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. 6, June 2022, pg.46 – 65

Two Complicated PKs to Protect Secret Messages

Prof. Ziad Alqadi

Albalqa Applied University

Faculty of Engineering Technology

Jordan – Amman

DOI: https://doi.org/10.47760/ijcsmc.2022.v11i06.004

Abstract: Increasing the message protection degree is a vital issue. In this paper research a new, simple, secure and efficient method of message cryptography will be proposed. The method will use two private keys for encryption decryption. The first key is to be generated from a secret image_key; the second key is to be generated using chaotic logistic map model. The two key will form a complicated complex key which cannot be hacked, thus will secure the transmitted messages from being hacked. The PK will be very sensitive to any changes: image_key, selected image color, message length and chaotic parameters. Any minor change in the decryption phase will generate new PK, and a corrupted damaged decrypted message will be produced.
A set of analyses (sensitivity, quality and throughput) will be performed to prove the improvements and efficiency provides by the proposed method.

Keywords: Cryptography, image key, chaotic key, PSNR, MSE, CC, throughput.

Introduction

Everything that can be stored and transmitted over the Internet, may be exposed to hacking or obtained by an unauthorized third party, which forces us to work on encrypting our files and messages of importance, which applies to all Internet users, especially those working in sensitive areas Like the press, documenting violations and crimes.
The occurrence of our secret messages, or our data that we would like to share selectively, may cost us in the hands of our opponents great losses, which may lead to arrest at times, or even the loss of life at other times, especially in periods of conflicts and wars, or under the control of tyrannical governments that find that it is It has the right to penetrate all information and messages, and to eliminate everything that contradicts its directions and opinions, apart from the right of individuals to privacy and freedom of expression [39-49].

Hence the importance of information encryption as an essential value in maintaining the digital security of users and protecting the confidentiality and privacy of their information, as encryption allows hiding the content of messages exchanged between two people from any third person who may intercept them, and in the event that the wrongly encrypted files fall into the hands of unauthorized persons to read them. The content of the messages will remain unread for them [8-12].
Cryptography is the process of converting information from its readable or clear form to a form that can only be read or viewed by authorized persons, and it falls within the framework of cryptography(see figure 1).

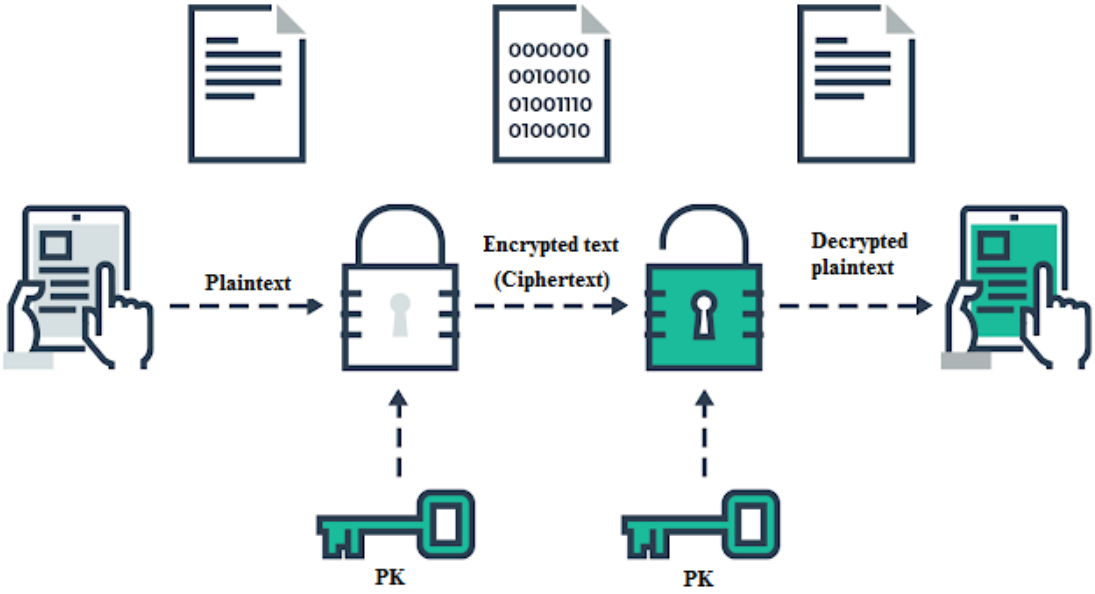


Figure 1: Data cryptography process

Encryption is the best way to protect valuable information, be it documents, images, or online electronic transactions, from falling into the wrong hands and the possible security risks that this entails.
Encryption methods have witnessed a clear development since its inception and throughout the ages to this day, and its practical applications have diversified to include several areas, such as informatics, security, military, diplomacy, commercial and banking [13-18].
Cryptography is the science of "breaking encryption" and breaching secure communications that interceptors of encrypted data use to learn about the content of this data.
The emergence of encryption methods has prompted software developers to update encryption methods in a sustainable and accelerated manner to provide more quality encryption methods, which also prompted those in charge of encryption to raise the level of their methods used, which led to the creation of a state of continuous chase between these two sciences, in an attempt One side is superior to the other [19-23].

The motivation of the proposed method of data cryptography is to introduce a simple, highly secure, efficient method.

The security of the proposed method will be achieved by the following add features:

1) Using two private keys to apply encryption-decryption.

2) Each key has a variable length and it contains a set of values, number of these values depends on the message (or message block) to be encrypted-decrypted, thus it is impossible to hack these keys.

3) The first private key is to be generated from an image_key, which must be kept in secret, one color matrix (see figure 2) will be used to generate this key.

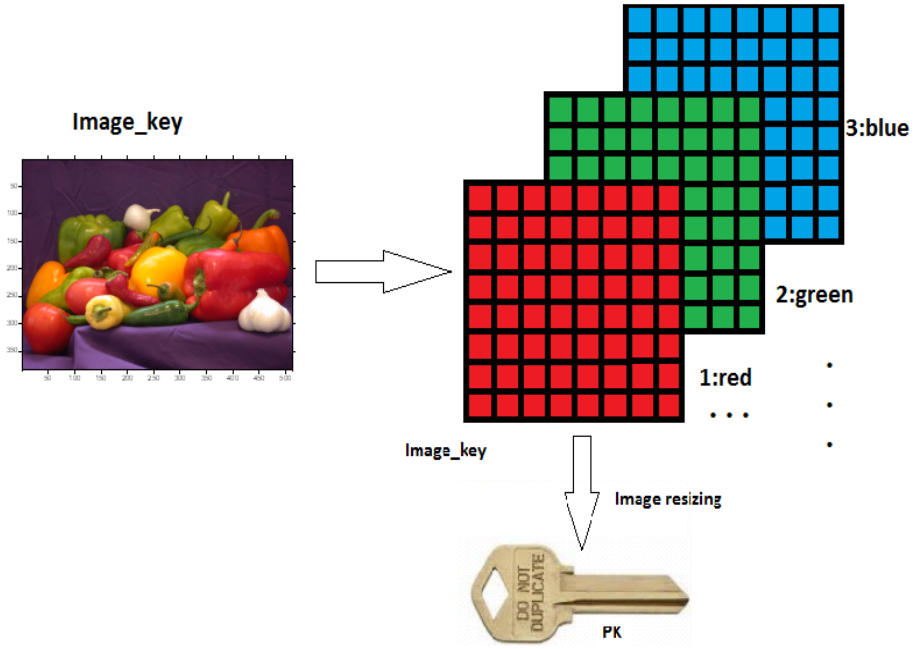


Figure 2: Image_key to generate first PK

The contents and the size of the first PK depend on the selected image_key, the selected color matrix and the length of the message to be encrypted-decrypted as shown in figures 3, 4 and 5 [24-30]:

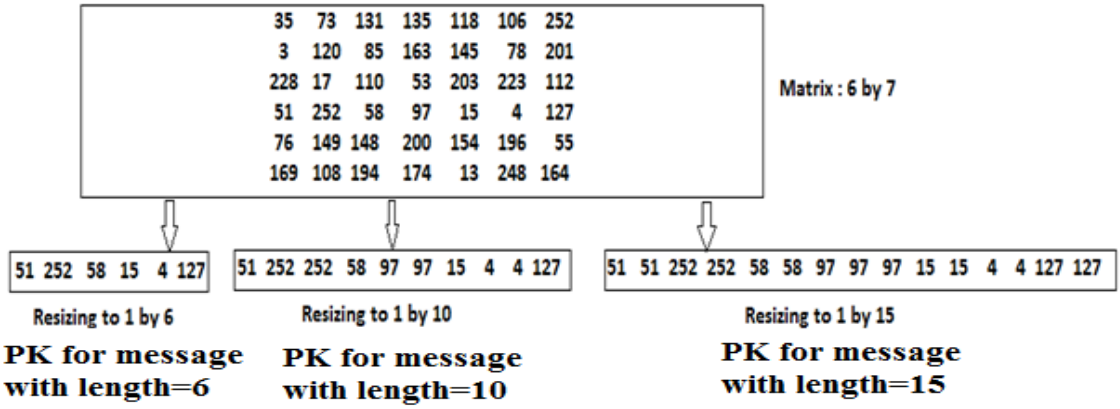


Figure 3: Using 2D matrix to generate various keys

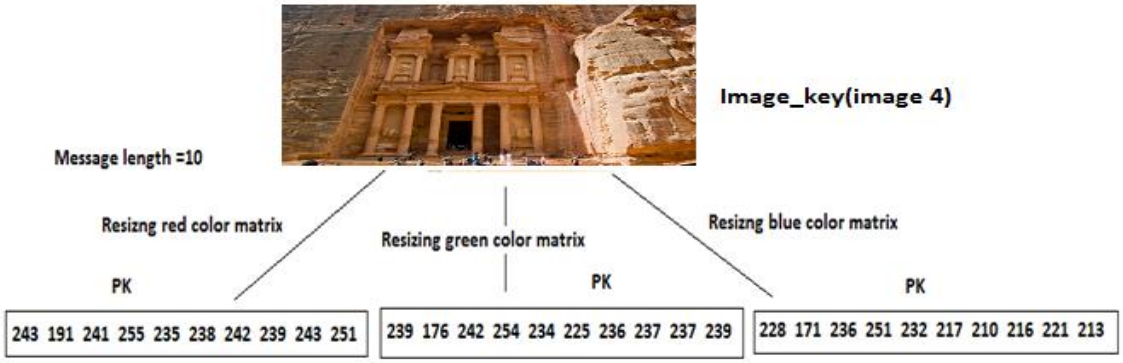


Figure 4: Different keys for the same message from different colors

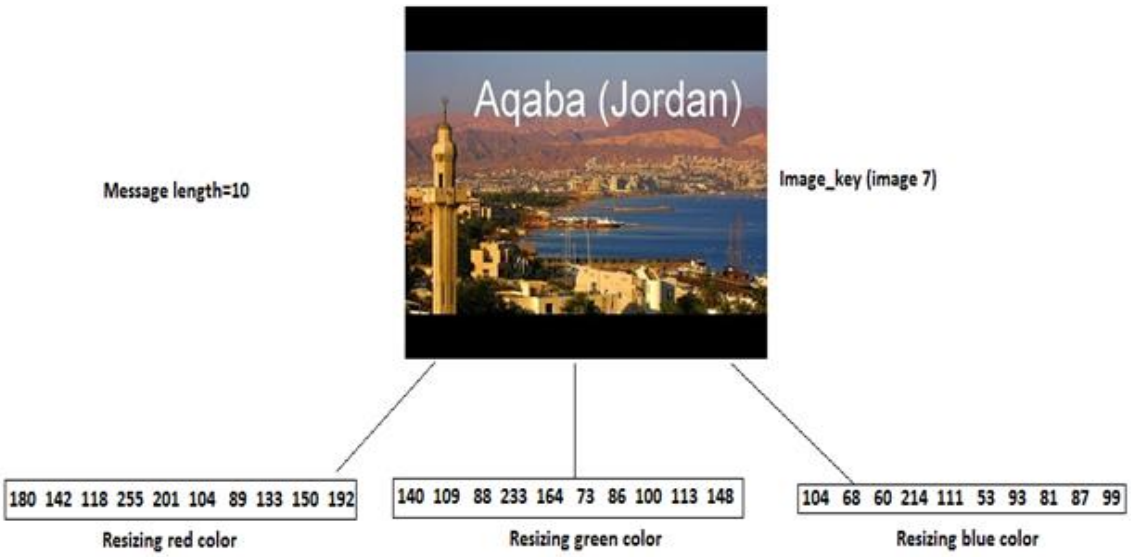


Figure 5: The keys are changed when selecting another image_key

4) The second key is to be generated using chaotic logistic map model. Chaotic logistic map is a one dimensional function which has the following main features [1]:

- The created values by the function are completely random, and they do not repeat themselves even after a number of iterations in a period.
- The created numbers are very sensitive to the selected initial values.

The chaotic logistic map (CLM) function is calculated by equation 1 [1-3]:

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

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.
- CPK can be generated using the sequence of operations shown in figure 6:

```
r1=3.99;x1=.01; Chaotic logistic map parameters
for i=1:L
   x1=r1*x1*(1-x1);
     key12(i)=x1;
    end
```

Figure 6: Second PK generation

The efficiency of the proposed method can be achieved by optimizing the encryption-decryption times, thus increasing the speed of the process of cryptography (maximizing the method throughput) [30-35].

The proposed method will totally destroy the encrypted data making it unreadable, and recovering the original data after decryption. The proposed method will decrease the correlation coefficient (CC) between the original and encrypted messages, decrease the value of peak signal to noise ratio (PSNR) between the original and encrypted messages, and increase the value of mean square error (MSE) between the original and encrypted messages.

In the decryption phase the value of MSE must be zero, the value of PSNR must be infinite, while the value of CC must be equal 1. The quality parameters between two messages can be calculated using equations 2, 3, and 4.

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

$$PSNR = 10 * \log_{10}\frac{(MAX_I)^2}{MSE_t} \qquad (3)$$

S and R are messages

$$cc = \frac{\sum (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum (x_i - \bar{x})^2 \sum (y_i - \bar{y})^2}} \quad (4)$$

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

Related Work

Many methods of message cryptography where introduced, most of the methods were based on the data cryptography standards [36-41]: data encryption standard (DES), 3DES, advance encryption standard (AES) and blowfish (BF). These methods share the following features, and most of these features can be considered as disadvantages:

- PK: private key has a fixed length of bits; this key is used to generate some other sub keys required in the encryption and decryption phases.
- Block size: the message must be divided into blocks, block size is fixed and cannot be change, for messages with long length the number of blocks will be high, thus an extra time will be required to apply encryption and decryption phases, the increasing in encryption-decryption times will negatively affect the efficiency of the process of cryptography, table 1 shows the average throughputs (number of bytes encrypted/decrypted per second) of the standard methods.

Table 1: Throughput of standard methods

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

- Rounds: Fixed number of rounds are used for each method, this will increase the required times for data cryptography.
- These methods give good values for MSE, PSNR and CC during the encryption and decryption phases.

The Proposed Method

The proposed method for encryption requires the following steps (see figure 7):

1) Get the message, get the message length, and convert the message to decimal.
2) Use chaotic logistic map parameters r and x and message length to generate key 1.
3) Use image_key to and message length generated key 2.
4) For each character in the message: convert the decimal version of the character to binary, rotate left the binary version to number of digits equal nrlb, then convert the binary results back to decimal to get the first version of the encrypted character.
5) Xor the encrypted message with key 1 to get the final encrypted message.

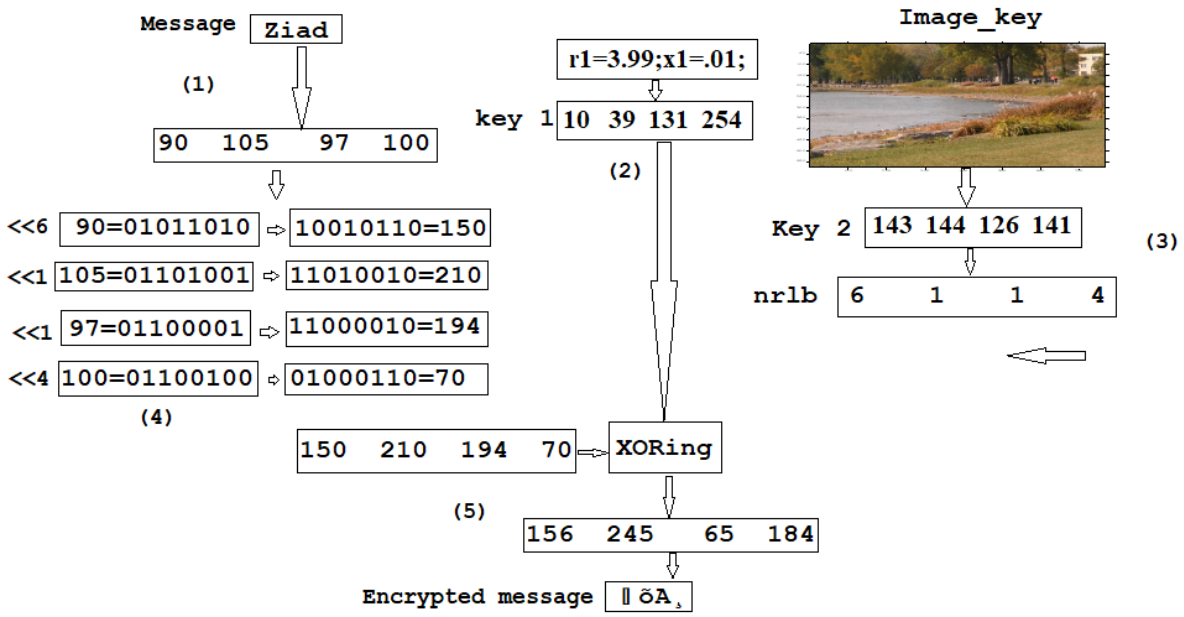


Figure 7: Proposed encryption phase

The proposed method for decryption requires the following steps (see figure 8):

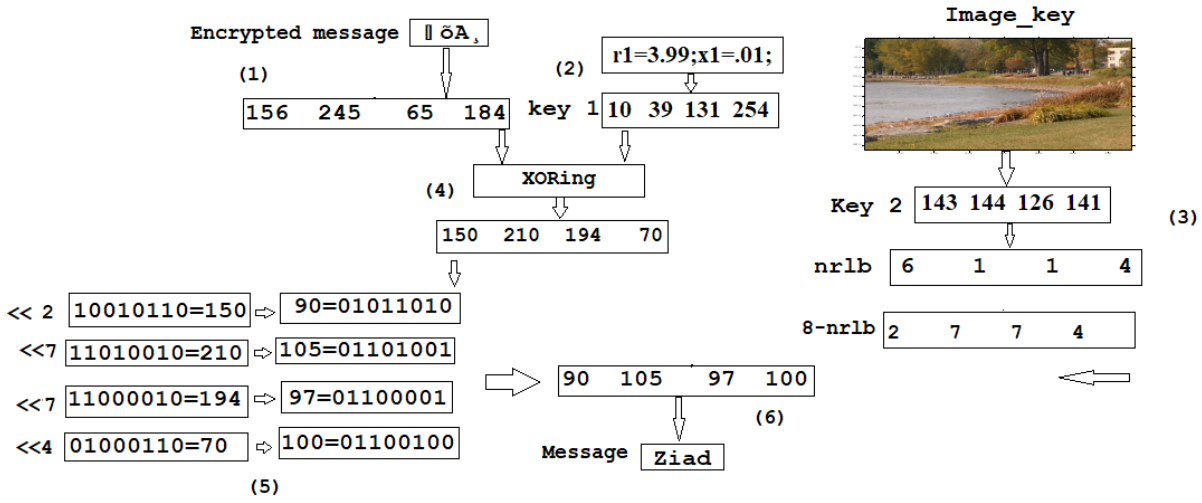


Figure 8: Proposed decryption phase

1) Get the encrypted message, get the message length, and convert the message to decimal.
2) Use the chaotic logistic map parameters and the message length to generate key 1.
3) Use image_key to and message length generated key 2.
4) XOR the message with key 1.
5) For each character in the received in step 4 message: covert the decimal value to binary, rotate left the binary value 8-nrlb times, and cover back the resulting binary value to decimal to get the decrypted version.
6) Convert the decimal message to character to get the decrypted message.

For other researchers to reproduce the results the following mat lab code can be used to implement the proposed method:

```
clear all,clc
%Inputs
a=imread('C:\Users\win 7\Desktop\sampleMerry_0055_Lasalle.jpg');
mes='ziad alqad  albalqa applied uinversity Amman Jordan';
w3=uint8(mes);
s=length(w3);
```



```
%Image_key generation
tic
key1=imresize(a(:,:,1),[1,s]);
k1t=toc;
%Chaotic logistic map key generaion
tic
r1=3.99;x1=.01;
for i=1:s
   x1=r1*x1*(1-x1);
   key12(i)=x1;
end
key2=uint8(255*key12);
k2t=toc;

%First round of encryption
tic
for i=1:s
   a1=w3(1,i);
   a2=dec2bin(a1,8);
   nbrr=mod(key1(i),6)+1;
   a3=rotl(a2,nbrr);
   en1(1,i)=bin2dec(a3);
end
rott=toc;
%Second round of encryption
tic
en=bitxor(uint8(en1),key2);
xort=toc

%decryption
de1=bitxor(en,key2);
for i=1:s
   a1=de1(1,i);
   a2=dec2bin(a1,8);
   nbrr=8-(mod(key1(i),6)+1);
   a3=rotl(a2,nbrr);
   de(1,i)=bin2dec(a3);
end
char(de);
```



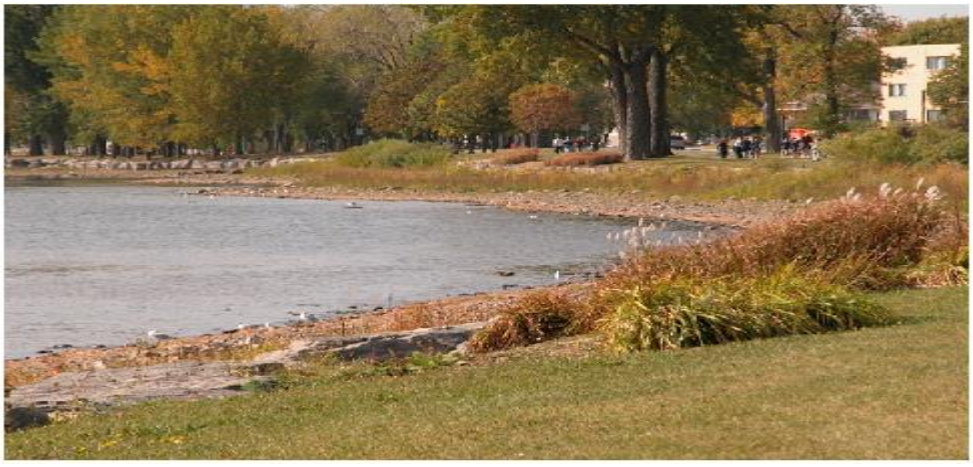
```
%Results
tt=k1t+k2t+xort+rott;
tp=s/tt;
k1t
k2t
xort
rott
tt
tp
[m1 m2]=PSNR_RGB(w3,en)
[m3 m4]=PSNR_RGB(w3,de)
cc1=corr2(w3,en);
cc2=corr2(w3,de);
[m1 m2 cc1];
[m3 m4 cc2];
```

```
%MSE and PSNR calculation function
function [mse psnr]=PSNR_RGB(X,Y)
 X=double(X);
 Y=double(Y);
  d1=max(X(:));
d2=max(Y(:));
d=max(d1,d2);
mse=mean2((X-Y).^2);
 psnr=10*log((d.^2)./mse);
```

This program was implemented using the color image with the link:

http://tabby.vision.mcgill.ca/html/Jpgpic/LandWater/sampleMerry_0055_Lasalle.jpg

The following are the obtained outputs:




```
xort =     0
ans =ziad alqad  albalqa applied uinversity Amman Jordan
k1t =    0.0590
k2t =  1.0000e-003
xort =     0
rott =    0.0220
tt =    0.0820
tp =  621.9512
m1 =  7.2972e+003
m2 =   21.2353
m3 =     0
m4 =     Inf +    NaNi
cc1 =   -0.0738
cc2 =     1
```

Implementation and Results Analysis

Several messages with various lengths using various images were treated using the proposed method, figures 9 and 10 show two groups of selected images (the size of these images ranges from small to huge), table 2 shows the basic information of these images.

Figure 9: Selected group 1 of images

Figure 10: Selected group 2 of images

Table 2 : Selected images basic information

Image number	Resolution (pixel)	Size (byte)	Image number	Resolution (pixel)	Size (byte)
H1	1880 x 2816	15882240	M1	151 x 333	150849
H2	1880 x 2816	15882240	M2	360 x 480	518400
H3	2848 x 4272	36499968	M3	1071 x 1600	5140800
H4	1880 x 2816	15882240	M4	981 x 1470	4326210
H5	1880 x 2816	15882240	M5	165 x 247	122265
H6	1880 x 2816	15882240	M6	360 x 480	518400
H7	1880 x 2816	15882240	M7	183 x 275	150975
H8	1880 x 2816	15882240	M8	183 x 275	150975
H9	1824 x 2736	14971392	M9	600 x 1050	1890000
H10	720 x 1280	2764800	M10	1144 x 1783	6119256

To prove the efficiency of the proposed method, the following analyses were performed:

1) Sensitivity analysis

The two PKs are very sensitive to any minor changes, any minor changes in the keys parameters in the decryption phase will be considered as a hacking attempt and the produced decrypted message will be corrupted and readable. The generated chaotic logistic map key (CLMK) is very sensitive to any changes in the chaotic parameters x and r and the message length, any changes in the values of these parameters will produce a new key as shown in figure 11.

The image key is also very sensitive, changing the image_key, or changing the image color, or changing the message length will produce a new key (see figure 12), using this key in the decryption phase will produce a damaged, unreadable message.

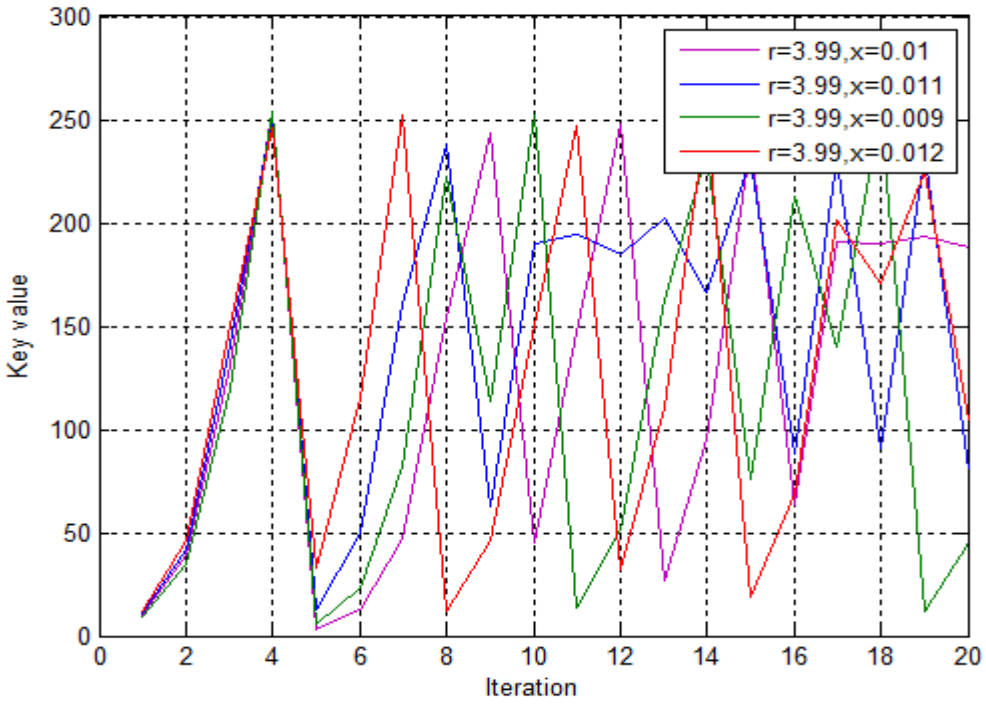


Figure 11: Chaotic key sensitivity

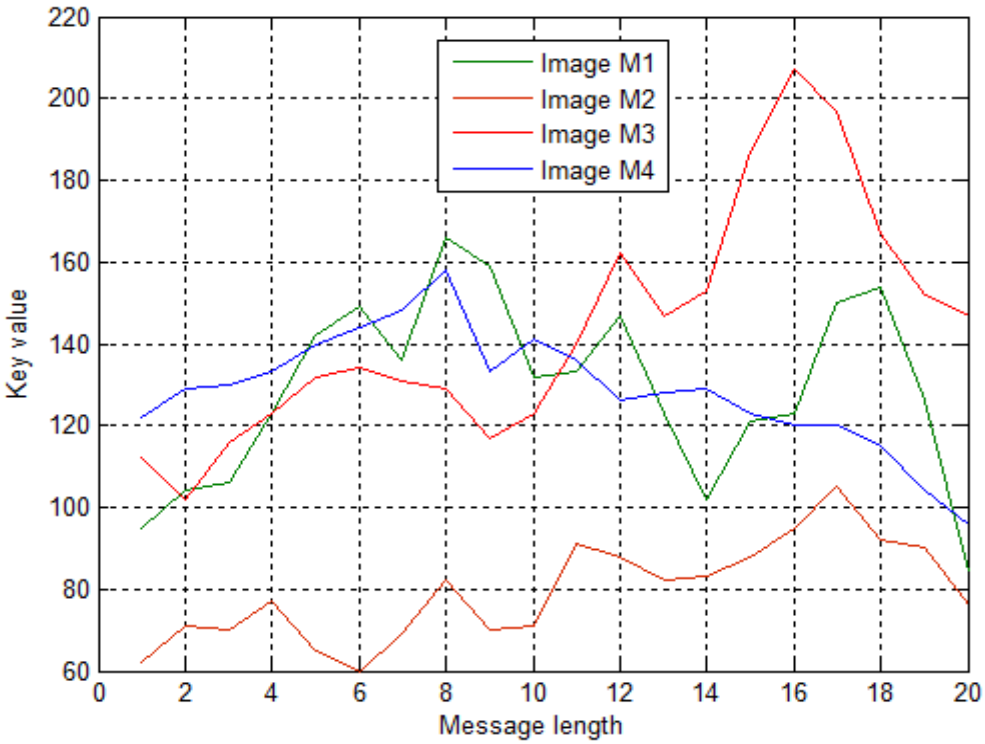


Figure 12: image key sensitivity

2) Quality analysis

Several messages were selected (short and long), these messages were encrypted-decrypted using the proposed method, MSE, PSNR and CC were calculated, table 3 shows the results of encrypting short messages using M1 image, while table 4 shows the results of encrypting long messages using H3 image. The results of MSE, PSNR and CC in the decryption phase were: MSE=0, PSNR=infinite, and CC=1. As we can see in tables 3 and 4(very high MSE, very low PSNR and closed to zero CC), these obtained values prove that the proposed method satisfies the quality requirements.

Table 3: Short messages quality

Message length(byte)	MSE	PSNR	CC
100	10887	17.8722	-0.1014
200	10004	18.7181	0.1115
300	9125.9	19.6366	0.1443
400	10999	17.6915	-0.0211
500	11283	17.5145	-0.0482
600	10615	18.1246	0.0553
700	10895	17.8648	-0.0637
800	11344	17.4604	-0.0404
900	11252	17.5425	-0.0309
1000	11220	17.5711	-0.0764

Table 4: Long messages quality

Message length(K byte)	MSE	PSNR	CC
10	11026	17.7453	-0.0168
20	11127	17.6536	-0.0260
30	11022	17.7491	-0.0135
40	11039	17.7332	-0.0174
50	11084	17.6928	-0.0184
60	11025	17.7465	-0.0164
70	11082	17.6948	-0.0176
80	11040	17.7328	-0.0160
90	11042	17.7307	-0.0150
100	11073	17.7022	-0.0204
1000	11034	18	0.0000

3) Throughput analysis

The encryption (decryption) times for processing short messages were calculated, table 5 shows the obtained results:

Table 5: Encryption time for short messages

Message length(Byte)	Encryption time(second)	Throughput(byte per second)
100	0.0710	1408.5
200	0.0850	2352.9
300	0.1010	2970.3
400	0.1110	3603.6
500	0.1290	3876.0
600	0.1420	4225.4
700	0.1600	4375.0
800	0.1760	4545.5
900	0.1940	4639.2
1000	0.2110	4739.3

From table 5 we can see that the encryption time increases when the message length increases, also the throughput increases (see figure 13) . The obtained throughput is better than the throughputs obtained for standard methods (see table 1).

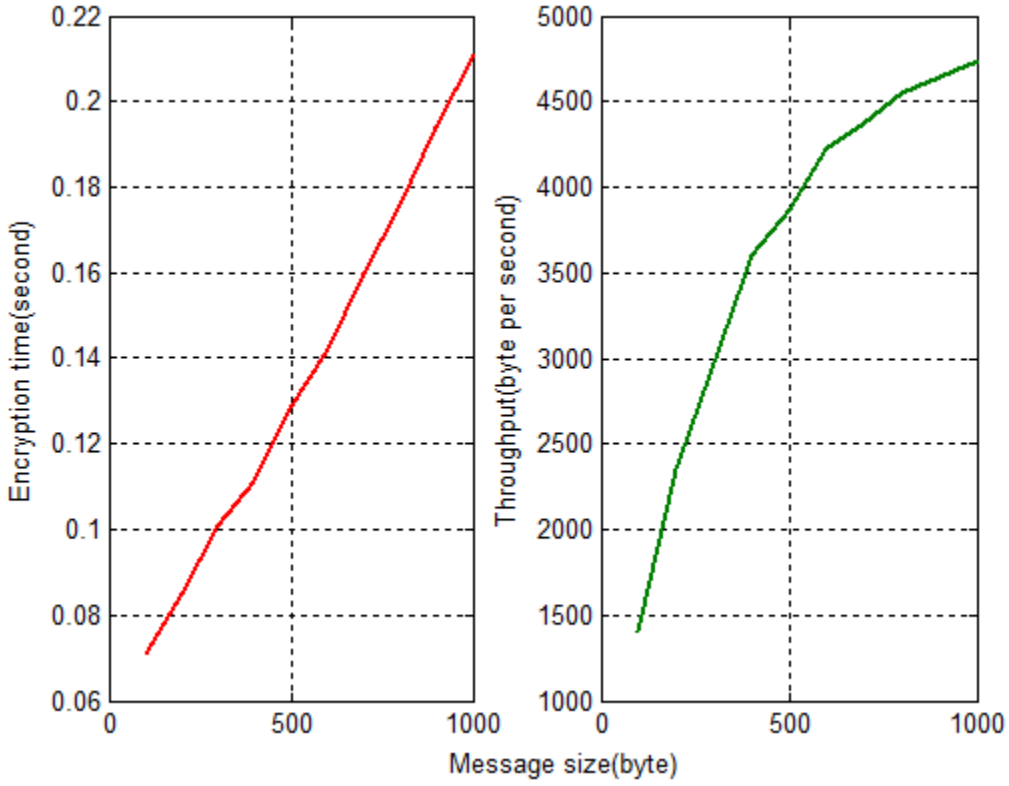


Figure 13: Encryption time, throughput VS message size (short messages)

The encryption (decryption) times for processing short messages were calculated, table 6 shows the obtained results:

Table 6: Encryption time for long messages

Message length(Kbyte)	Encryption time(second)	Throughput(byte per second)
10	2.2270	4598.1
20	5.5080	3718.2
30	10.4690	2934.4
40	17.0830	2397.7
50	25.0070	2047.4
60	34.2250	1795.2
70	47.3150	1515.0
80	62.8190	1304.1
90	79.5980	1157.8
100	98.8120	1036.3
1000	10760	95

From table 6 we can see that the encryption time increases when the message length increases, the throughput decreases (see figure 14) . The obtained throughput is better than the throughputs obtained for standard methods (see table 1).

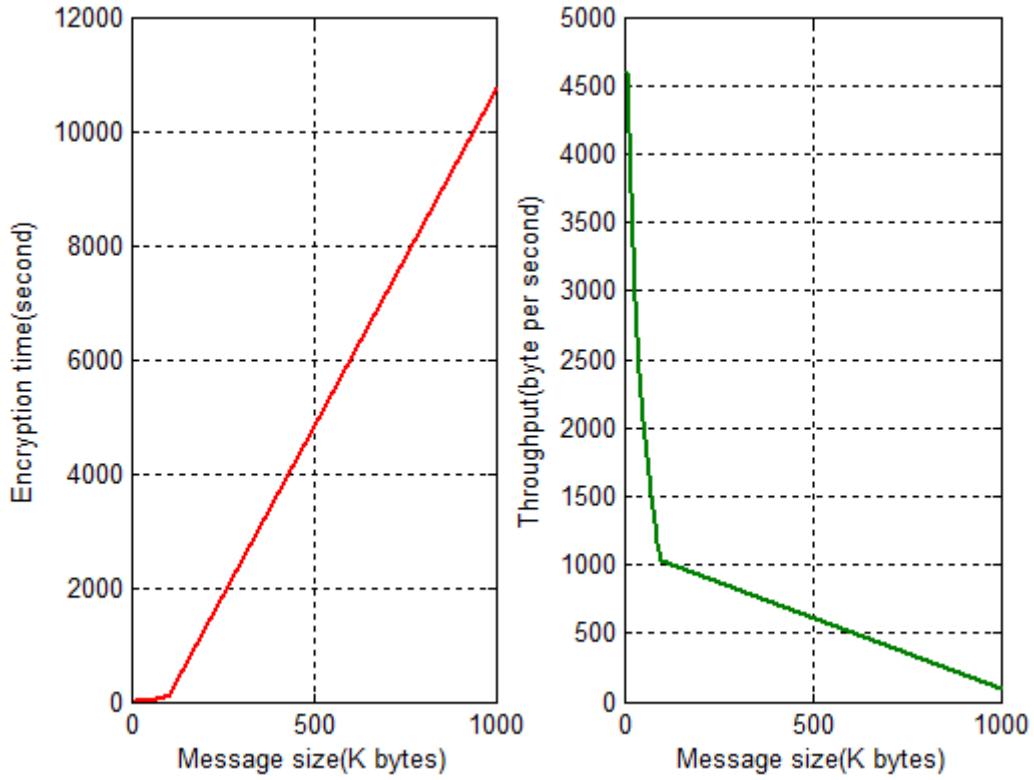


Figure 14: Encryption time, throughput VS message size (long messages)

The chaotic key requires time to be generated; this time will grow up when increasing the key length, table 7 shows the required time needed to generate chaotic keys with various lengths (see figure 15).

Table 7: Time to generate chaotic key

Key length	Processing time(second)	Remarks
100	**0.0006406000000000**	Low
200	**0.0007604000000000**	Low
400	**0.0007841000000000**	Low
500	**0.0009060000000000**	Low
1000	**0.001567900000000**	Low
2000	**0.003238700000000**	Low
4000	**0.007943700000000**	Low
5000	**0.012307600000000**	High
10000	**0.041075900000000**	High
50000	**2.042507500000000**	High
100000	**10.471385400000001**	High
1000000	**1742.065657100000**	Very high

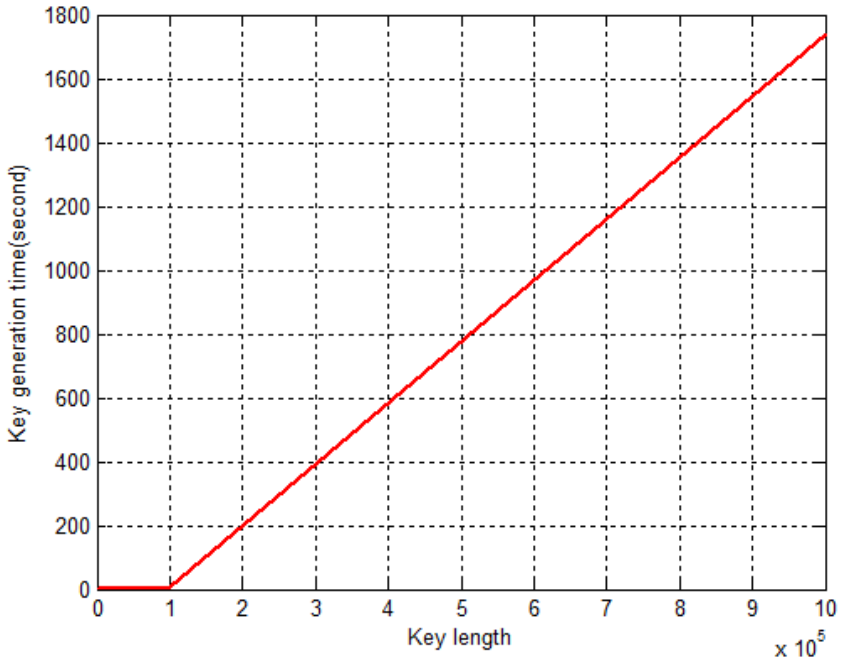


Figure 15: Chaotic key generation time vs key length

To make a balance between the key generation time and encryption process time we recommend dividing the message into blocks, then a chaotic key can be generated for each block, this will optimize the throughput. Table 8 shows how to increase the throughput by dividing a message into blocks with block size =5000 bytes.

Table 8: Improving the throughput by message blocking

Message length(Kbyte)	Encryption time(second)	Throughput(byte per second)
10	0.7837	13066
20	1.8232	11233
30	3.3255	9238
40	5.6765	7216
50	8.5021	6022
60	11.4595	5361
70	15.1779	4723
80	21.6875	3777
90	24.6757	3735
100	30.6497	3341

Conclusion

A simple, secure and efficient method of data cryptography was proposed. The obtained results showed that proposed method satisfied the quality of cryptography by providing excellent values MSE, PSNR and CC during the encryption and decryption phases applying two rounds of encryption: bit rotation and XORing. The proposed method used two complicated keys: the image key and the chaotic key which are very sensitive to any minor changes in the parameters used to generate these key. The image key was used to implement the first round of message encryption using the rotation left operation, while the second key was used in the second round to apply XORing of the encrypted in round 1 message with the chaotic key.

The performed various types of results analysis showed that the proposed method is highly secure and efficient, the obtained throughput was better than those obtained by standard method of data cryptography.

References

[1]. Stallings, W. (2014) Cryptography and Network Security Principles and Practice, Sixth Edition, prentice Hall, Upper Saddle River.

[2]. Forouzan, B.A. (2007) Cryptography and Network Security, Special Indian Edition, Tata McGraw-Hill Publishing Company Limited, New Delhi.

[3]. Mathur, M. and Kesarwani, A. (2013) Comparison between DES, 3DES, RC2, RC6, Blowfish and AES. Proceedings of National Conference on New Horizons in IT, NCNHIT, Mumbai, September 2013, 143-148.

[4]. Alanazi, H.O., Zaidan, A.A., Jalab, H.A., Shabbir, M. and Al-Nabhani, Y. (2010) New Comparative Study between DES, 3DES and AES within Nine Factors. Journal of Computing, 2, 152-157.

[5]. Aamer Nadeem, A Performance Comparison of Data Encryption Algorithms, IEEE 2005. https://www.cse.wustl.edu/~jain/cse567-06/ftp/encryption_perf/#Nadeem2005.

[6]. Rania A. Elmanfaloty, Ehab Abou-Bakr, An Image Encryption Scheme Using a 1D Chaotic Double Section Skew Tent Map, Complexity, Volume 2020 |Article ID 7647421 | https://doi.org/10.1155/2020/7647421

[7]. 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.

[8]. 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.

[9]. 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.

[10]. 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.

[11]. 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.

[12]. 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.

[13]. 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.

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

[15]. 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.

[16]. 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.

[17]. 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.

[18]. 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.

[19]. 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.

[20]. 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.

[21]. 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.

[22]. 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.

[23]. 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.

[24]. 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.

[25]. 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.

[26]. 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.

[27]. 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.

[28]. 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.

[29]. 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.

[30]. 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.

[31]. 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.

[32]. 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.

[33]. 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.

[34]. 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.

[35]. 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.

[36]. 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.

[37]. 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.

[38]. 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.

[39]. 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.

[40]. 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.

[41]. 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.

[42]. 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.

[43]. 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.

[44]. 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.

[45]. 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.

[46]. 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.

[47]. 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.

[48]. 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.

[49]. 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.

