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. 5, May 2022, pg.51 – 67

Three Levels of Protection to Secure Secret Message

Prof. Ziad A. Alqadi
Albalqa Applied University
Faculty of Engineering Technology, Jordan-Amman
DOI: https://doi.org/10.47760/ijcsmc.2022.v11i05.005

Abstract: Many data cryptography methods are based on DES; these methods have a lot of disadvantages such as fixed block size, fixed private key length, multiple rounds and sometimes low level of security. In this research paper a method of secret messages cryptography will be introduced. It will be shown that the proposed method can be easily used to apply data cryptography for short, medium and long messages keeping the values of the quality parameters (MSE, PSN and CC) acceptable. The method will use three image_key to generate the required private keys needed to calculate the number of rotation digits used in character rotation. The images are to be kept in secret and it is possible to change them any time without changing the operations used in the proposed method.
The proposed method will be compared with DES to show the improvements provided by the proposed method.
Keywords: Cryptography, PK, key, throughput, MSE, PSNR, CC.

Introduction

The text messages circulated through different social media vary and may be short, medium or long in length, and many of these messages can be of a special nature or carry confidential data, which calls for protecting the text message from penetration or protecting it from intruders or from data thieves [50-54].
Data cryptography is one of the most important methods used to protect secret data and secret messages, this process as shown in figure 1 uses encryption to destroy the source data and make it unreadable, the encrypted data must be decrypted to retrieve or recover the source data [12-17].

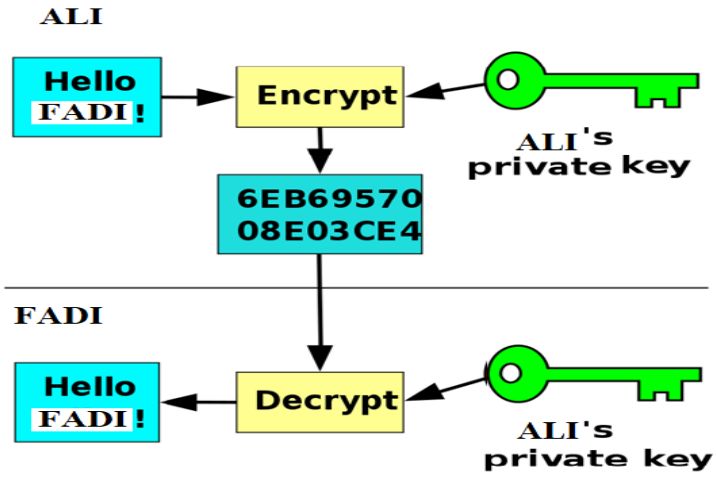

Figure 1: Data cryptography process

The level of data protection depends on the used private key (PK), the longer the PK is the higher protection level [18-22].

A good method of data cryptography must full destroy the source data after encryption and full recover the source dat after decryption (see figure 2), the level o data destruction and recovery can be measured between two data sets by mean square error (MSE), or peak signal to noise ratio (PSNR) and correlation coefficient (CC) [48-52]. Fully destruction means small PSNR and CC and at the same time big MSE (see table 1), while fully recovery means zero MSE, infinite PSNR and CC equal 1, MSE, PSNR and CC are considered to be used as a quality parameters and they can be calculated using equations 1, 2 and 3[23-29].

Table 1: Requirement of good data cryptography

	Encrypted image			Decrypted image		
	MSE	PSNR	CC	MSE	PSNR	CC
Original image	High	Low	Low	Close to zero	Very high	Close to 1

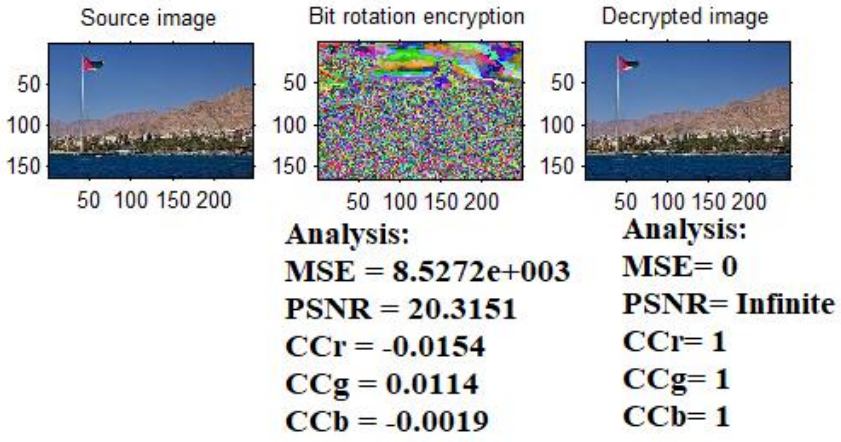

Figure 2: Fully data destruction and fully data recovery

MSE of x channel

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

Total MSE

$$MSE_t = MSE_R + MSE_G + MSE_B$$

Calculate PSNR

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

$$r = \frac{\sum (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum (x_i - \bar{x})^2 \sum (y_i - \bar{y})^2}} \tag{3}$$

Where

r = correlation coefficient

x_i = values of first image matrix

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

y_i = values of second image matrix

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

Digital color image is [30-35]a huge data bank, which containes a big number of data bytes arranged in 3D matrix (one 2D matrix for each color:red, green and blue) as shown in figure 3 [43-50]. Each color can be used separetly and it can be resized to form ant vector with any needed length as shown in figure 4. These vectors can be used as a secret private key, this key will be secret because the image (image_key) will be kept in sexret and the length of the resizing process can be determined by the secret message length[36-42].

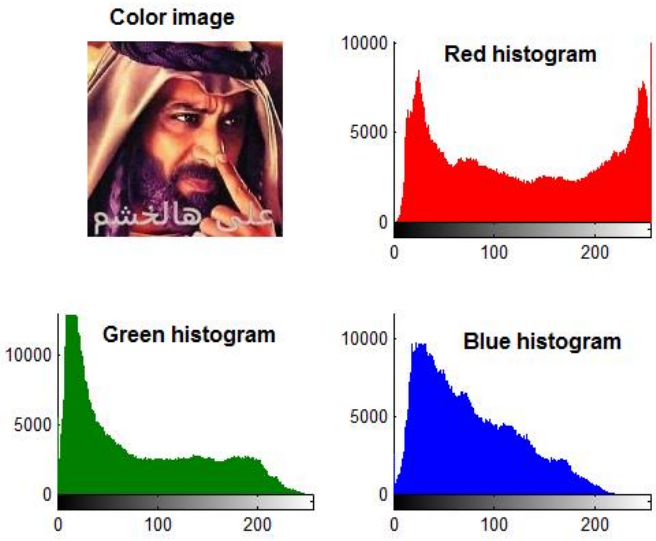

Figure 3: Image colors

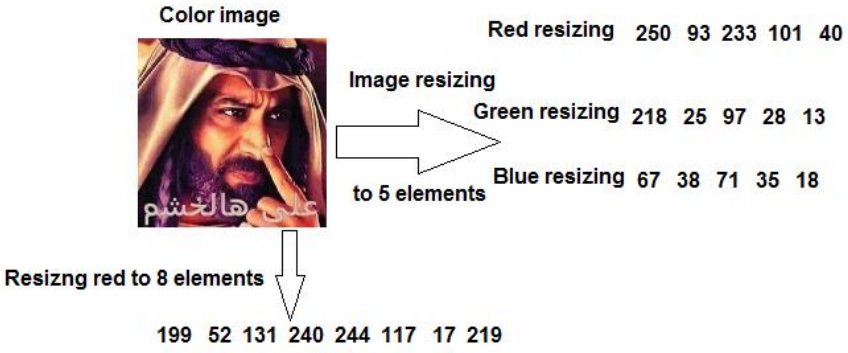

Figure 4: Various ways of image resizing

ASCII characters can be easily processed using logical operations such as rotate left(see figure 5) with a selected number of digits and XORing operations, theses operation can be handled to apply character encryption-decryption as illustrated in the examples shown in figures 6 and 7

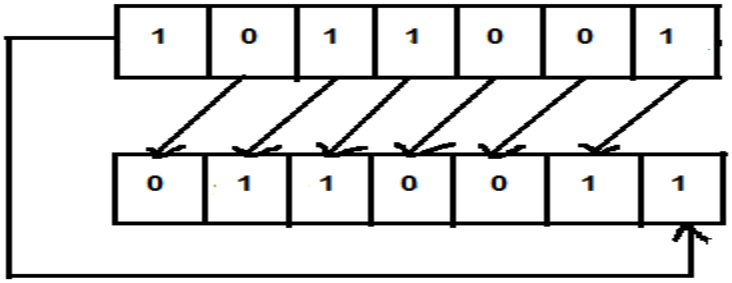

Figure 5: Rotate to one digit left operation

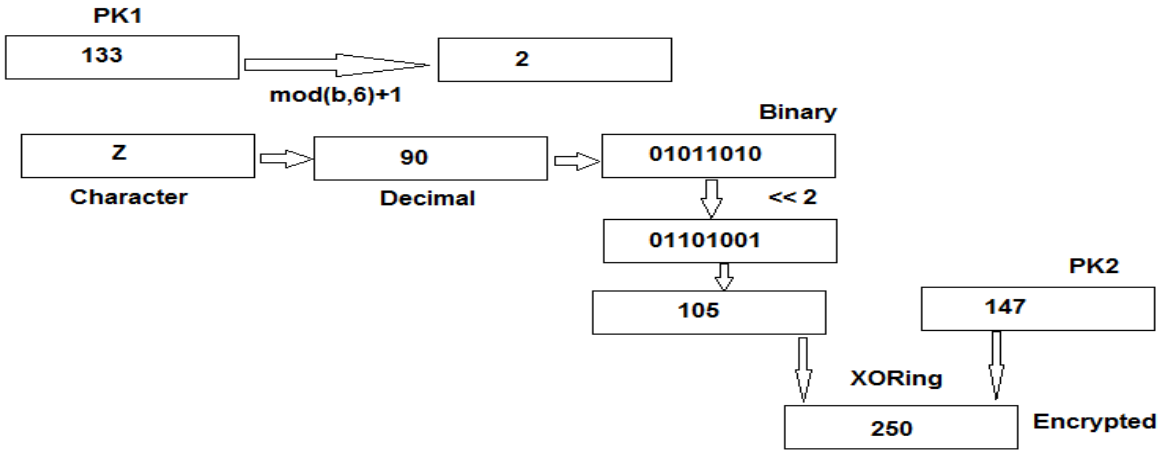

Figure 6: Example of using rotate left and XORing to encrypt character

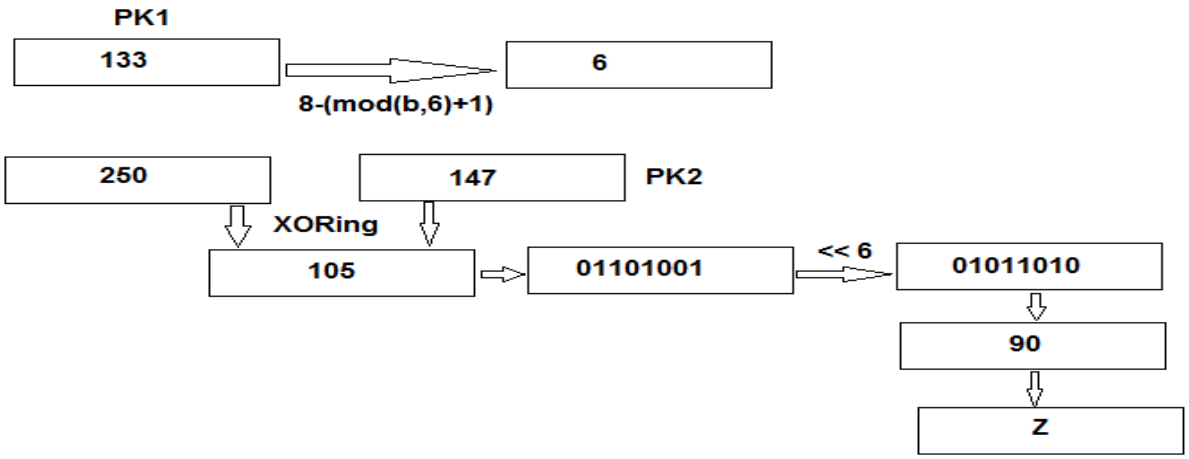

Figure 7: Example of using XORing and rotate left for decryption

Related Works

Many methods were introduced for data cryptography, many o them were based on data encryption standard (DES), mostly these methods share the following characteristics (some of the characteristics are considered as a disadvantages which need solving (see table 2)) [1-11]:

Table 2: Standard encryption methods features [1-11]

Method parameter	DES	3DES	AES	Blowfish
PK length(bit)	56(fixed)	112, 168(fixed)	128, 192, 256(fixed)	32-448(fixed)
Block size(bit)	64(fixed)	64(fixed)	128(fixed)	64(fixed)
Ability to deal with images	Difficult	Difficult	Difficult	Difficult
Encryption quality	Excellent: High MSE and low PSNR	Excellent: High MSE and low PSNR	Excellent: High MSE and low PSNR	Excellent: High MSE and low PSNR
Decryption quality	Excellent: Zero MSE and infinite PSNR	Excellent: Zero MSE and infinite PSNR	Excellent: Zero MSE and infinite PSNR	Excellent: Zero MSE and infinite PSNR
Efficiency	Slow	Slow	Slow	Moderate
Attack	Brute force attack	Brute force attack, Known plaintext, Chosen plaintext	Side channel attack	Dictionary attack
Structure	Feistel	Feistel	Substitution-Permutation	Feistel
Block cipher	Binary	Binary	Binary	Binary
Rounds	16(fixed)	48(fixed)	10,12,14(fixed)	16(fixed)
Flexibility to modification	no	yes	yes	yes

Methods based on DES technique have common features, some of the features are considered as disadvantages, bellow is the main features of these methods:

- Private key (PK): PK has a fixed length (some times it can be hacked), this key is used in generation other sub keys to be used in various rounds.

- Block size: Data is divided into equal blocks, block size usually fixed and small.
- Rounds: The process of cryptography (encryption-decryption) is accomplished using a fixed number of rounds, each round uses its own sub key and Feistel functions, the number of executed rounds negatively affect the efficiency of data cryptography (see figure 8).
- Data size: Increasing the data size will rapidly decrease the cryptography process efficiency.
- Simplicity: It is difficult to change the sequence of operations required to perform encryption and decryption phases, the number of rounds is fixed and cannot be changed, also the block size and the PK size are fixed and cannot be changed.

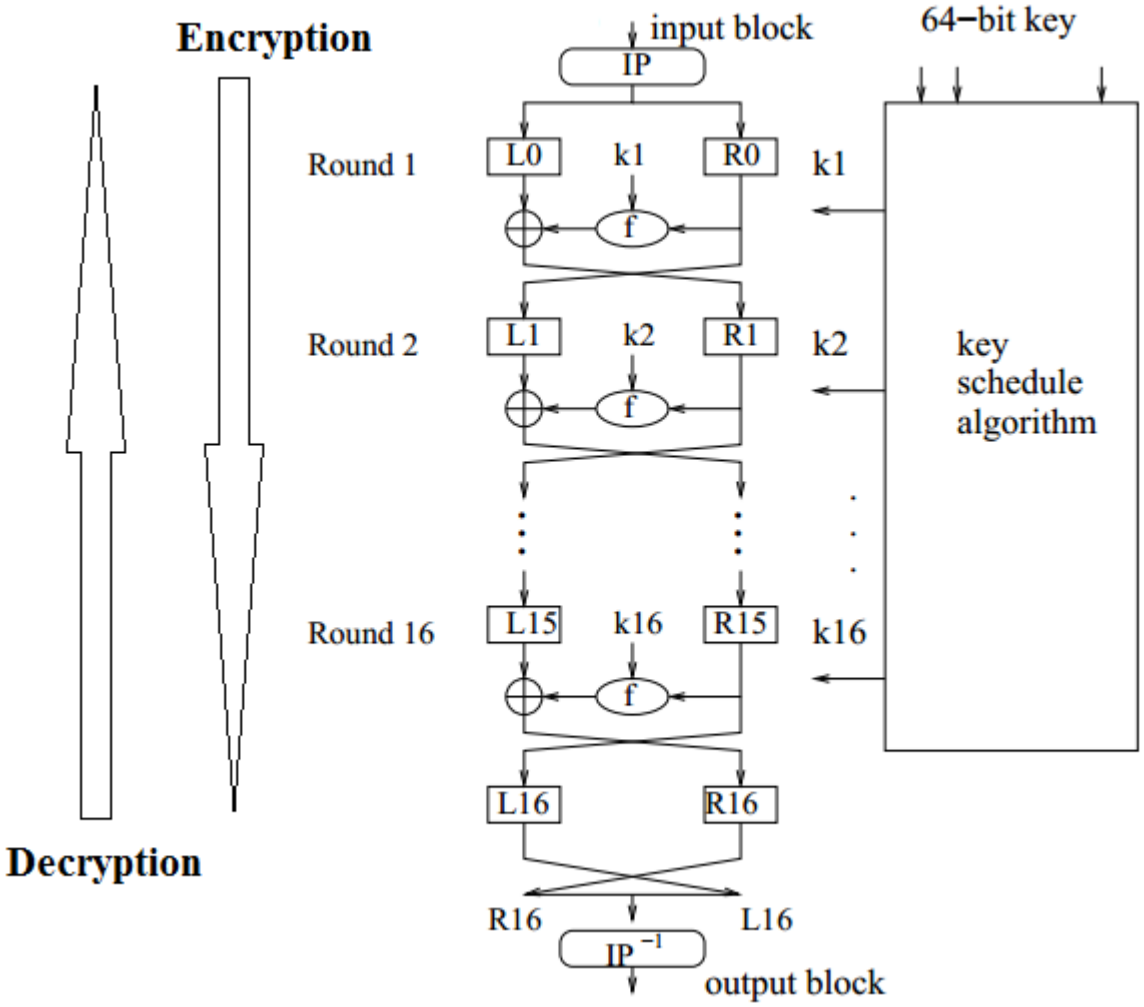

Figure 8: DES rounds

The Proposed Method

In the proposed method, we will use three digital images to generate the necessary keys for the following reasons:

- ✓ Ease of obtaining a digital color image at no cost due to the availability of various sources and the availability of equipment that can generate the digital image
- ✓ Easy to keep a digital photo
- ✓ Ease of digital image processing
- ✓ Ease of replacing the digital image with another if necessary
- ✓ Ease of use of each color matrix and ease of use of parts of the digital image.

Each selected image_key is to be resized to match the message size, the selected color in each image is determined by a secret key as shown in figure 9

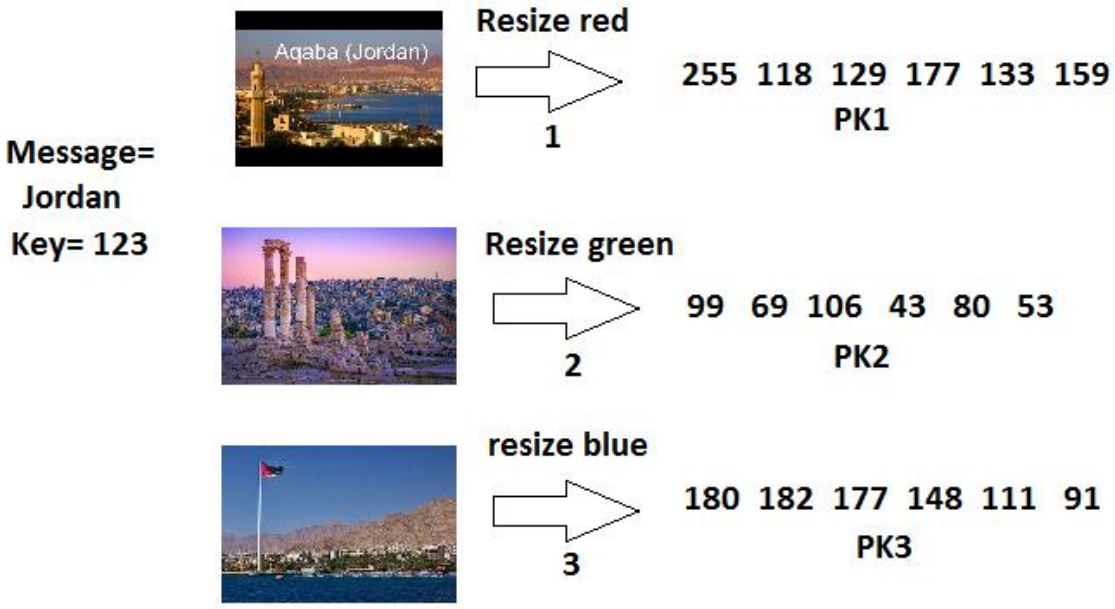

Figure 9: Image_keys resizing

The resized image_keys are to be used as a PKs, these PKs are used to generate the number of rotation right digits (RDL), these digits are used later in the data rotation process (see figures 10 and 11).

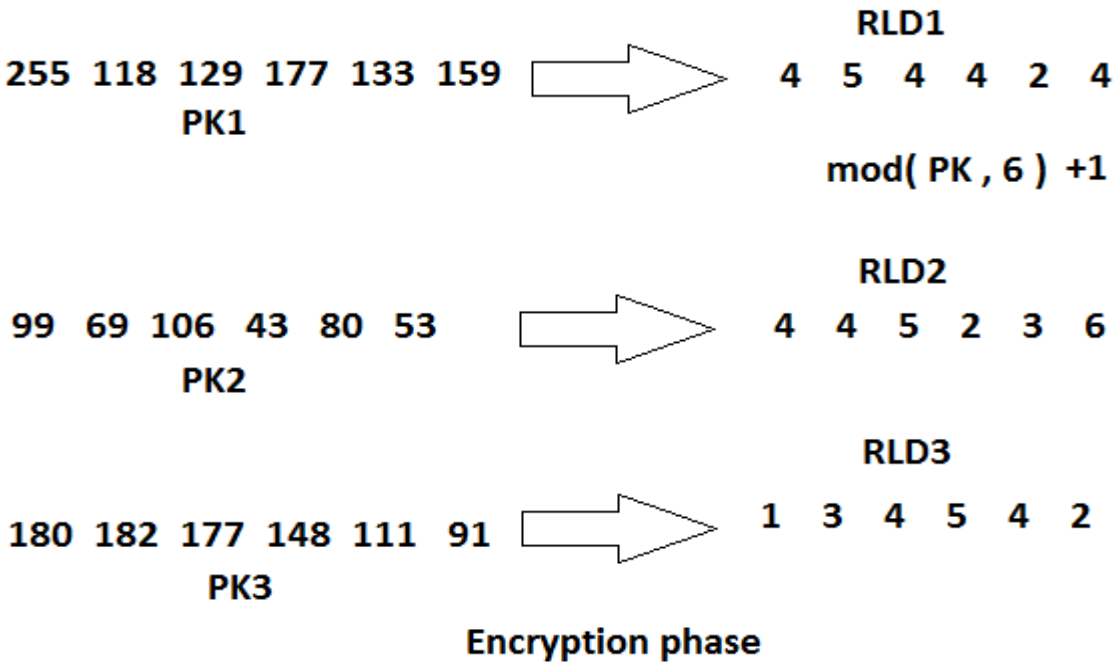

Figure 10: Generating RLDs in the encryption phase

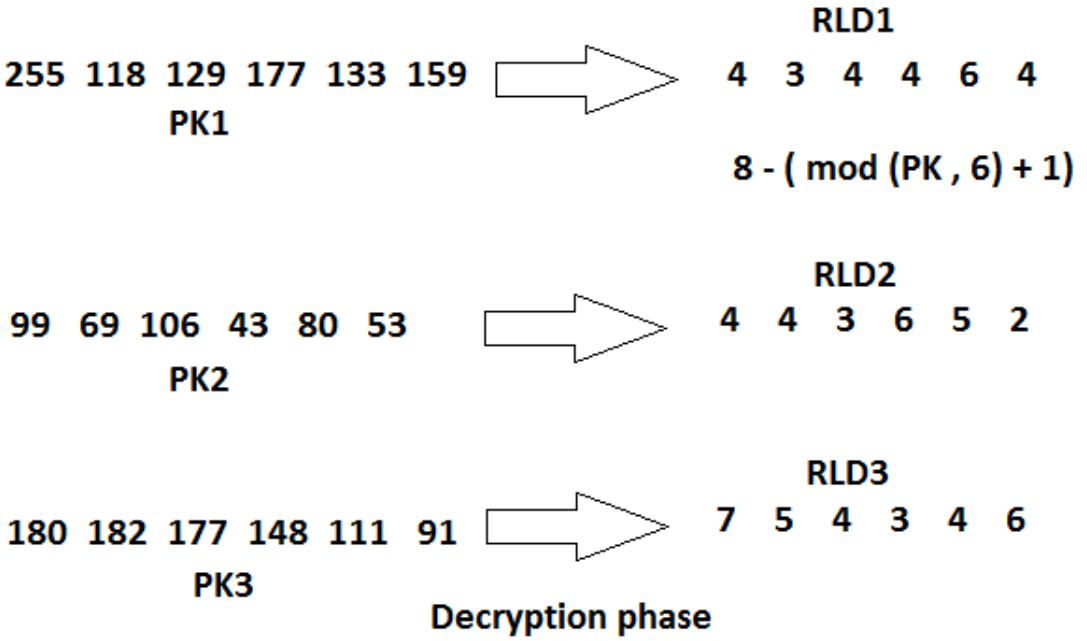

Figure 11: Generating RLDs in the decryption phase

In the encryption phase, each character in the secret message is to converted to decimal then to binary, the binary version is to be rotated right using the calculated RLDs, the three rotated results to be XORed to get the encrypted character as shown in figure 12

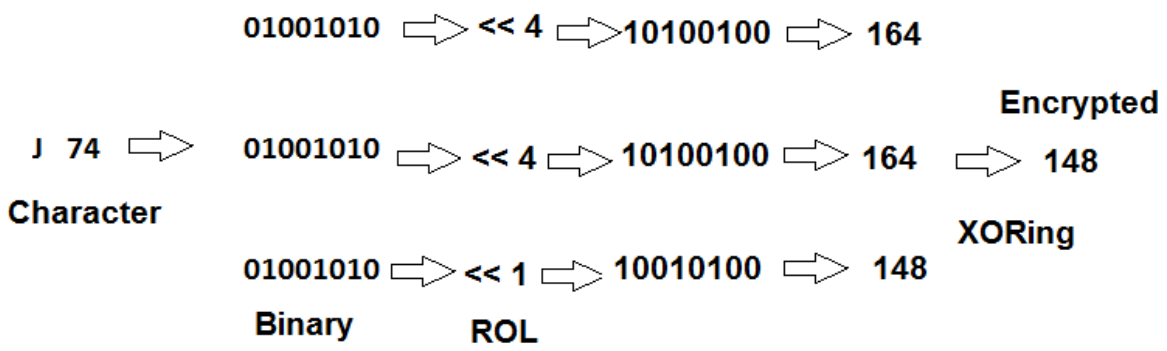

Figure 12: Encrypting 1 character

The decryption process will be performed in the same manner as in the encryption phase but using decryption RLDs as shown in figure 13.

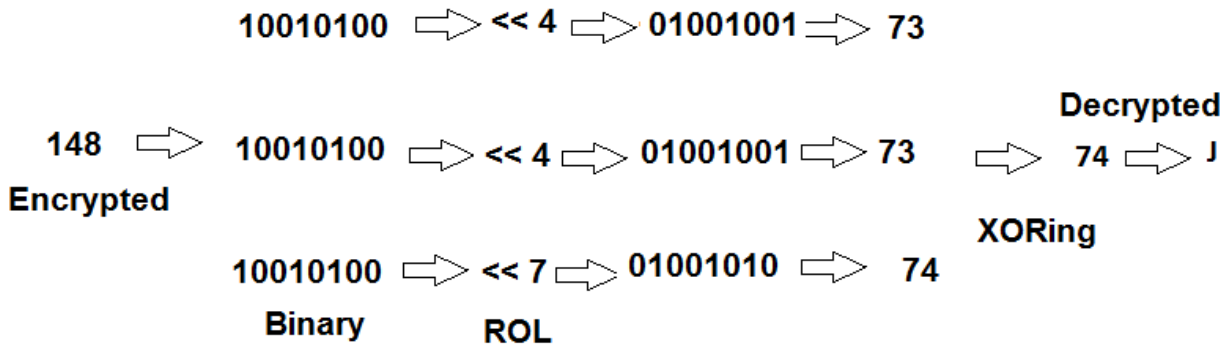

Figure 13: Decrypting 1 character

Below is the proposed method algorithm

Encryption phase/decryption

Inputs:

Three image_keys, secret message, key

Outputs

\Encrypted message

Process

1- *Get the inputs*

2- *Get the message length (L)*

3- *Resize each of the image_ keys to L*

4- *Use key to get PKs (see figure 9)*

5- *For each character calculate RLDs, and then use each of them to rotate the character right (see figures 10 and 11)*

6- *XOR the results in 5 to get the encrypted character (see figures 12 and 13)*

Implementation and Experimental Results

The proposed method was implemented using various images and messages, the messages were also encrypted-decrypted using DES method to make comparisons and to show how the proposed method increases the efficiency of message cryptography.

First we took short messages shown in table 3, the messages were encrypted-decrypted using DES method of data cryptography, figure 14 shows a sample output of the implementations, while table 4 shows the obtained results.

Table 3: Used short messages

Message number	Length (byte)	Message
1	35	Amman is the capital city of Jordan
2	27	Secret message cryptography
3	33	Using color image as an image_key
4	48	Aqaba is a beautiful city located on the red see
5	71	Aqaba is a beautiful city located on the red see in the south of Jordan
6	17	Mean square error
7	26	Peak signal to noise ratio
8	29	Three levels of data security
9	35	Encryption: Fully image destruction
10	32	Decryption: Fully image recovery
Average	35.3000	

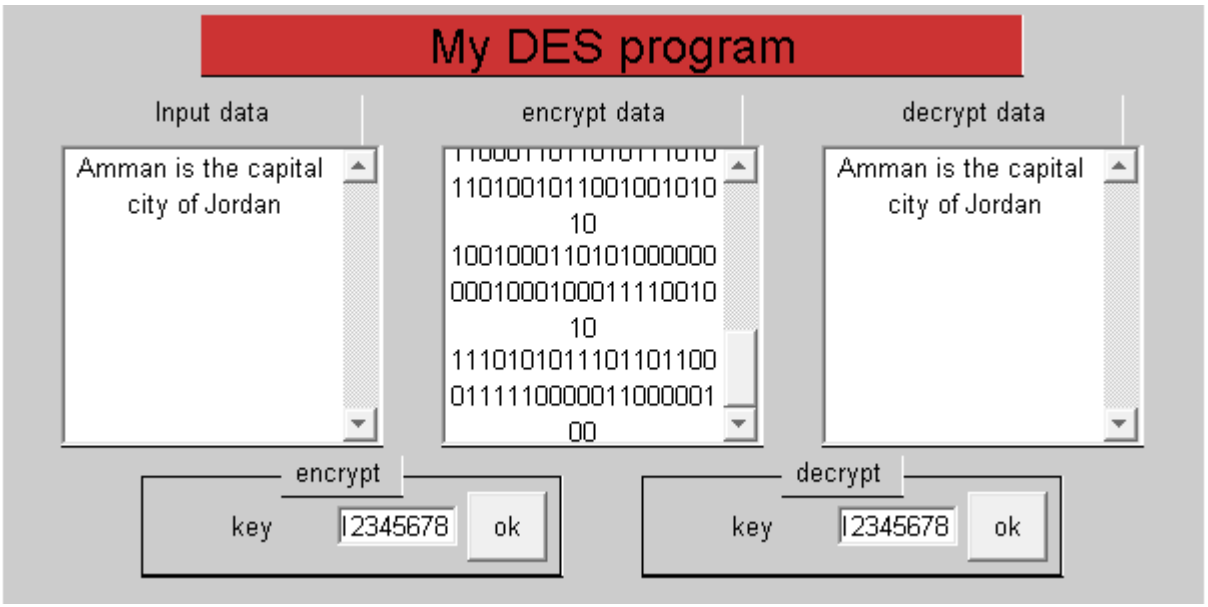

Figure 14: DES sample output (short message)

Table 4: Times results using DES (short messages)

Message number	Encryption time(second)	Decryption time(second)	Decryption throughput(byte per second)	Decryption throughput(byte per second)
1	0.0690	0.0820	507.2464	426.8293
2	0.0550	0.0810	490.9091	333.3333
3	0.0670	0.0810	492.5373	407.4074
4	0.0940	0.1070	510.6383	448.5981
5	0.1320	0.1460	537.8788	486.3014
6	0.0410	0.0710	414.6341	239.4366
7	0.0540	0.0760	481.4815	342.1053
8	0.0560	0.0780	517.8571	371.7949
9	0.0540	0.0760	648.1481	460.5263
10	0.0530	0.0750	603.7736	426.6667
Average	0.0675	0.0873	520.5104	394.2999

The same selected short messages were encrypted-decrypted using the proposed method, table 5 shows the obtained results:

Table 5: Times results using proposed method (short messages)

Message number	Image resizing time(second)	Encryption time(second)	TET(second)	TDET(second)	Decryption throughput(byte per second)	Decryption throughput(byte per second)
1	0.0530	0.0240	0.0770	0.0770	454.5455	454.5455
2	0.0470	0.0180	0.0650	0.0650	415.3846	415.3846
3	0.0480	0.0210	0.0690	0.0690	478.2609	478.2609
4	0.0470	0.0250	0.0720	0.0720	666.6667	666.6667
5	0.0480	0.0300	0.0780	0.0780	910.2564	910.2564
6	0.0470	0.0150	0.0620	0.0620	274.1935	274.1935
7	0.0470	0.0180	0.0650	0.0650	400.0000	400.0000
8	0.0470	0.0190	0.0660	0.0660	439.3939	439.3939
9	0.0480	0.0200	0.0680	0.0680	514.7059	514.7059
10	0.0470	0.0200	0.0670	0.0670	477.6119	477.6119
Average			0.0689	0.0689	503.1019	503.1019

From tables 4 and 5 we can see that proposed method encryption efficiency is closed to DES efficiency, while the proposed method added an enhancement to the decryption efficiency.

Medium in length messages were selected and treated using DES and the proposed methods, figure 15 shows a sample output of DES implementation; table 6 shows the obtained results for DES method, while table 7 shows the obtained results for the proposed method.

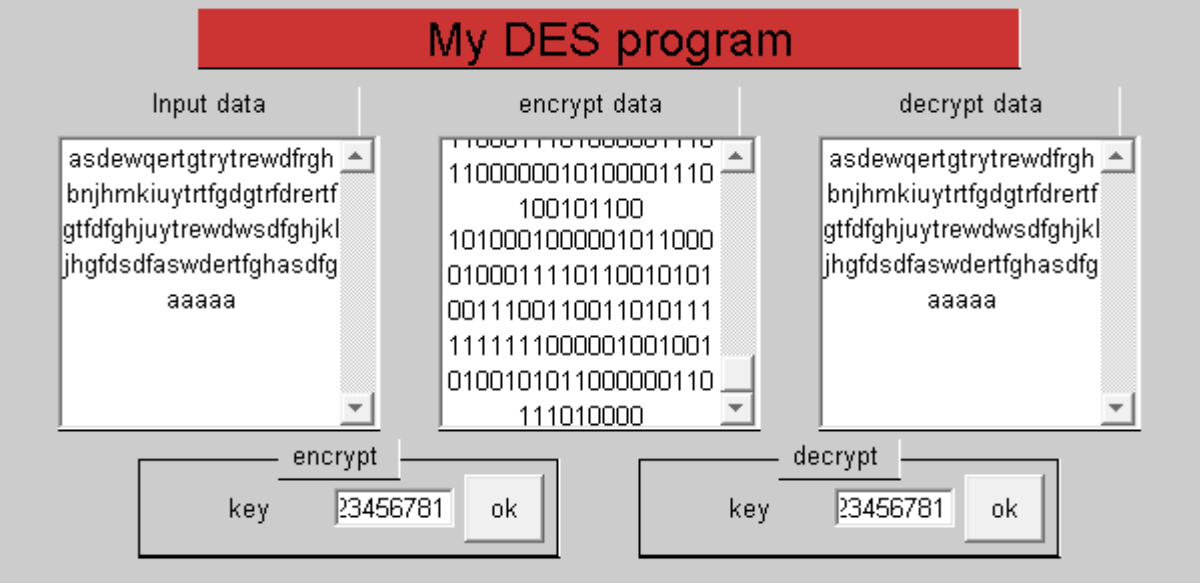

Figure 15: DES sample output (short medium message)

Table 6: Times results using DES method (medium messages)

Message length (byte)	Encryption time(second)	Decryption time(second)	Encryption throughput(byte per second)	Decryption throughput(byte per second)
100	0.1721	0.2506	581.0575	399.0423
200	0.3742	0.5012	534.4735	399.0423
300	0.5664	0.7508	529.6610	399.5738
400	0.7675	1.0045	521.1726	398.2081
500	0.9506	1.2581	525.9836	397.4247
600	1.1507	1.5117	521.4217	396.9041
700	1.3348	1.7653	524.4231	396.5332
800	1.5270	2.0229	523.9031	395.4718
900	1.7091	2.2725	526.5929	396.0396
1000	1.9112	2.5261	523.2315	395.8671
Average	1.0464	1.3864	520.5104	394.2999

Table 7: Times results using proposed method (medium messages)

Message length (byte)	Image resizing time(second)	Encryption time(second)	TET(second)	TDET(second)	Decryption throughput(byte per second)	Decryption throughput(byte per second)
100	0.0460	0.0400	0.0860	0.0860	1162.8	1162.8
200	0.0470	0.0680	0.1150	0.1150	1739.1	1739.1
300	0.0470	0.0990	0.1460	0.1460	2054.8	2054.8
400	0.0460	0.1220	0.1680	0.1680	2381.0	2381.0
500	0.0480	0.1580	0.2060	0.2060	2427.2	2427.2
600	0.0470	0.1860	0.2330	0.2330	2575.1	2575.1
700	0.0470	0.2150	0.2620	0.2620	2671.8	2671.8
800	0.0480	0.2440	0.2920	0.2920	2.7397	2.7397
900	0.0470	0.2780	0.3250	0.3250	2769.2	2769.2
1000	0.0460	0.3150	0.3610	0.3610	2770.1	2770.1
Average			0.2194	0.2194	2055.4	2055.4
Speedup of the proposed method					3.9488	5.2128

From table 6 and 7 we can see that the proposed method increases the throughput of encryption and decryption process and the proposed method has a significant speedup comparing with DES method.

Increasing the message size will keep the proposed method efficient, table 8 shows that the proposed method provides an average throughput equal 3 K bytes per second when dealing with long length messages, this throughput will increase when increasing message length as shown in figure 16.

Table 8: Times results using proposed method (Long messages)

Message length (K byte)	Image resizing time(second)	Encryption time(second)	TET(second)	TDET(second)	Decryption throughput(byte per second)	Decryption throughput(byte per second)
1	0.0490	0.3210	0.3700	0.3700	2767.6	2767.6
2	0.0460	0.6560	0.7020	0.7020	2917.4	2917.4
3	0.0470	0.9360	0.9830	0.9830	3125.1	3125.1
4	0.0480	1.2630	1.3110	1.3110	3124.3	3124.3
5	0.0480	1.5250	1.5730	1.5730	3254.9	3254.9
6	0.0490	1.8340	1.8830	1.8830	3262.9	3262.9
7	0.0490	2.1710	2.2200	2.2200	3228.8	3228.8
8	0.0470	2.4880	2.5350	2.5350	3231.6	3231.6
9	0.0480	2.8450	2.8930	2.8930	3185.6	3185.6
10	0.0490	3.4510	3.5000	3.5000	2925.7	2925.7
20	0.0510	6.5380	6.5890	6.5890	3108.2	3108.2
50	0.0540	17.2030	17.2570	17.2570	2966.9	2966.9
Average			3.4847	3.4847	3091.6	3091.6

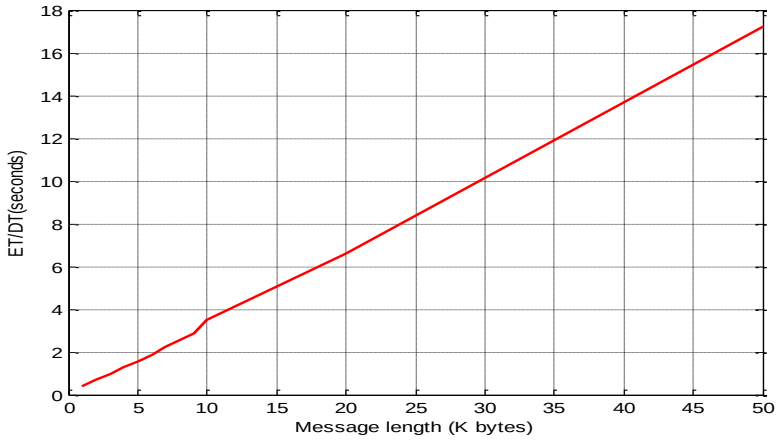

Figure 16: Throughput vs message length

The proposed method was tested for quality, the MSE between the decrypted message and the original one was always zero, while the PSNR between them was always infinite. MSE between the encrypted and the original message was very high, and the PSNR between them was very low, which means that the encryption process destroys the message making it unreadable, the obtained results shown in table 9 proves these facts.

Table 9: Quality results of the proposed method

Message length (byte)	MSE	PSNR	CC
100	1.0316e+004	18.3324	0.0083
200	7.6594e+003	21.3098	0.2255
300	7.5468e+003	21.5365	0.2908
400	8.0546e+003	20.8853	0.2670
500	7.7552e+003	21.2641	0.2529
600	8.7266e+003	20.0839	0.2230
700	8.4705e+003	20.3818	0.2107
800	8.1533e+003	20.7635	0.2439
900	8.1791e+003	20.7319	0.2575
1000	8.5191e+003	20.3246	0.2135

Conclusion

A simple and easy to implement method of data cryptography was proposed. The method increases the level of security by providing a high degree of message protection; this was done thru the use of special key to determine the color channel to be used to formulate the PK. Three color image-keys were used to extract the PKs; the contents of each PK were used to calculate the required RLDs to apply character rotation. The obtained results showed that the proposed method provided a significant speedup comparing with DES method and the proposed method adds a good enhancement in the encryption and decryption processes. The method was tested for quality and the obtained results of MSE, PSNR and CC during the encryption and decryption phases were acceptable.

References

[1]. Diaa Salama Abdul. Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12, pp. 280-286, December 2008.

[2]. W. Stallings, Cryptography and Network Security, 4th Edition, Pearson Prentice Hall, 2006.

[3]. Singh S Preet, Mani Raman, "Comparison of Data Encryption Algorithms", International Journal of Computer science and Communications, Vol. 2, No.1, January-June 2011, pp. 125-127.

[4]. Singh Gurjeevan, Kumar Ashwani, Sandha K.S. "A Study of New Trends in Blowfish Algorithm" International Journal of Engineering Research and Applications (IJERA), Vol. 1, Issue 2, pp.321-326.

[5]. Agrawal Monika, Mishra Pradeep, "A Comparative Survey on Symmetric Key Encryption Techniques", International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 05 May 2012, pp. 877-882.

[6]. Seth Shashi Mehrotra, Mishra Rajan, "Comparative analysis of Encryption algorithm for data communication", International Journal of Computer Science and Technology, vol. 2, Issue 2, June 2011, pp. 292-294.

[7]. Mandal Pratap Chandra, "Superiority of Blowfish Algorithm" IJARCSSE, volume 2, Issue 9, September 2012, pp. 196-201.

[8]. Apoorva, Kumar Yogesh, "Comparative Study of Different Symmetric Key Cryptography", IJAIEM, vol. 2, Issue 7, July 2013, pp. 204-206.

[9]. Abdul D.S, Kader H.M Abdul, Hadhoud, M.M., "Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMA, Volume 8, 2009, pp. 58-64.

[10]. Abdul D.S, Kader H.M Abdul, Hadhoud, M.M., "Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMA, Volume 8, 2009, pp. 58-64.

[11]. Thakur Jawahar, Kumar Nagesh. "DES, AES and Blowfish Symmetric Key Cryptography algorithm Simulation Based Performance Analysis", IJETAE, vol. 1, Issue 2, DEC. 2011, pp. 6-12.

[12]. 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.

[13]. 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.

[14]. 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.

[15]. 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.

[16]. 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.

[17]. 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.

[18]. 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.

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

[20]. 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.

[21]. 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.

[22]. 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.

[23]. 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.

[24]. 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.

[25].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.

[26].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.

[27]. 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.

[28].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.

[29]. 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.

[30]. 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.

[31]. 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.

[32]. 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.

[33]. 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.

[34]. 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.

[35]. 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.

[36]. 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.

[37]. 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.

[38]. 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.

[39].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.

[40].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.

[41].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.

[42]. 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.

[43]. 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.

[44]. 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.

[45]. 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.

[46]. 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.

[47]. 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.

[48]. 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.

[49]. 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.

[50]. 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.

[51]. 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.

[52]. 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.

[53]. 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.

[54]. 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.

