556	2649.4	2.5873
9	0.0560	2637.7	2.5759
10	0.2359	25328	24.7344
Average		9988.5	

Table 10: Efficiency parameters (Using 2D key)

Image	Encryption time(second)	Throughput (K byte per second)	Throughput (M byte per second)
1	0.0930	1584.0	1.5469
2	0.1260	4017.9	3.9237
3	0.3200	15688	15.3203
4	0.2460	17174	16.7715
5	0.1460	817.8042	0.7986
6	0.1100	4602.3	4.4944
7	0.1530	963.6374	0.9411
8	0.0970	1520.0	1.4844
9	0.1090	16933	16.5361
10	0.1430	41789	40.8096
Average		10509	

From tables 9 and 10 we can see that the proposed method provided an excellent throughput, the average throughput is better than any throughput provided by the best method listed in the related work section. From table 9 and 10 we can also see that using PK to generate 2D keys enhanced the efficiency keeping the quality acceptable, so we recommend this key, also this key will enhance the security level by expanding the key space.

4) Sensitivity analysis

The proposed method uses a PK key with components; these components are CLMM parameters, the parameters values are used to generate the needed keys for image cryptography, any minor changes in CLMM parameters values will lead to generate different keys. Changes done in the decryption phase will be considered as a hacking attempts and a damaged decrypted image will be produced. Figure 22 shows how the generated key is sensitive to any changes in CLMM parameters.

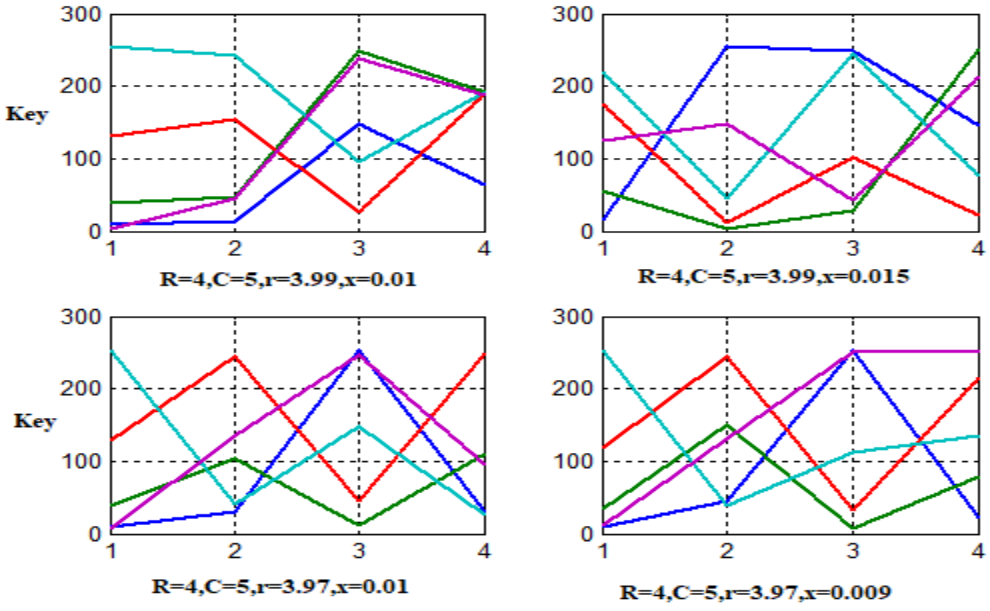

Figure 22: Generated key sensitivity

To prove the sensitivity effects of the proposed method image "sampleMerry_0055_Lasalle.jpg" was encrypted using the PK shown in figure 23

First round PK part

R=70;C=80;r1=3.9;x1=0.025;	R=100;C=100;r1=3.99;x1=0.012;	R=50;C=60;r1=3.97;x1=0.009;

Second round PK part

R=45;C=75;r1=3.95;x1=0.005;	R=90;C=100;r1=3.91;x1=0.0092;	R=75;C=90;r1=3.89;x1=0.027;

Figure 23: PK used in the encryption phase (PK1)

Minor changes were applied and the PK shown in figure 24 was used in the decryption phase

First round PK part

R=70;C=80;r1=3.9;**x1=0.028;**	R=100;C=100;**r1=3.89**;x1=0.012;	R=50;**C=66**;r1=3.97;x1=0.009;

Second round PK part

R=45;C=75;r1=3.95;x1=0.005;	R=90;C=100;r1=3.91;x1=0.0092;	R=75;C=90;r1=3.89;x1=0.027;

Figure 24: PK used in the Decryption phase (PK2)

Figures 25, 26, 27 and 28 show the obtained outputs:

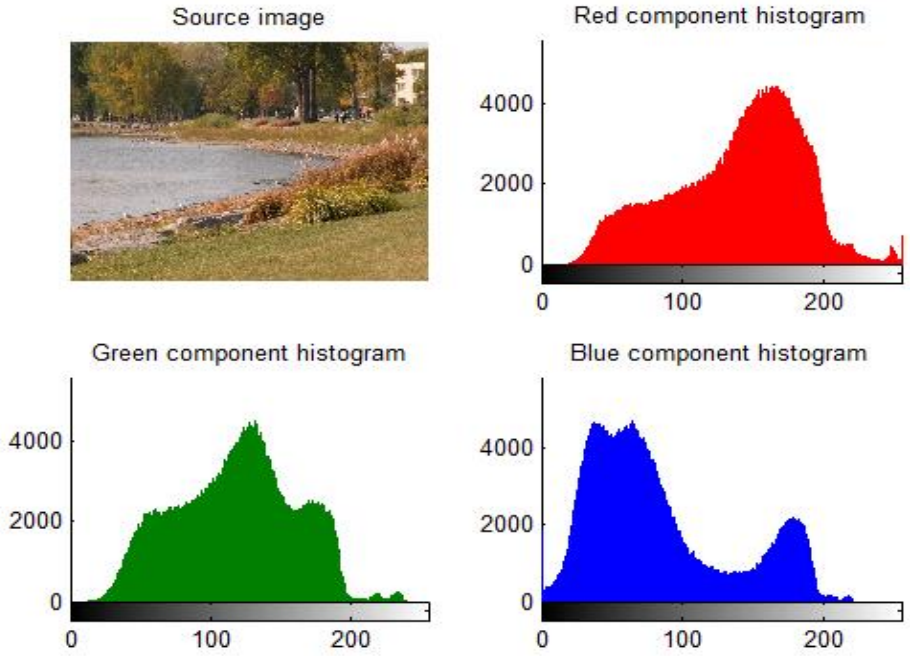

Figure 25: Image to be encrypted

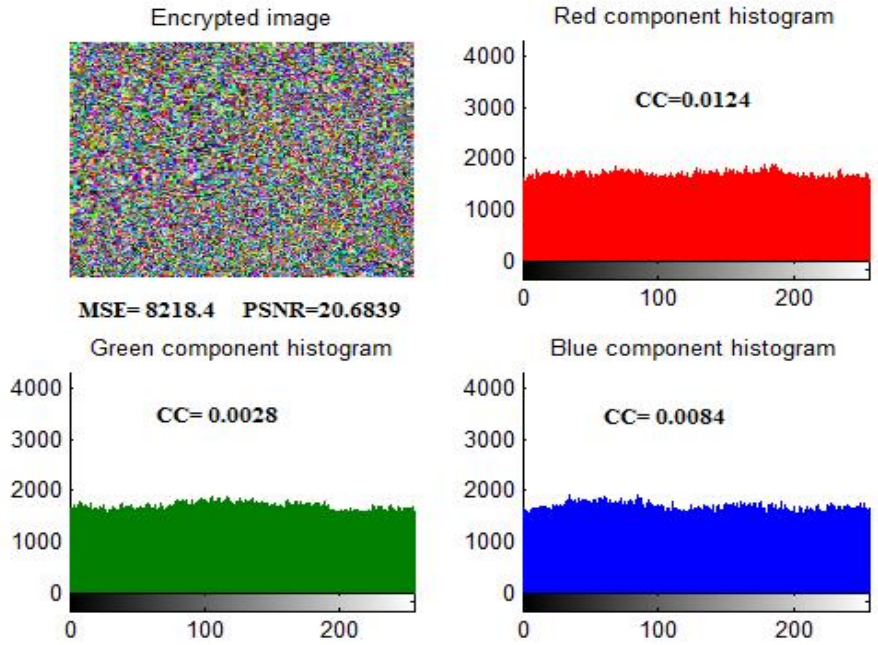

Figure 26: Encrypted image using PK 1

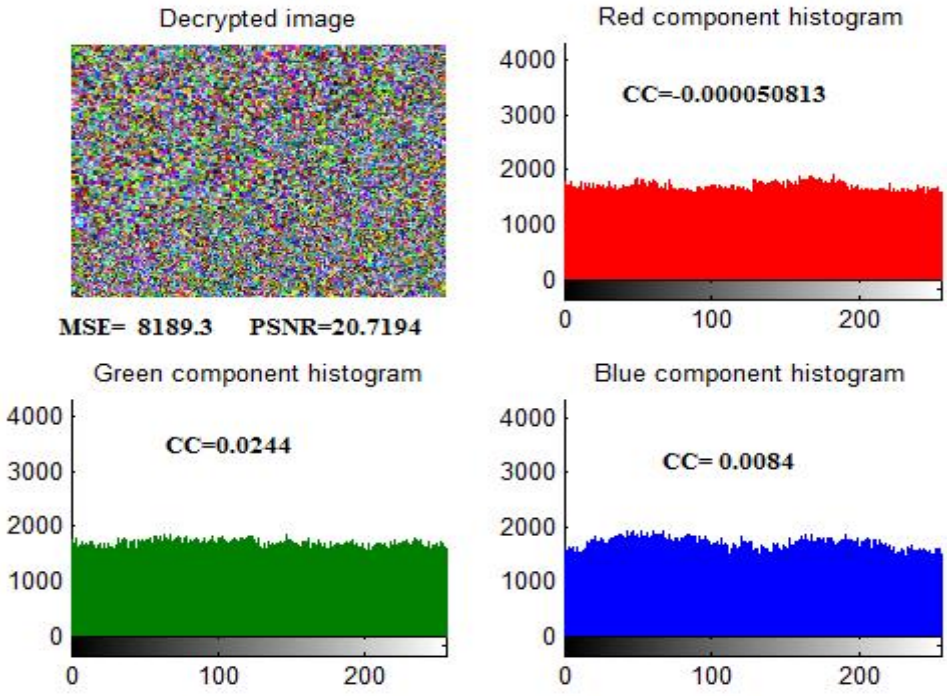

Figure 27: Decrypted image using PK2

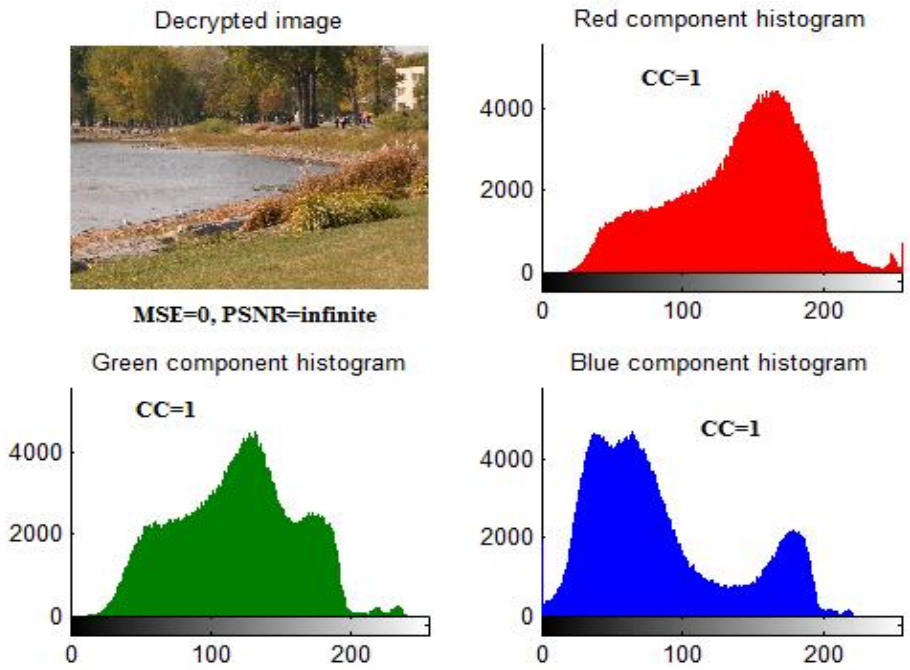

Figure 28: Decrypted image using PK1

From figure 27 we can see making any changes in the PK will produce a corrupted damaged image, the changes in the PK in the decryption phase will be wrong PK and will be considered as a hacking attempt.

5) Security analysis

The proposed method uses a complicated complex structure; this will increase the key space and prevent any hacking process.

The PK contains 24 components with double data type, each component requires 64 bits to represented, so the available number combinations for each component is equal 2^{64} and the key space will equal:

$$\textbf{Key space=} \ (2^{64})^{24} = 2^{1536}$$

6) Simplicity analysis

The proposed method is very simple and easy to implement. The method can be used for image cryptography; the image can be with any size. PK can be changed from time to time without any need to change the method operations, changing the image also does not require any change in sequence of operations, the proposed method can be implemented using any programming language, in this research the method was programmed using matlab, and for researchers who want to reproduce the outputs the following code can be used:

```
clear all,close all
%Get the image
a = imread('C:\Users\win 7\Desktop\sampleMerry_0055_Lasalle.jpg');
[n1 n2 n3]=size(a);
```


Round 1 keys generation

```
tic
R=70;C=80;r1=3.9;x1=0.025;
for i=1:R
   for j=1:C
      x1=r1*x1*(1-x1);
      k12(i,j)=x1;
   end
   x1=x1+0.001;
end
k1=uint8(255*k12);
t1=toc;
```

```
tic
R=100;C=100;r1=3.99;x1=0.012;
for i=1:R
   for j=1:C
      x1=r1*x1*(1-x1);
      k13(i,j)=x1;
   end
   x1=x1+0.001;
end
k2=uint8(255*k13);
t2=toc;
```

```
tic
R=50;C=60;r1=3.97;x1=0.009;
for i=1:R
   for j=1:C
      x1=r1*x1*(1-x1);
      k14(i,j)=x1;
   end
   x1=x1+0.001;
end
k3=uint8(255*k14);
t3=toc;
```

Round 2 key generation

```
tic
R=45;C=75;r1=3.95;x1=0.005;
for i=1:R
   for j=1:C
      x1=r1*x1*(1-x1);
      k15(i,j)=x1;
   end
   x1=x1+0.001;
end
k4=uint8(255*k15);
t4=toc;
```

```
tic
R=90;C=100;r1=3.91;x1=0.0092;
for i=1:R
   for j=1:C
      x1=r1*x1*(1-x1);
      k16(i,j)=x1;
   end
   x1=x1+0.001;
end
k5=uint8(255*k16);
t5=toc;
```

```
tic
R=75;C=90;r1=3.89;x1=0.027;
for i=1:R
   for j=1:C
      x1=r1*x1*(1-x1);
      k12(i,j)=x1;
   end
   x1=x1+0.001;
end
k6=uint8(255*k12);
t6=toc;
```

Keys resizing and encryption

```
tic
imk1(:,:,1)=imresize(k1,[n1 n2]);
imk1(:,:,2)=imresize(k2,[n1 n2]);
imk1(:,:,3)=imresize(k3,[n1 n2]);
imk2(:,:,1)=imresize(k4,[n1 n2]);
imk2(:,:,2)=imresize(k5,[n1 n2]);
imk2(:,:,3)=imresize(k6,[n1 n2]);
en1=bitxor(a,imk1);
en=bitxor(en1,imk2);
tren=toc
```

Conclusion

A simple and easy to implement method of image cryptography was proposed, this method can be used to encrypt-decrypt any color image without needing any modifications in method operations. It was shown that the proposed method was very secure and it can prevent hacking and it increases the image protection degree. The method uses a PK with complex structure; the components of the PK are various CLMM parameters. The proposed PK is very sensitive to any changes in any PK component and provides a huge key space making the hacking process impossible.

The proposed method was implemented using various images, the obtained results were analyzed using various types of analysis's (quality, statistical, sensitivity, security and efficiency analyses) , and it was proved that the proposed method satisfied the quality requirements by giving excellent values of MSE, PSNR and CC in both the encryption and decryption phases.

The obtained results proved that the proposed method is very efficient by maximizing the throughput of image cryptography; the proposed method gave an average throughputs better than the existing methods of image cryptography.

References

[1]. Aamer Nadeem, Dr M. Younus Javed, A Performance Comparison of Data Encryption Algorithms, Conference Paper · September 2005 DOI: 10.1109/ICICT.2005.1598556 · Source: IEEE Xplore.

[2]. M. Bala Kumara, P. Karthikkab , N. Dhivyac , T. Gopalakrishnan, A Performance Comparison of Encryption Algorithms for Digital Images, International Journal of Engineering Research & Technology (IJERT), Vol. 3 Issue 2, February – 2014.

[3]. Lee Mariel Heucheun Yepdia, Alain Tiedeu, and Guillaume Kom, A Robust and Fast Image Encryption Scheme Based on a Mixing Technique, Security and Communication Networks, Volume 2021 |Article ID 6615708 | https://doi.org/10.1155/2021/6615708

[4]. Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Information Sciences*, vol. 480, pp. 403–419, 2019.

[5]. M. Asgari-chenaghlu, M.-A. Balafar, and M.-R. Feizi-Derakhshi, "A novel image encryption algorithm based on polynomial combination of chaotic maps and dynamic function generation," *Signal Processing*, vol. 157, p. 1, 2019.

[6]. X. Zhang and X. Wang, *Multiple-image Encryption Algorithm Based on DNA Encoding and Chaotic System*, Springer, New York, NY, USA, 2019.

[7]. J. S. Zhenjun and R. Sun, "Multiple-image encryption with bit-plane decomposition and chaotic maps," *Optics and Lasers in Engineering*, vol. 80, pp. 1–11, 2016.

[8]. Bhattacharjee S, Gupta M, Chatterjee B. Time Efficient Image Encryption-Decryption for Visible and COVID-19 X-ray Images Using Modified Chaos-Based Logistic Map. Appl Biochem Biotechnol. 2023 Apr;195(4):2395-2413. doi: 10.1007/s12010-022-04161-7. Epub 2022 Sep 24. PMID: 36152105; PMCID: PMC9510176

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

[10]. Ziad AA Alqadi, Musbah Aqel, Ibrahiem MM El Emary, Multiple Skip Multiple Pattern Matching Algorithm (MSMPMA), IAENG International Journal of Computer Science, vol. 34, issue 2, IJCS_34_2_03, 2017.

[11]. Raqqad, Ziad Alqadi, Securing Message Steganography by using Modified LSB Method, International Journal of Computer Science and Mobile Computing, vol. 12, issue4.13, pp. 110 – 124, 2023.

[12]. 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, pp. 20-33, 2019.

[13]. Dr Rushdi S Abu Zneit, Dr Ziad AlQadi, Dr Mohammad Abu Zalata, A Methodology to Create a Fingerprint for RGB Color Image, IJCSMC, vol. 6, issue 1, pp. 205-212, 2017.

[14]. 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

[15]. Dr. Mohammed Abbas Fadhil Al-Husainy**,** COMPARISON STUDY BETWEEN CLASSIC-LSB, SLSB AND DSLSB IMAGE STEGANOGRAPHY**,** ICIT 2013 The 6th International Conference on Information Technology**,** http://icit.zuj.edu.jo/icit13/Papers%20list/Camera_ready/Computers%20and%20Networks%20Security/713_final.pdf

[16]. 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**.**

[17]. 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**.**

[18]. 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.

[19]. 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

[20]. 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.
[21]. Waheeb, A. and Ziad AlQadi, 2009. Gray image reconstruction, Eur. J. Sci. Res., 27: 167-173.
[22]. 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
[23]. 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
[24]. 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.
[25]. 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.
[26]. 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.
[27]. Z Alqadi, A Abu-Jazzar, Analysis of program methods used in optimizing matrix multiplication, Journal of Engineering, 2005
[28]. 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.
[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, Vol. 96. No. 13, pp. 4081-4091, 2018.
[30]. 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.
[31]. 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.
[32]. 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
[33]. 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
[34]. 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.
[35]. 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
[36]. 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
[37]. 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
[38]. 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.
[39]. 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.
[40]. 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.
[41]. 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.
[42]. 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.
[43]. 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.
[44]. 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.
[45]. 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.
[46]. 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.

[47]. 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.
[48]. 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.
[49]. 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.
[50]. 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.
[51]. 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.
[52]. 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.
[53]. 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.
[54]. Ziad alqadi, Analysis of stream cipher security algorithm, Journal of Information and Computing Science, vol. 2, issue 4, pp. 288-298, 2007.
[55]. 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.
[56]. 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.
[57]. 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.
[58]. 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.
[59]. 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.
[60]. 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.
[61]. 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.
[62]. Ashraf Abu-Ein, Ziad AA Alqadi, Jihad Nader, A TECHNIQUE OF HIDING SECRETE TEXT IN WAVE FILE, International Journal of Computer Applications, 2016
[63]. 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.
[64]. 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.
[65]. 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.
[66]. 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.
[67]. 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
[68]. 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.
[69]. 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.
[70]. M Mua'ad, Khaled Aldebei, Ziad A Alqad, Simple, Efficient, Highly Secure, and Multiple Purposed Method on Data Cryptography, Traitement du Signal, vol. 39, issue 1, pp. 173-178, 2022.

