Available Online at www.ijcsmc.com/journal

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 11, Issue. 11, November 2022, pg.180 – 199

Digital Image Cryptography using Lookup Table

Dr. Dojanah "Mohammad Kadri" Bader; Prof. Ziad Alqadi

Albalqa Applied University
Jordan Amman
DOI: https://doi.org/10.47760/ijcsmc.2022.v11i11.015

Abstract: Protecting digital images is an important task, because images may be secret or may be contain valuable secret information. In this paper research a simple, efficient and high secure method of digital images protection will be introduced. The method will use a chaotic logistic map model with a selected chaotic parameter to generate a lookup table, which will be used in the encryption and decryption phases. The proposed method can use one lookup table to encrypt-decrypt color images, or it can use three lookup tables to encrypt-decrypt each color channel. The method will secure the encrypted image by using a complicated private key, which will provide a suitable key space capable to resist hacking attacks, the method outputs will be very sensitive to the selected private key contents, any minor changes in these contents in the decryption phase will be considered as a hacking attempt by producing a damaged decrypted image. It will be shown how using lookup table simplifies the process of image cryptography using the indexes and the indexes contents of the lookup table. The proposed method will be implemented and the obtained results will be analyzed to prove the quality of encryption and decryption phases based on the calculated MSE, PSNR, CC and NSCR. The speed of the proposed method will be tested, to show how the proposed method will increase the throughput of data cryptography by decreasing both the encryption and decryption times.

Keywords: Cryptography, PK, CLK, CLMM, LUT, MSE, PSNR, CC, NSCR, TP.

Abbreviations

The following abbreviations will be used in this research paper:

PK: private key

CLK: chaotic logistic key

LUT: lookup table

CLMM: chaotic logistic map model

ET: encryption time

DT: decryption time

ETP: encryption throughput

DTP: decryption throughput

MSE: mean square error

PSNR: peak signal to noise ratio

CC: correlation coefficient

NSCR: number of samples change ratio

Introduction

Digital image [10-15] may be secret or may private or it can contain confidential information, they are used in many applications, and many of these applications require protecting the images from being hacked. In this paper research anew, simple, secure and efficient method of image cryptography will be introduced. This method will be used to encrypt-decrypt gray and color images with any type and size. The proposed method will use a lookup tables to apply encryption-decryption, these table will be generated by running a CLMM using a selected chaotic parameters values, which form the private key [16-22].

Digital color image is huge data set, which can be represented by a 3D matrix as shown in figure 1(one 2D matrix for each color: red, green and blue), the quality of the image can be examined by the image itself or by colors histograms as shown in figure 1 [23-30].

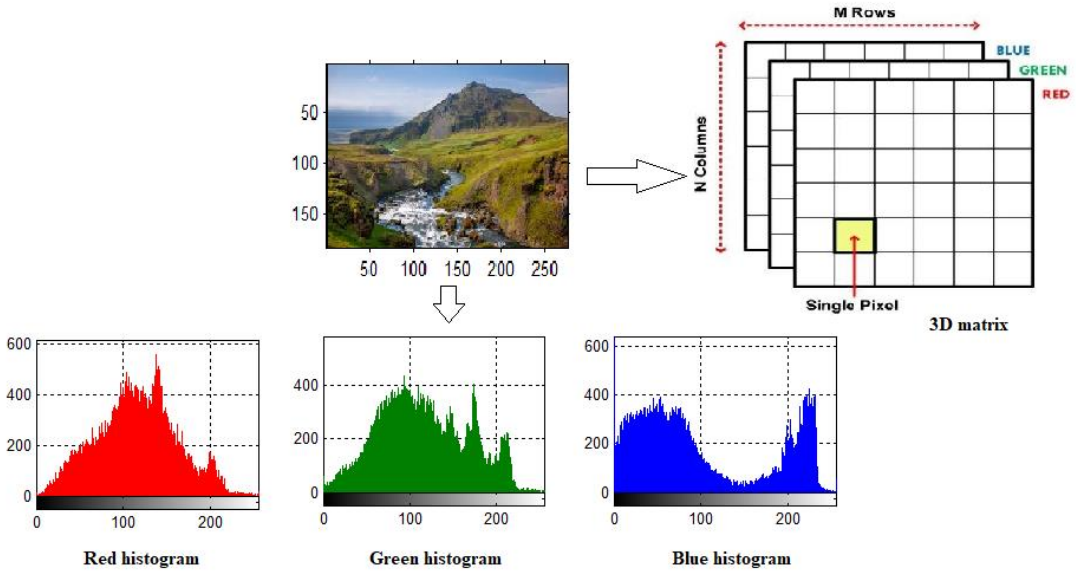

Figure 1: Image representation

Using the image matrix will simplify the process of image processing, and the color image has the following good features [31-36]:

- Color image can be processed as 3D matrix, or each color can be extracted and processed separately.
- Each color image contains a set of pixel as shown in figures 2 and 3, the pixel color ranges from 0 to 255, so we can create a lookup table with values from 0 to 255 to use it in the encryption and decryption phases [50-58].

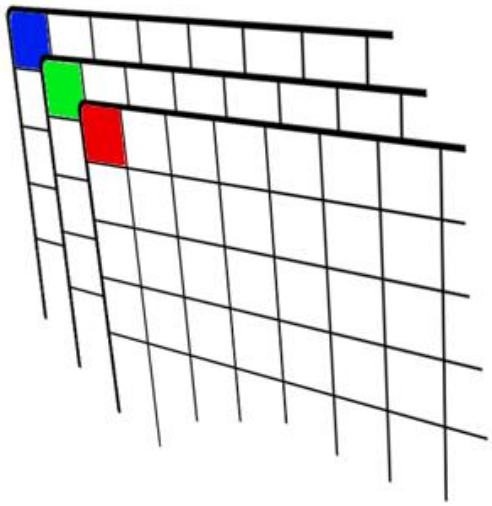

Figure 2: Color pixel

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 3: Pixels colors

Cryptography is the study of securing communications from outside observers. Encryption algorithms take the original image, or plaintext, and converts it into cipher image, which is not understandable [37-45]. The key allows the user to decrypt the image, thus ensuring on they can read the image. The strength of the randomness of an encryption is also studied, which makes it harder for anyone to guess the key or input of the algorithm (see figure 4). Cryptography is how we can achieve more secure and robust connections to elevate our privacy. Advancements in cryptography makes it harder to break encryptions so that encrypted files, folders, or network connections are only accessible to authorized users [46-50].

Cryptography focuses on four different objectives:

1. **Confidentiality**: Confidentiality ensures that only the intended recipient can decrypt the image and read its contents.

2. **Non-repudiation**: Non-repudiation means the sender of the image cannot backtrack in the future and deny their reasons for sending or creating the image.

3. **Integrity**: Integrity focuses on the ability to be certain that the information contained within the image cannot be modified while in storage or transit.

4. **Authenticity**: Authenticity ensures the sender and recipient can verify each other's identities and the destination of the image.

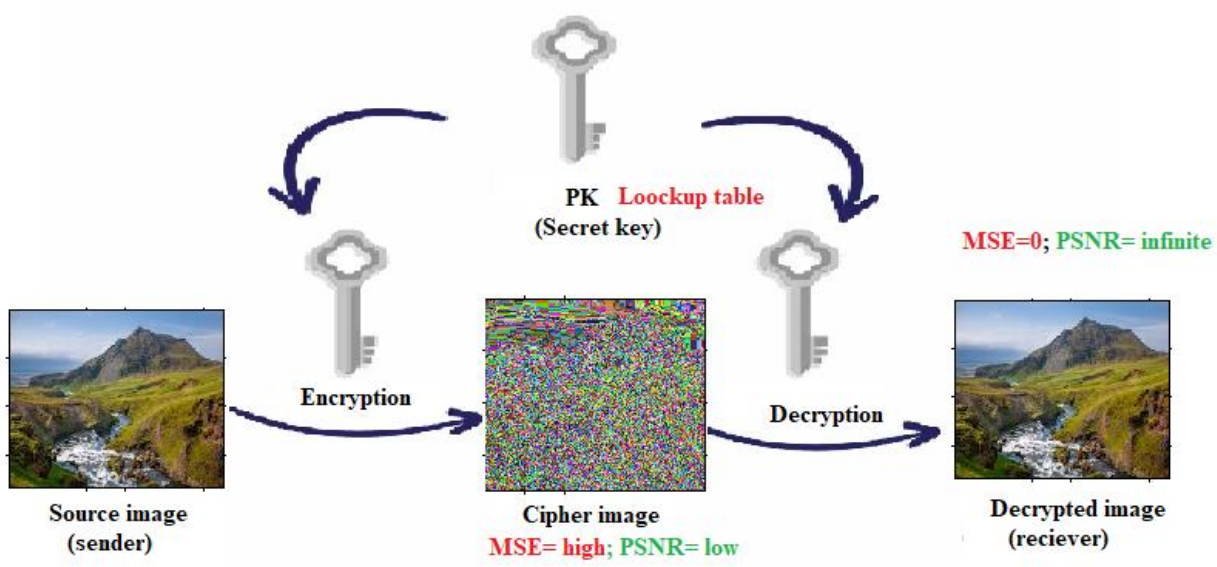

Figure 4: Image cryptography

A good method of image cryptography must satisfy the quality requirements by producing a damaged encrypted image and producing a decrypted image which is identical to the source image, thus the method must satisfy the requirements listed in table 1[58-65].

Table 1: Quality requirements

Quality parameter	Measured between source and encrypted images	Measured between source and decrypted images
MSE	High	0
PSNR	Low	Infinite
CCr	Low	1
CCg	Low	1
CCb	Low	1
NSCR	High	0
Remarks	Low quality	High quality

Many methods were introduced to encrypt-decrypt digital images. In [1, 2] the authors produced a blocked based method to encrypt-decrypt color images, this method gave a TP equal 3.6 M bytes per second. The authors in [3, 4] introduced a scrambling method through folding transform, this method gave a TP of 2.8 M bytes per second. In [5} the authors introduced a scheme based on logistic maps, which gave a TP of 0.8 M bytes per second. In [6] the authors introduced a novel image encryption approach using matrix reordering which provided an average TP equal to 0.37 M byte per seconds. In [7] the authors provided a new logistic maps for image encryption which provided an average TP equal to 0.46 M byte per seconds. In [8] the authors introduced a symmetric image encryption scheme based on 3D Chaotic cat maps, which provided an average TP equal to 1.56 M byte per seconds. In [9] the authors produced two versions of a secure image encryption algorithm based on Rubik's Cube principle, which gave the maximum TP equal 0.33 M bytes per seconds, table 2 summarizes the throughputs of the previous works.

Table 2: TPs of the related works

Method	TP(M bytes per second)
Ref. [1,2]	3.6550
Ref. [3, 4]	2.8985
Ref. [5]	0.8152
Ref. [6]	0.3750
Ref. [7]	0.4688
Ref. [8]	1.5625
Ref. [9], V1	0.3348
Ref. [9], V2	0.1857

Lookup table generation

Chaotic logistic map model can be easily used to generate a CLK, this model uses equation 1

$$x_{n+1} = rx_n(1 - x_n) \quad (1)$$

where *r* is the so-called driving parameter. The equation is used in the following manner. Start with a fixed value of the driving parameter, *r*, and an initial value of x_0. One then runs the equation recursively, obtaining x_1, x_2, . . .x_n. For low values of *r*, x_n (as *n* goes to infinity) eventually converges to a single number. In biology, this number (x_n as *n* approaches infinity) represents the population of the species.

It is when the driving parameter, *r*, is slowly turned up that interesting things happen. When $r = 3.0$, x_n no longer converges — it oscillates between two values. This characteristic change in behavior is called a bifurcation. Turn up the driving parameter even further and x_n oscillates between not two, but four values. As one continues to increase the driving parameter, x_n goes through bifurcations of period eight, then sixteen, then chaos! When the value of the driving parameter *r* equals 3.57, x_n neither converges or oscillates — its value becomes completely random. For values of *r* larger than 3.57, the behavior is largely chaotic. However, there is a particular value of *r* where the sequence again oscillates with period of three. The bifurcations then begin again with period 6, 12, 24, then back to chaos.

A lookup table is an array of data that maps input values to output values, thereby approximating a mathematical function. Given a set of input values, a lookup operation retrieves the corresponding output values from the table. In the proposed method the data items will be replaced by their indexes in the lookup table during the encryption phase and the encrypted data items are to be used as an indexes in the lookup table and replaced by the contents of the indexes during the decryption phase as shown in figures 5 and 6.

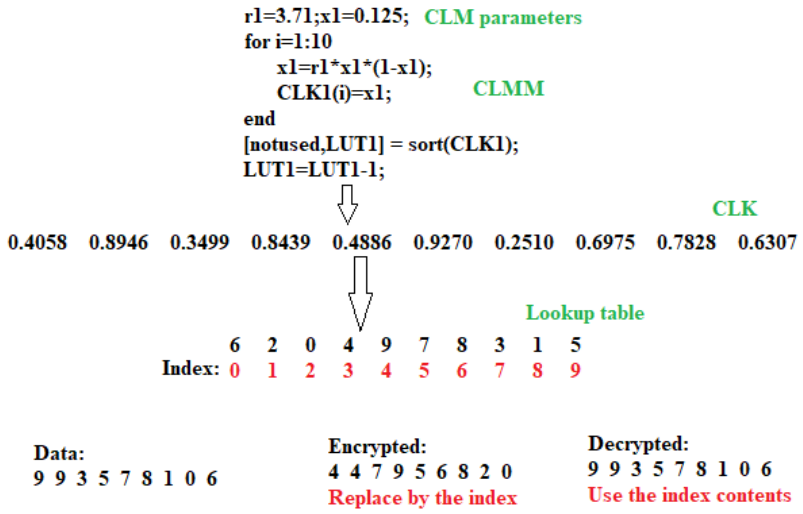

Figure 5: Using LUT for encryption-decryption

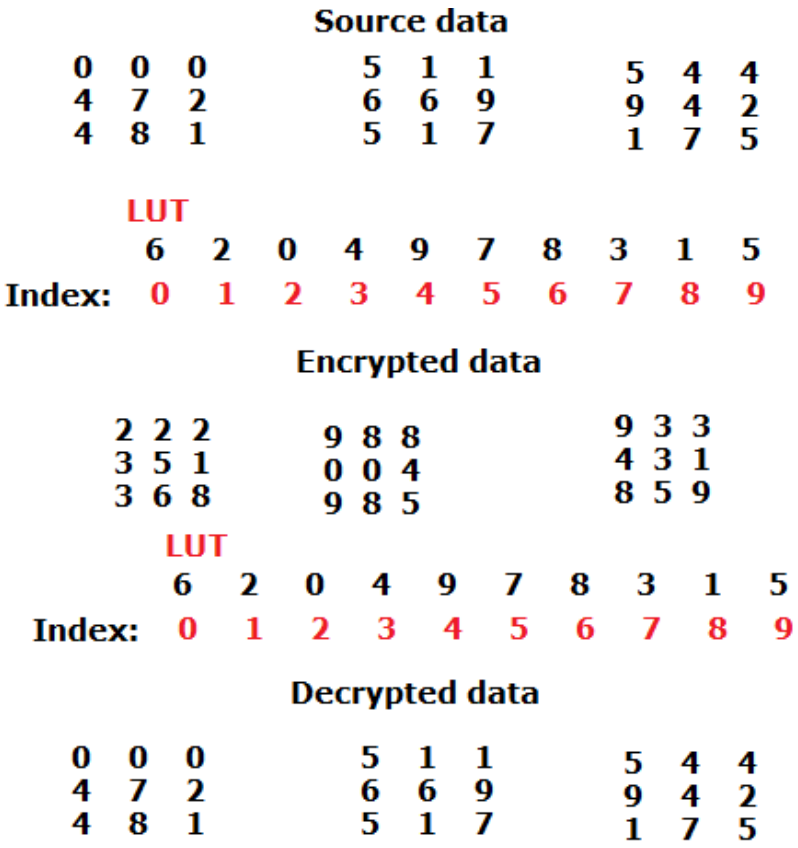

Figure 6: Using LUT to encrypt-decrypt 3D matrix

The following sequence of operations can be used to generate the lookup table:

```
rr=reshape(in,1,L);
r1=3.71;x1=0.125;
for i=1:256
    x1=r1*x1*(1-x1);
    CLK1(i)=x1;

end
[notused,LUT1] = sort(CLK1);
LUT1=LUT1-1;
```

The generated LUT is very sensitive to any changes in the chaotic parameters, any changes in them will change the contents of the LUT, thus changing the outputs of image cryptography as shown in figure 7.

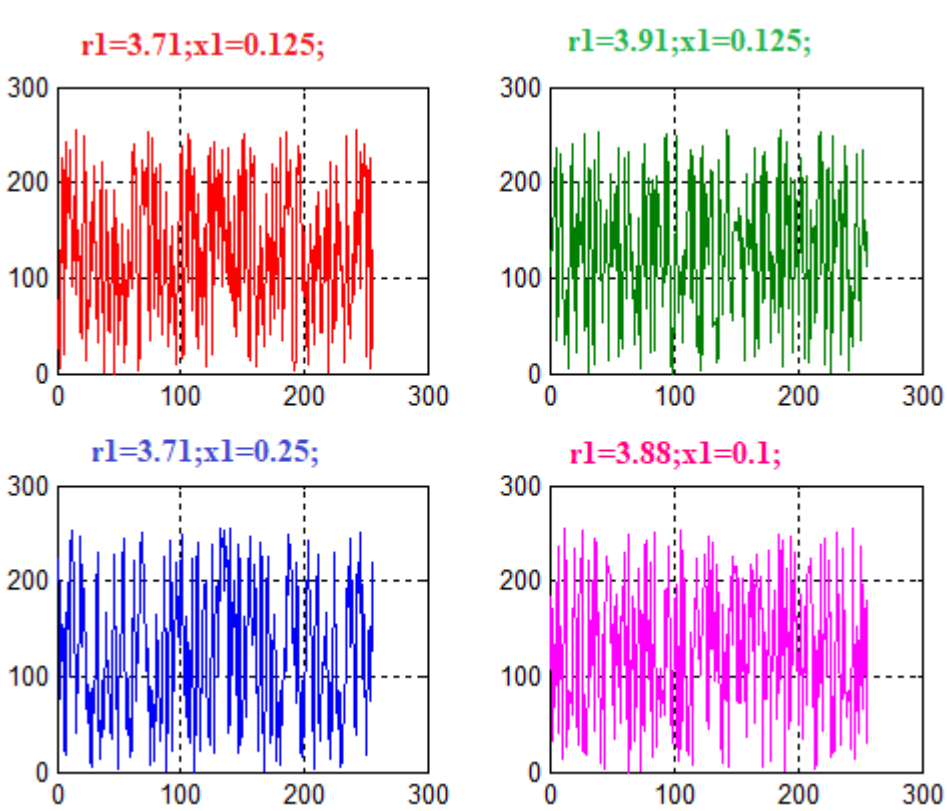

Figure 7: LUTs sensitivity

Proposed method

The proposed method uses a PK which contains the CLMM parameters values, the number of values can be equal two if the color image is to be treated as a 3D matrix, or 6 values if the color channel are to be treated separately.

The generated CLK can be easily converted to LUT by using the sort function. The pixel's values are to be replaced by the indexes of the LUT during the encryption and the encrypted value are to be replaced by the contents of indexes in the LUT during the decryption phase.

The encryption phase can be implemented applying the following steps (see figures 5 and 6):

Step 1: Get the PK

Step 2: Run CLMM to get the CLK.

Step3: Convert CLK to LUT using sort function.

Step 4: Get the image and retrieve its size.

Step 5: For each pixel in the image replace the pixel value by its index in the LUT to get the encrypted image.

The following sequence can be used to apply image encryption:

```
in=imread('E:\my_images\a12.jpg');
[n1 n2 n3]=size(in);
numbers =double(in);
codednumbers = zeros(n1,n2,n3);
for i = 1:n1
   for j = 1:n2
     for k = 1:n3
   ff=numbers(i,j,k)+1;
   codednumbers(i,j,k) = LUT1(ff);
     end
   end
end
en=uint8(codednumbers);
```

The decryption phase can be implemented applying the following steps (see figures 5 and 6):

Step 1: Get the PK

Step 2: Run CLMM to get the CLK.

Step3: Convert CLK to LUT using sort function.

Step 4: Get the image and retrieve its size.

Step 5: For each pixel in the image use the pixel value as an index in the LUT and replace it with the contents of this index to get the decrypted image.

The following sequence can be used to apply image encryption:

```
numbers =double(en);
decodednumbers = zeros(n1,n2,n3);
for ii = 1:n1
   for jj = 1:n2
     for kk = 1:n3
                ff=numbers(ii,jj,kk);
                decodednumbers(ii,jj,kk) = find(LUT1==ff);
  decodednumbers(ii,jj,kk)=decodednumbers(ii,jj,kk)-1;

     end
    end
end

de=uint8(decodednumbers);
```


Implementation and results analysis

The proposed method was implemented using various images, the obtained results were analyzed to prove the quality, security and speed enhancements provided by the proposed method.

- **Visual analysis**

The outputs generated by the method can be tested by eyes, the encrypted image must have a low quality and it must be a damaged version of the source image, while the decrypted image must have a high quality and must be identical to the source image, this fact can be proved by looking to the images and their histograms.

The proposed method was implemented using various images, all the obtained images satisfied the quality requirements, visual it can be proved that the method satisfied the quality requirement by locking to the images and the histograms as shown in figures 8, 9, and 10.

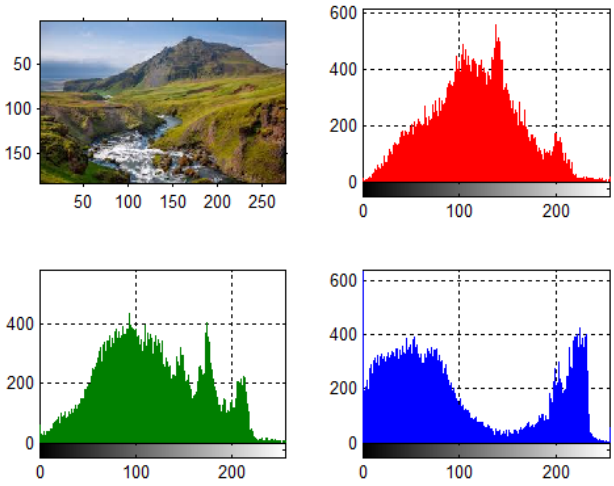

Figure 8: Sample source image and histograms

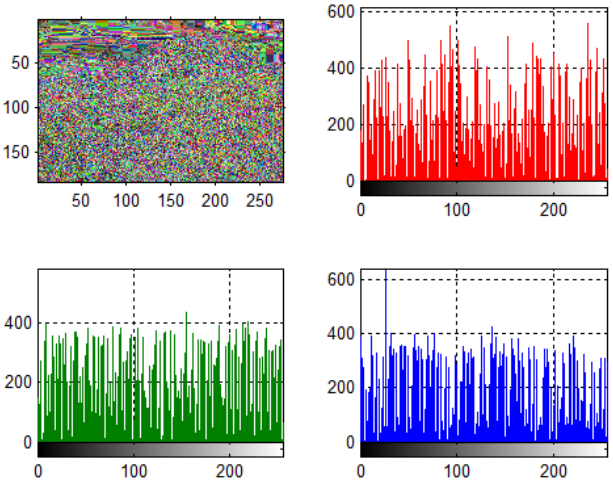

Figure 9: Sample encrypted image and histograms

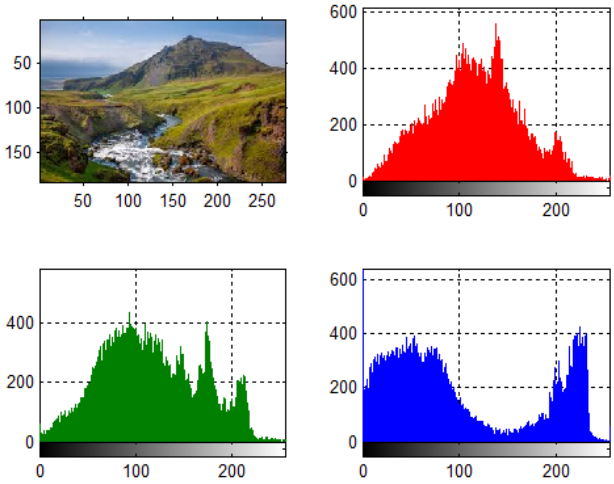

Figure 10: Sample decrypted image and histograms

- **Quality analysis**

The quality of the images can be measured by the quality parameters, the values of these parameters must meet the requirements listed in table 1.

The encryption phase must produce a low quality image file, while the decryption phase must provide a high quality image file, the quality level can be measured by MSE, PSNR, CC and NSCR.

MSE and NSCR between the source and the encrypted images must be high, while PSNR and CC must be low. The MSE and NSCR between the source and the decrypted images must be very low, while the CC between the source and decrypted image must be closed to 1 and the PSNR between them must be closed to infinite.

Quality between two image files can be measured by Mean square error (MSE) and peak signal to noise ratio (PSNR), high value of MSE and low value of PSNR points to the low quality, while low MSE and high PSNR points to the high quality. A good method of data cryptography must provide a high quality (low MSE and high PSNR) of the decrypted image file, (low PSNR and high PSNR between the source and the encrypted image files), MSE and PSNR can be calculated using equations 2 and 3:

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

$$MSE = \frac{1}{N} \sum_{i=1}^{N} (x_i - y_i)^2, \quad \textbf{(3)}$$

Where: MAX is the maximum possible value of samples values, N is the total number of samples, xi and yi are the corresponding sample values of the source and encrypted/decrypted speeches.

The value of CC between two image files expresses the dependency between their corresponding gray values. This is another statistical evaluation for testing the quality of the algorithm of data cryptography. Calculating correlation coefficient determines the level of correlation between two images and the correlation coefficient is always in range [−1, 1]. Values between |1–0.7| is considered as strong correlation (samples from the source files are similar to

samples from the encrypted file), correlation between |0.7–0.3| is considered as medium correlation and values between |0.3–0| is considered as weak correlation. Correlation coefficient can be calculated using equation 4:

$$\mathbf{CC}_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \quad \textbf{(4)}$$

where

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})^2,$$

$$D(y) = \frac{1}{N}\sum_{i=1}^{N}(y_i - \bar{y})^2,$$

$$cov(x,y) = \sum_{i-1}^{N}(x_i - \bar{x})(y_i - \bar{y}),$$

N is the total number of samples, xi and yi are the sample values of two image files, $\bar{x}$ and $\bar{y}$ are the mean values of samples, and finally cov (x, y) is covariance between both files.

Number of sample change rate (NSCR) is robustness test for establishing the quality of data cryptography algorithms. The purpose of the test is to compare the corresponding sample values of two image files to show the difference in percent. NSCR can be calculated using equation 5.

$$NSCR = \frac{\sum_{i=1}^{N} D_i}{N} \times 100\%, \quad \textbf{(5)}$$

where

$$D_i = \begin{cases} 1, x_i \neq y_i \\ 0, Otherwise \end{cases}$$

The selected image files were processed using the proposed method, the quality parameters values were calculated, and tables 5 and 6 show the obtained results between the source and the encrypted images. In the decryption phase MSE was always zero, PSNR was always infinite, CC was always 1 and NSCR was always 0.:

Table 3: MSE, PSNR and NSCR results

Image number	Size (byte)	MSE	PSNR	NSCR(%)
1	150849	12714	16.3209	99.4630
2	518400	8745.7	20.0621	99.5791
3	5140800	9259.0	19.4918	99.6467
4	4326210	9329.6	19.4158	99.7686
5	122265	8034.1	20.9107	99.8397

6	518400	7475.1	21.6319	99.7953
7	150975	9032.3	19.7396	99.6264
8	151353	11544	17.2863	99.3314
9	1890000	12161	16.7657	99.8437
10	6119256	7066.0	22.1948	99.9696
Remarks		High	Low	High

From table 3 we can see the quality of the encrypted images were low, and this prove the quality of the proposed method.

The CCs were also calculated between the color channels of the source and encrypted images, these values were always low, and this also prove the quality of the proposed method, the results of calculations are listed in table 4.

Table 4: CCs Results

Image number	Size (byte)	CCr	CCg	CCb
1	150849	-0.0641	-0.0170	0.0880
2	518400	0.1979	0.2070	0.2046
3	5140800	-0.0270	0.0317	0.0748
4	4326210	0.0238	0.0352	0.0413
5	122265	0.0729	0.1561	0.0277
6	518400	0.0379	0.0407	0.0291
7	150975	0.0325	0.0105	0.0171
8	151353	-0.0122	0.0316	0.1260
9	1890000	-0.00074099	-0.0398	-0.0659
10	6119256	-0.0510	0.0198	0.0366
Remarks		Low	Low	Low

- **Sensitivity analysis**

The encryption and decryption phases must use the same PK, any changes in the PK during the decryption phase will be considered as a hacking attempt by producing a damaged decrypted image, the following test prove this fact:

An image was encrypted using PK1, and it encrypted image was decrypted using PK2, figures 11, 12, and 13 show how the results are very sensitive to the used PKs:

PK1:

r1=3.71; x1=0.125;

PK2:

r1=3.92; x1=0.225;

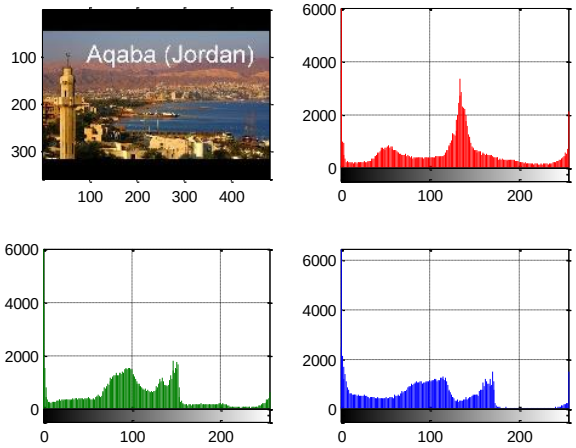

Figure 11: source image and histograms

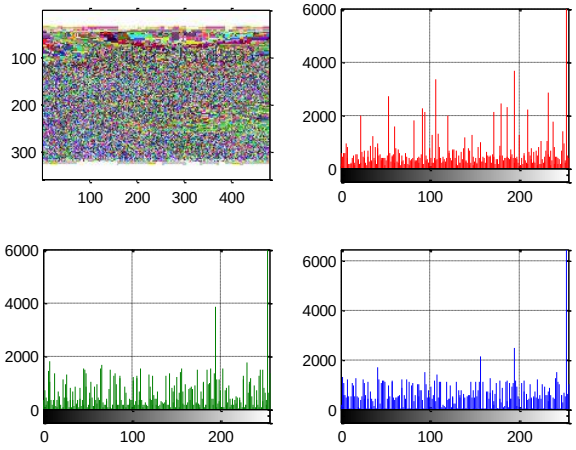

Figure 12: Encrypted image using PK1

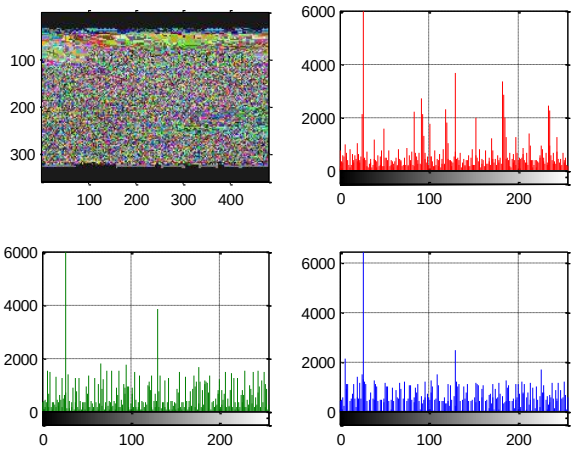

Figure 13: Decrypted image using PK2

- **Security analysis**

The proposed method uses a PK with two components if the image to treated as a 3D matrix, or 6 components if the image to be encrypted color by color, thus the key space will be calculated using equation 6:

$$\text{Key space} = 2^{64x6} = 2^{384} \quad (6)$$

This big number of combinations provides a huge key space, which can resist hacking attempt.

- **Speed analysis**

The selected images were processed using the proposed method the ETs, DTs, ETPs and DTPs were calculated, table 5 shows the obtained results:

Table 5: Speed results

Image number	Size (byte)	ET/DT(second)	ETP/DTP(M bytes per second)
1	150849	0.0093	15.5480
2	518400	0.0371	13.3412
3	5140800	0.3298	14.8640
4	4326210	0.2897	14.2394

5	122265	0.0079	14.8287
6	518400	0.0296	16.7103
7	150975	0.0094	15.2553
8	151353	0.0092	15.6166
9	1890000	0.1322	13.6343
10	6119256	0.4066	14.3524
Average	1908900	0.1261	14.8390

The obtained results shown in table 5 shows that the proposed method provided a good speed measurement and it improved the speed of image cryptography, and comparing with other existing method it has a significant speedup as shown in table 6:

Table 6:

Method	TP(M bytes per second)	Speedup of the proposed method
Ref. [1,2]	3.6550	4.0599
Ref. [3, 4]	2.8985	5.1195
Ref. [5]	0.8152	18.2029
Ref. [6]	0.3750	39.5707
Ref. [7]	0.4688	31.6532
Ref. [8]	1.5625	9.4970
Ref. [9], V1	0.3348	44.3220
Ref. [9], V2	0.1857	79.9085
Proposed	14.8390	1.0000

Conclusion

A simple, efficient and secure method of image cryptography was proposed. The method can be used to encrypt-decrypt gray and color images with any size and type. The proposed method used a complicated PK, which contains the values of CLMM parameters, these parameters were used to run a CLMMs to generate the required LUTs. The PK provided a huge key space capable to resist any hacking attacks, the decrypted images were very sensitive to the PK, any changes in the PK during the decryption phase was considered as a hacking attempt by producing damaged decrypted image.

The proposed method was implemented using various images, the obtained results were analyzed and it was shown that the proposed method satisfied the quality requirements, the proposed method improved the throughput of image cryptography and it was shown that the proposed method had a significant speedup comparing with other existing methods of image cryptography.

References

[1]. 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.

[2]. Jamil Al-Azzeh, Ziad Alqadi, Qazem Jaber, A Simple, Accurate and Highly Secure Method to Encrypt-Decrypt Digital Images, INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION, VOL 3 (2019) NO 3, pp. 262-265.

[3]. S. Wang, Y. Zheng, Z. Gao, "A New Image Scrambling Method through Folding Transform", IEEE International Conference on Computer Application and System Modelling, Taiyuan, China, October 22-24, 2010.

[4]. J. N. Abdel-Jalil, "Performance analysis of color image encryption\decryption techniques", International Journal of Advanced Computer Technology, Vol. 5, No. 4, pp. 13-17, 2016.

[5]. G. Yet, "An Efficient Image Encryption Scheme based on Logistic maps", International Journal of Pure and Applied Mathematics, Vol. 55, No.1, pp. 37-47, 2009.

[6]. T. Siva Kumar, R. Venkatesan, "A Novel Image Encryption Approach using Matrix Reordering", WSEAS Transactions on Computers, Vol. 12, No. 11, pp. 407-418, 2013.

[7]. H. Gao, Y. Zhang, S. Liang, D. Li, "A New Logistic maps for Image Encryption", Chaos- Solutions & Fractals, Vol. 29, No. 2, pp. 393- 399,2006.

[8]. G. Chen, Y. Mao, C. K. Chui, "A Symmetric Image Encryption Scheme based on 3D Chaotic Cat Maps", Chaos, Solutions & Fractals, Vol. 21, No. 3, pp. 749–761, 2004.

[9]. K. Loukhaoukha, J. Y. Chouinard, A. Berdai, "A Secure Image Encryption Algorithm Based on Rubik's Cube Principle", Journal of Electrical and Computer Engineering, Vol. 2012, Article ID 173931, pp. pp. 1-13, 2012.

[10]. 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.

[11]. 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.

[12]. 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.

[13]. 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.

[14]. 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.

[15]. 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.

[16]. 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.

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

[18]. 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.

[19]. 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.

[20]. 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.

[21]. 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.

[22]. 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.

[23]. 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.

[24]. 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.

[25]. 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.

[26]. 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.

[27]. 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.

[28]. 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.

[29]. 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.

[30]. 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.

[31]. 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.

[32]. 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.

[33]. 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.

[34]. 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.

[35]. 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.

[36]. 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.

[37]. 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.

[38]. 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.

[39]. 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.

[40]. 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.

[41]. 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.

[42]. 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.

[43]. 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.

[44]. 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.

[45]. 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.

[46]. 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.

[47]. 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.

[48]. AlQaisi Aws, Tarawneh Mokhled, A Alqadi Ziad, A Sharadqah Ahmad, Analysis of Color Image Features Extraction using Texture Methods, TELKOMNIKA, vol. 17, issue 3, 2018.

[49]. 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.

[50]. 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.

[51]. 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.

[52]. 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.

[53]. 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.

[54]. 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).

[55]. 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)

[56]. 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)

[57]. 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)

[58]. 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)

[59]. 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)

[60]. 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)

[61]. 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.

[62]. 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.

[63]. 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.

[64]. 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.

[65]. 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.

