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.190 – 211

DES Based Method to Improve Color Image Cryptography

Akram Naser Adam Mousa*; Talal Bukewitin*; Tarek R. S. Al Aga
*Higher Institute for Science and Technology
Bayda, Libya
College of Computer Technology Zawia,
Ministry for Technical and Vocational Education, Libya

DOI: https://doi.org/10.47760/ijcsmc.2022.v11i06.014

Abstract:

Color image cryptography is one of the popular methods used to protect data from being hacked. In this research paper a novel method of color image cryptography will be introduced, tested and implemented. This method will enhance some features of the DES standard by increasing the level of security and providing a high degree of image protection. Two image_keys will be used to generate two sets of primary keys, the first set will be used to calculate RLDs for each value in the image, the second set will be used to apply XORing operations, the two images must be kept in secret, the user has the ability to replace these images when needed without modifying the method.
The proposed method will divide the image to be encrypted (decrypted) into block, the block size is variable and the user must determine the block size. The process of cryptography can be accomplished using a selected number of rounds, the number of rounds is also determined by the user, more number of rounds are needed to optimize the values of MSE and PSNR between the source and the encrypted images. The method will use a variable length private key; this length will depend on the selected number of rounds and the selected block size.
The proposed method will be implemented; the obtained results will be compared with DES results to show how the proposed method improves the efficiency of color image cryptography.

Keywords: Cryptography, image_key, resizing, RLD, PK, MSE, PSNR, CC, TP.

Introduction

Digital color image [48-56] is very important type of digital data, because it is widely used in many important and vital applications for many reasons, the most important of them are:

- Ease of obtaining them and at the lowest cost due to the multiplicity of devices that generate them and the multiplicity of sources through which they can be obtained [1- 5].
- The color image is represented by a three-dimensional matrix (see figure 1), which makes the process of processing it easy, because the process of digital image processing is nothing but the process of processing matrices[6-11].
- The matrix of each of the three colors (red, green and blue) can be processed separately, and any of these matrixes can be used to perform a specific operation [12-18].

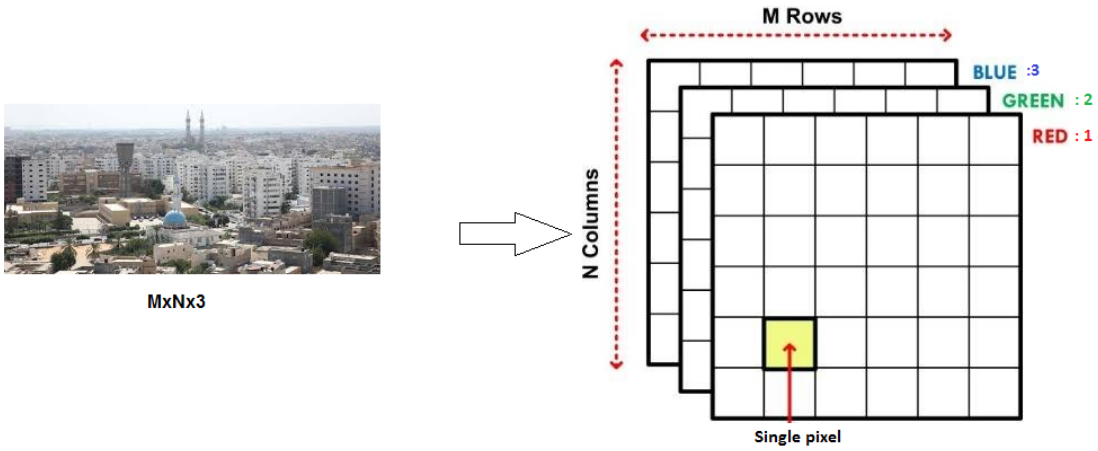

Figure 1: Color image 3D matrix

- Image matrix can be resized to a specified number of elements, this feature is very useful and it can easily be used to generate private keys (PK) with various lengths as shown in figure 2 [20-24].

- Easy of implementing logical operations such as rotating left to a specific digits and XORing, these operations are widely used in encryption-decryption as shown in figures 3 and 4 [19].

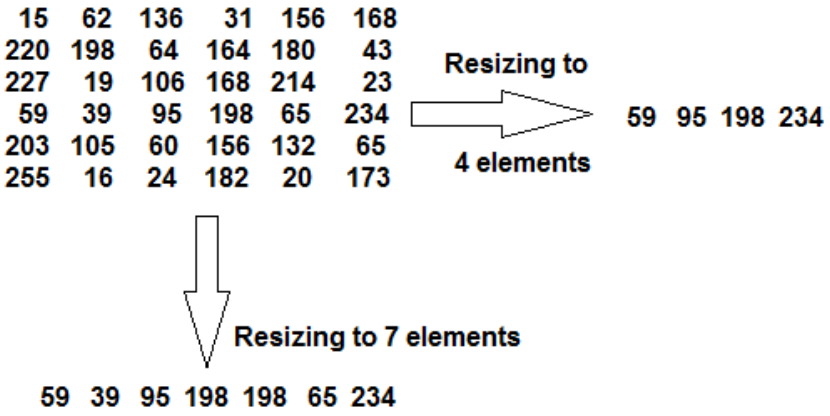

Figure 2: Various ways of matrix resizing

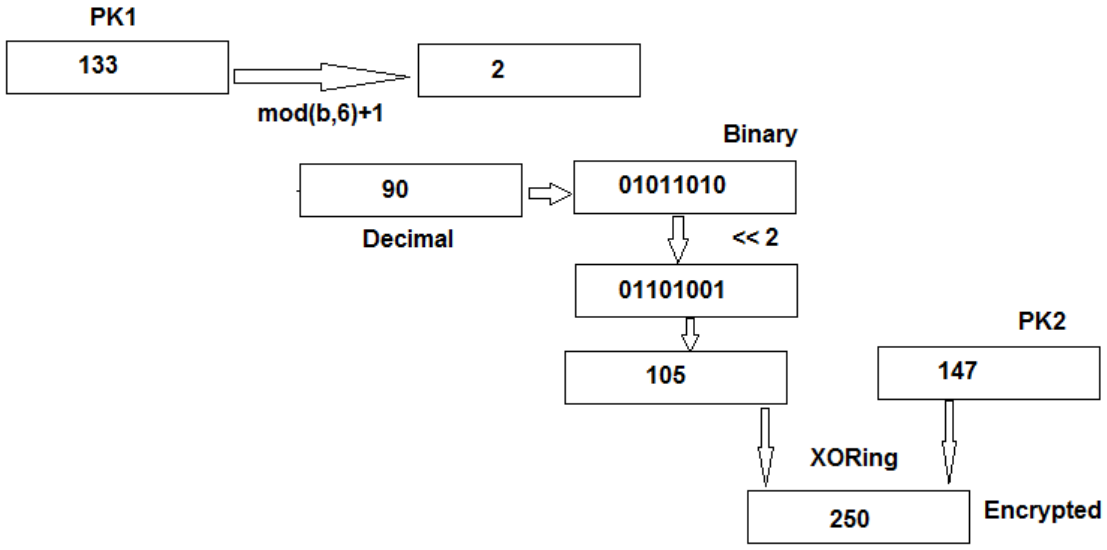

Figure 3: Using logical operations to encrypt a decimal value

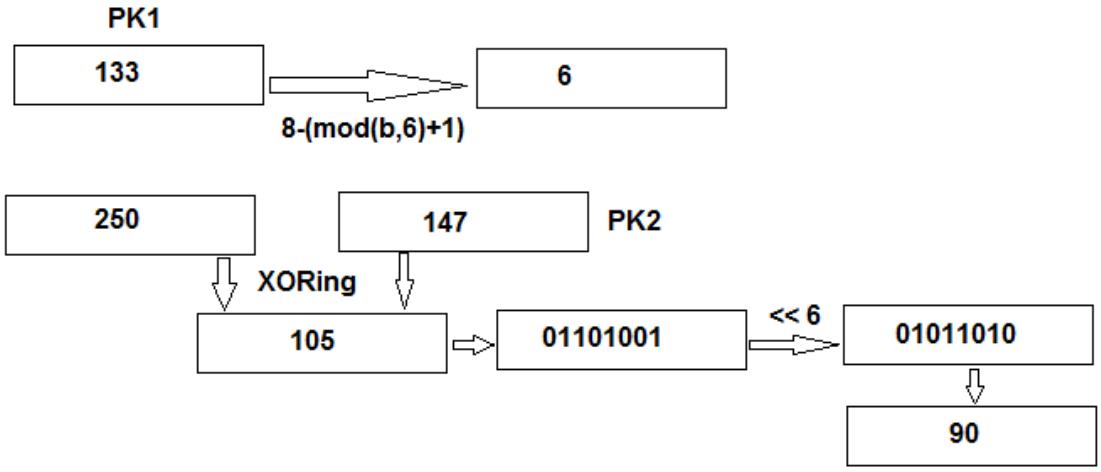

Figure 4: Using logical operations to decrypt a decimal value

The color digital image often requires protection from hacking and protection from data thieves when sending the image through various social media for many reasons, the most important of which are [25-30]:

- The image may be of a personal nature and no unauthorized person has the right to view it
- The image may be important and very confidential
- The digital image may contain confidential data that has been included in the digital image using not secure method of data steganography [31-36].

Data cryptography is one of the famous and widely used method to protect data from any danger, it can be done (as shown in figure 5) by applying a sequence of operations using one or more secret private key (PK), this key is to be selected by the sender and agree upon with the receiver [37-40].

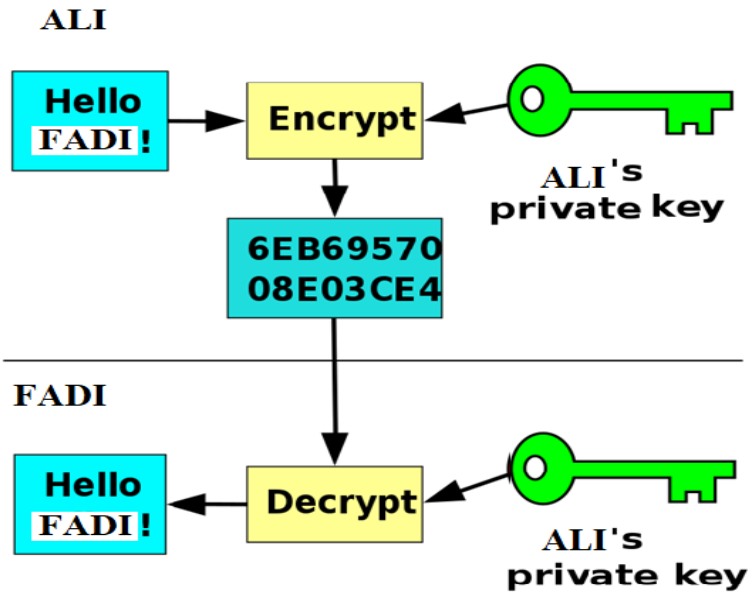

Figure 5: Data cryptography process

The level of security and protection for the data provided by the method of data cryptography depends on the length and complexity of the private key and the complexity of the operations used in the method of data cryptography.
Data cryptography (as shown in figure 5) means encrypting the data before sending and decrypting the data after receiving. The data encryption process is used to destroy it completely and make it incomprehensible and useless to any third party. As for the decryption process, it means returning data that is exactly the same as the original data without any change. The level of destruction and the level of data recovery between two images can be measured using the quality parameters: Mean square error (MSE), peak signal to noise ratio (PSNR) and correlation coefficient (CC), for a high level of destruction MSE must be very high, while PSNR and CC must be very low, for a full recovery of the original data MSE must equal zero, PSNR must equal infinite, and CC must equal 1. MSE, PSNR and CC can be calculated between two data sets using equations 1, 2, and 3, figure 6, 7 and 8show the expected values of the quality parameters after applying encryption and decryption processes [41-49].

MSE of x channel

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

Total MSE

$$MSE_t = MSE_R + MSE_G + MSE_B$$

Calculate PSNR

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

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

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

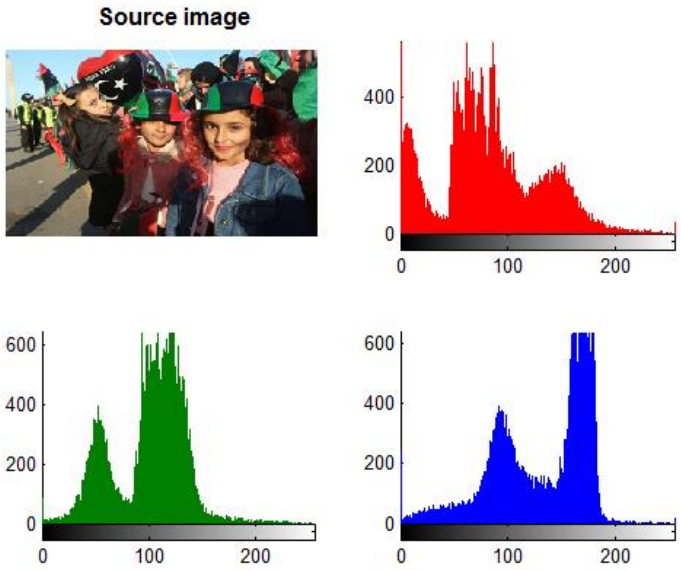

Figure 6: Source image example

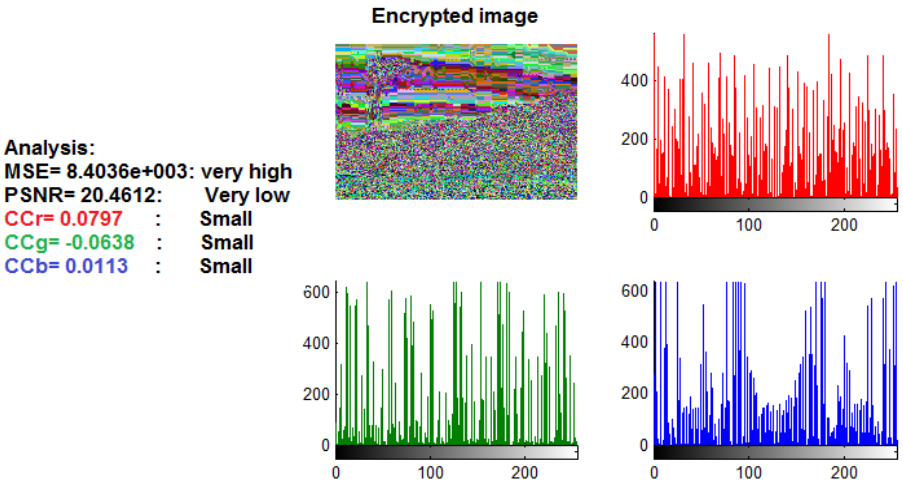

Figure 7: Encrypted image

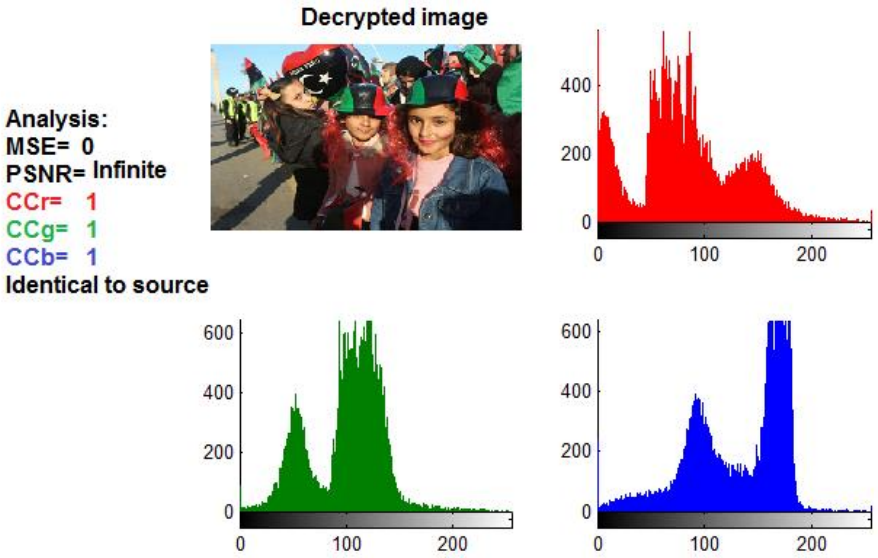

Figure 8: Decrypted image

Related Works

Many methods are used in data cryptography; many of them are based on the standards: DES (data encryption standard), AES (advanced encryption standard), 3DES, and blowfish (BF) [15-19], these methods share some characteristics which are considered as disadvantages. Here we will focus on DES and the comparisons will based on DES results of data cryptography. Table 1 shows some features of DES and how to improve theses features[50-51].

Table 1: DES features to be improved

Feature	Description	Improvement
Block size	Block size is fixed and it cannot be changed, block size = 8 bytes (64 bits) (see figure 9)	Block size must be variable and it must be selected by the sender and receiver and must be kept in secret to avoid hacking.
Private key	One private key is used, it has a fixed size which is equal 56 bits, and it can be hacked	Long private key is required, multiple variable length PKs must be used, this will increase the level of data security
Key scheduling	PK is used to generate other keys used to accomplish data cryptography process	Other data sets can be used to generate variable length PKs, these data set can be color image_keys, and it is easy to keep them in secret

Rounds	16 rounds are used (see figure 10)	Variable number of rounds must be used, this number must be selected by the user and must be kept in secret and agree upon between the sender and receiver
Quality of encryption-decryption	Excellent values for MSE, PSNR and CC	-
Ability to color image cryptography	Hard	Must be easy
Throughput	Poor, especially when the data to be encrypted is a color image	Must be high by reducing the encryption-decryption time
Level o protection	Low and it can be hacked	Must be very high by making the hacking process impossible

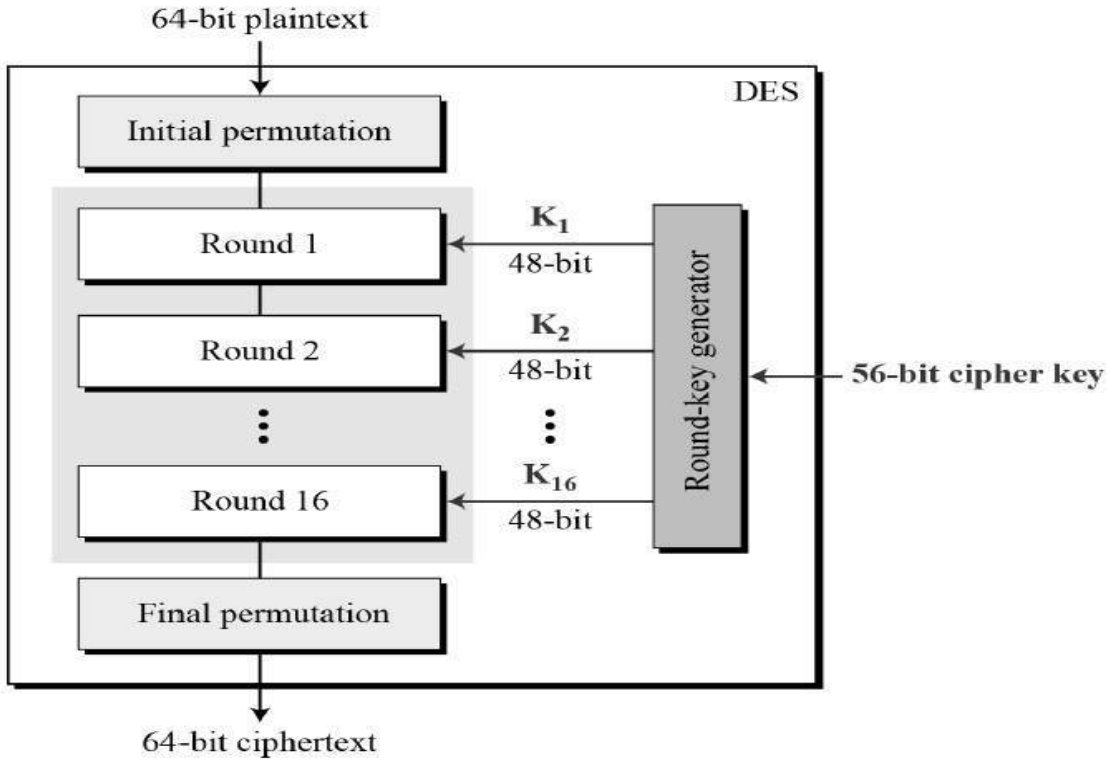

Figure 9: DES architecture

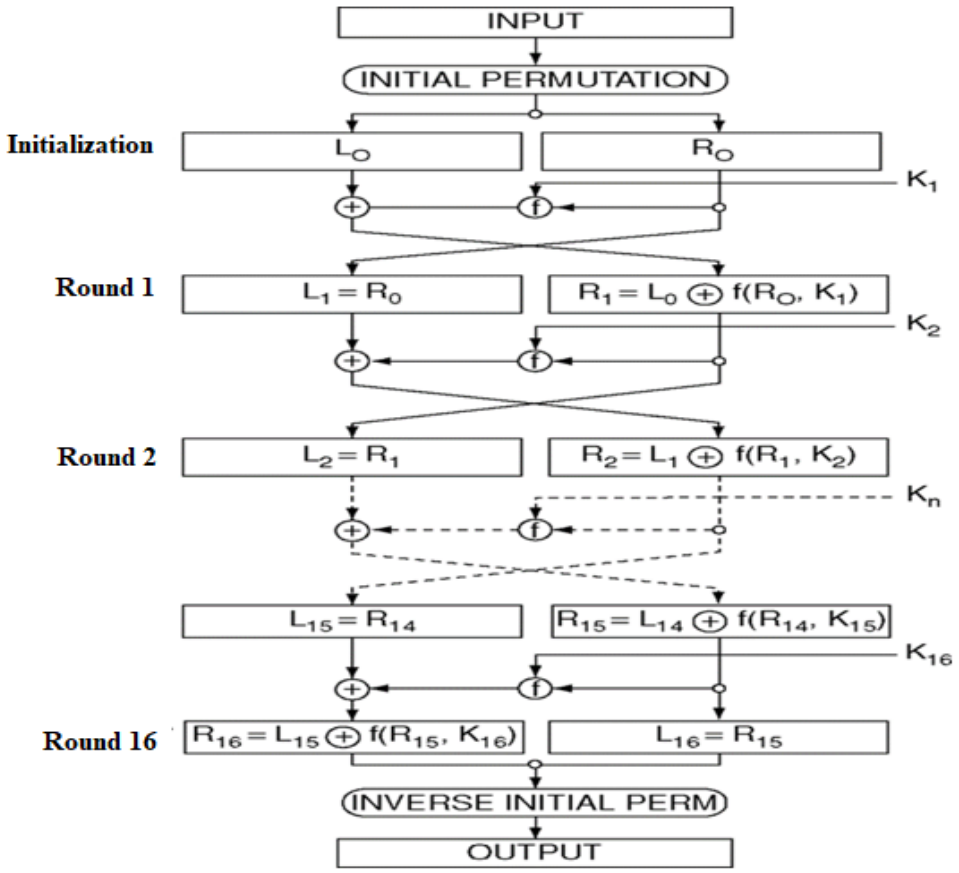

Figure 10: DES rounds

The Proposed Method

The proposed method divides the color image to be encrypted into equal block, block size is variable, the block size must be used as an input to the proposed method and it must be kept in secret by both the data sender and receiver. Block size length can be updated from time to time and when the needs arise. The proposed method uses two image_key to generate two sets of private keys. The first PK elements are to be used to calculate the number of rotation left digits(RLD) used to rotate the color value in the image, while the second PK elements are used to apply XORing operations. The length in bytes of each of the two PKs depends on the block size and selected number or rounds used to accomplish data cryptography. Here the number of rounds also must be used as an input to the proposed method and must be kept in secret with the ability to change it from time to time if needed.

The proposed method uses two color images as an image_keys to generate the private keys PK1 and PK2. The length of each PK will equal the block size in bytes multiplied by the number of selected rounds of data cryptography. PK1 will be used to calculate various RLDs required for data rotation and the RLD in the encryption phase will equal mod(PK 1 value,6) +1, while in the decryption phase RLD will equal 8-(mod(PK 1 value,6)+1). PK 2 values will be used to apply XORing operations. Figures (11 and 12) show an example of PK1 and PK2 generations in the encryption and decryption phases:

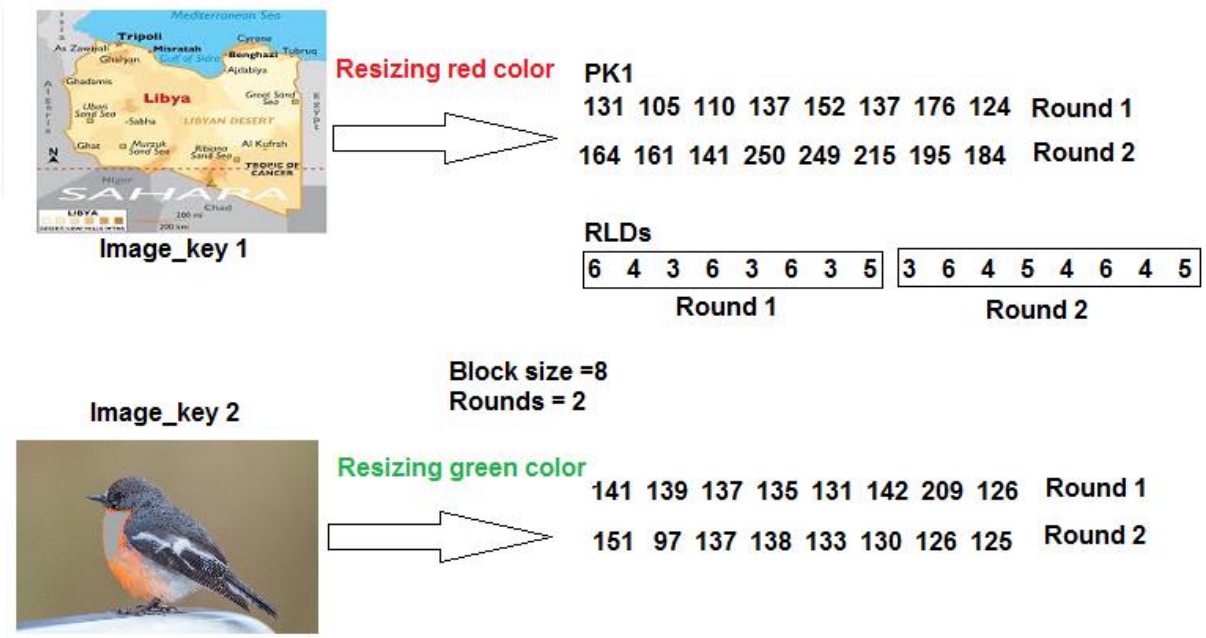

Figure 11: Generating PKs in the encryption phase

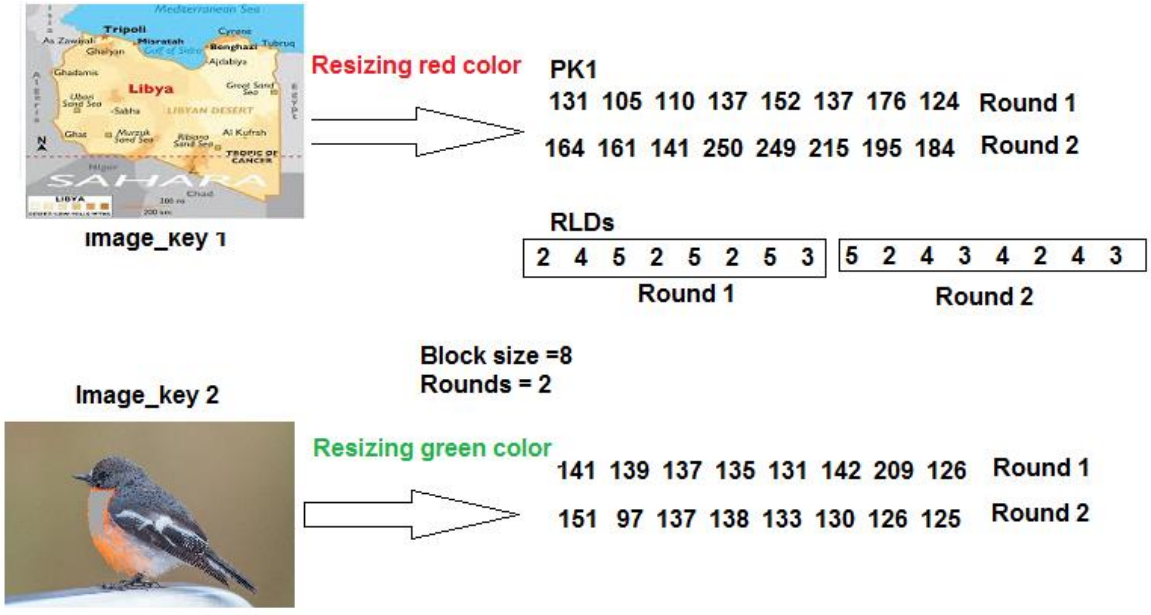

Figure 12: Generating PKs in the decryption phase

The proposed method requires at least one round to perform encryption and decryption, the number of rounds can be increases depending on the use wishes, increasing the number of rounds will increase the security level, but the throughput will be decreased. Figures (13 and 14) show a two rounds block diagram of the proposed encryption and decryption.

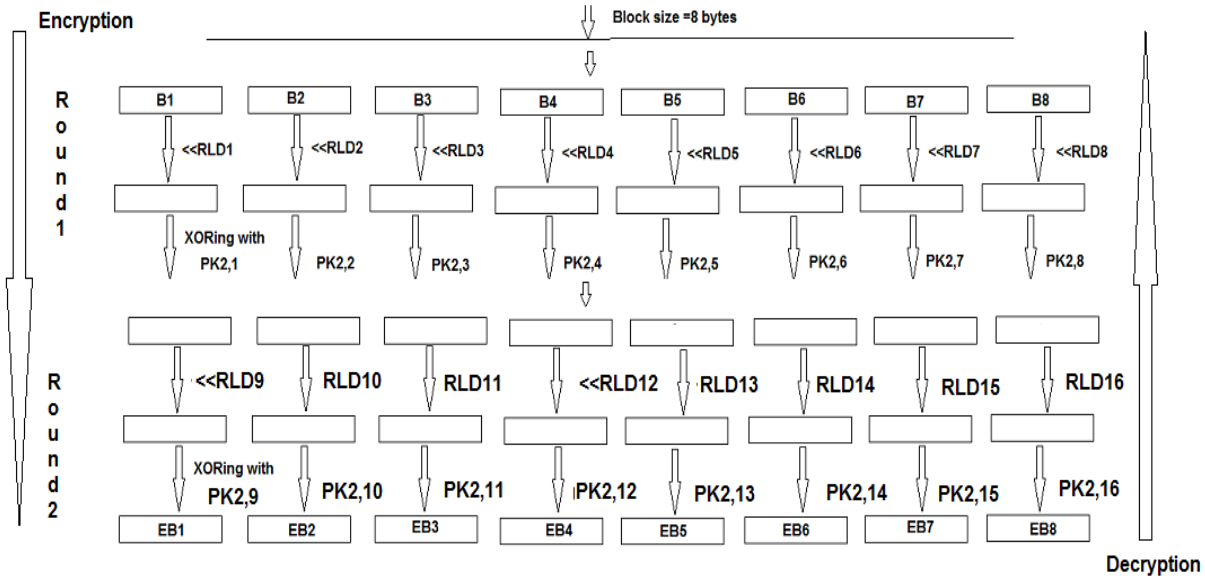

Figure 13: Two rounds of the proposed encryption

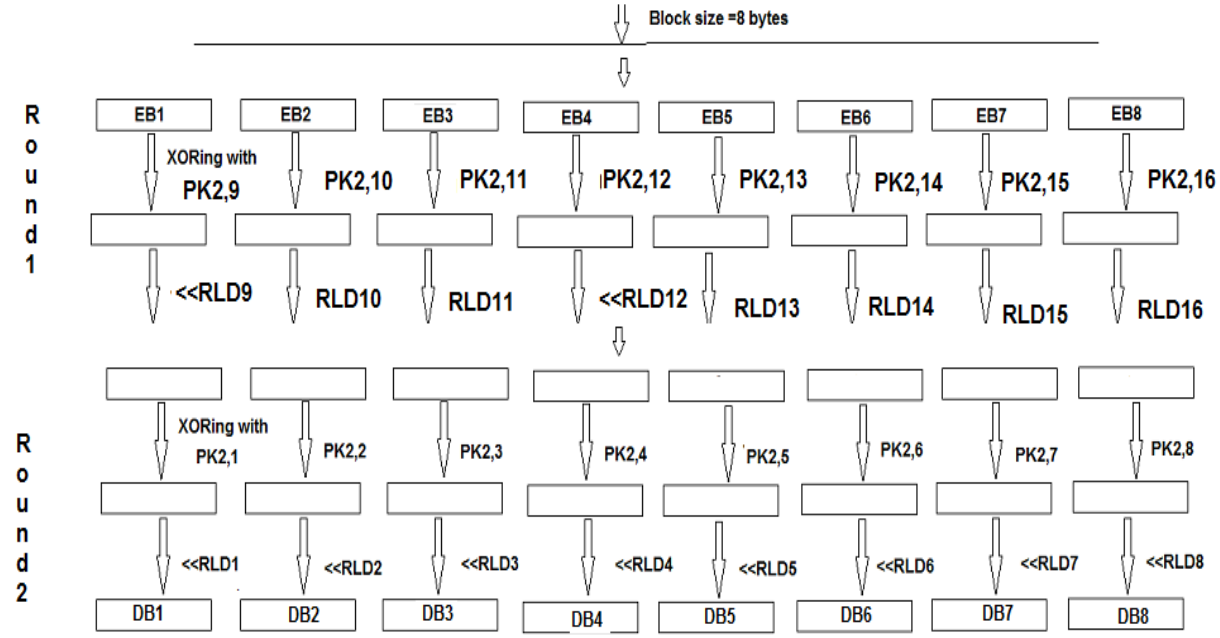

Figure 14: Two rounds of the proposed decryption

The color image to encrypted-decrypted must be reshaped from 3D matrix to one row matrix as illustrated in the example shown in figure 15.

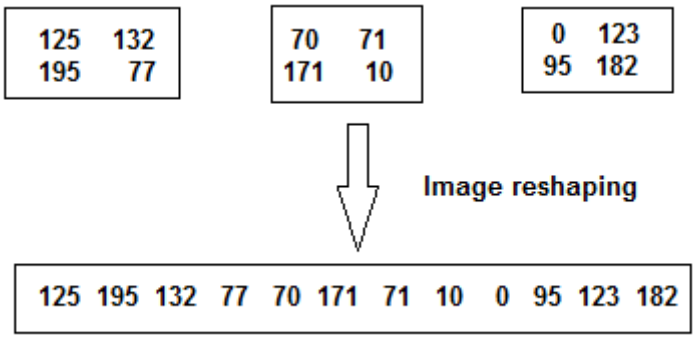

Figure 15: Example of 3D matrix reshaping

Below is the proposed algorithm of color image cryptography:

Encryption phase

Inputs:

Color image to be encrypted (C), two image_keys (I1, I2), and block size in bytes (BS), number of rounds (NR).

Outputs:

Encrypted image (E)

Process:

1. *Get the inputs*
2. *Reshape C to one row matrix (RC)*
3. *Divide RC into blocks using BS*
4. *Resize I1 and I2 to BS*NR to get PK1 and PK2*
5. *For each block do*
6. *For each round do*
7. *From PK1 calculate RLDs*
8. *Rotate each byte in the block left using the associated RLD*
9. *XOR the results obtained in 8 using the associated value from PK2*
10. *Pad the encrypted block to the encrypted one row matrix*
11. *Reshape back one row matrix to 3D matrix to get the encrypted image (E)*

Decryption phase

Inputs:

Color image to be decrypted (E), two image_keys (I1, I2), and block size in bytes (BS), number of rounds (NR).

Outputs:

Decrypted image (D)

Process:

1. *Get the inputs*
2. *Reshape E to one row matrix (RE)*
3. *Divide RE into blocks using BS*
4. *Resize I1 and I2 to BS*NR to get PK1 and PK2*
5. *For each block do*
6. *For each round do*
7. *From PK1 calculate RLDs*
8. *XOR block byte with the associated value from PK2*
9. *Rotate Results in step 8 left using the associated RLD*
10. *Pad the decrypted block to the decrypted one row matrix*
11. *Reshape back one row matrix to 3D matrix to get the decrypted image (D)*

Implementation and Experimental Results

For comparisons purposes DES was implemented using various images, figure 16 shows an implementation task, while table 2 shows the obtained experimental results.

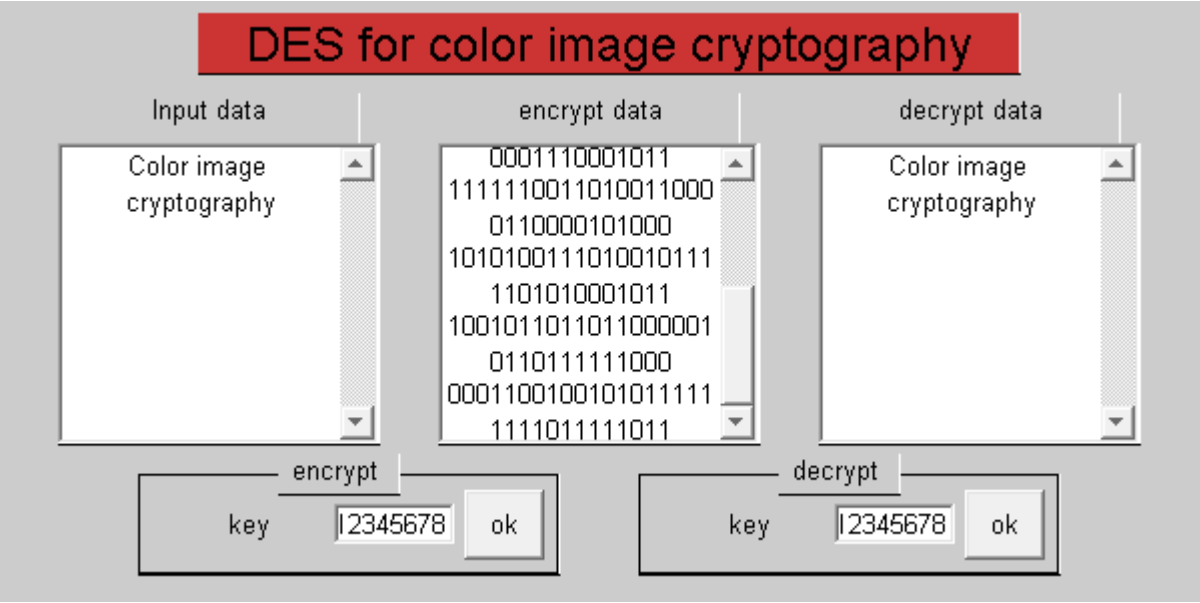

Figure 16: DES implementation results

Table 2: DES results

Image number	Size (byte)	ET(second)	DT(second)	ETP(byte per second)	DTP(byte per second)
1	150849	341	491	442.3724	307.2281
2	77976	172	252	453.3488	309.4286
3	518400	1174	1688	441.5673	307.1090
4	5140800	11638	16816	441.7254	305.7088
5	4326210	9778	14168	442.4432	305.3508
6	122265	269	400	454.5167	305.6625
7	518400	1154	1678	449.2201	308.9392
8	150975	325	484	464.5385	311.9318
9	150975	325	484	464.5385	311.9318
10	151353	340	486	445.1559	311.4259
11	1890000	4306	6120	438.9224	308.8235
12	6119256	13912	20001	439.8545	305.9475
Average	1609800	3644.5	5255.7	448.1836	308.2906

From table 2 we can see that the encryption (decryption) time will rapidly increased when increasing the image size, an image with big size will require hours to be encrypted.

The proposed method was implemented using the same condition as for DES (Block size (BS) = 8 bytes, and number of rounds (NR) =16), table 3 shows the obtained experimental results

Table 3: Results using the proposed method (BS=8 bytes, NR=16)

Image number	Size (byte)	ET(second)	DT(second)	ETP(byte per second)	DTP(byte per second)
1	150849	339.7820	339.7820	443.9582	443.9582
2	77976	177	177	440.5424	440.5424
3	518400	1178	1178	440.0679	440.0679
4	5140800	11676	11676	440.2878	440.2878
5	4326210	9818	9818	440.6407	440.6407
6	122265	277	277	441.3899	441.3899
7	518400	1168	1168	443.8356	443.8356
8	150975	341	341	442.7419	442.7419
9	150975	343	343	440.1603	440.1603
10	151353	344	344	439.9797	439.9797
11	1890000	4203	4203	449.6788	449.6788
12	6119256	13901	13901	440.2026	440.2026
Average	1609800	3647.1	3647.1	441.9571	441.9571

As we can see from table 3, the proposed method results are very closed to DES results and using the selected conditions does not provide any improvement, and the encryption time will grow up rapidly when the image size grows as shown in figure 17.

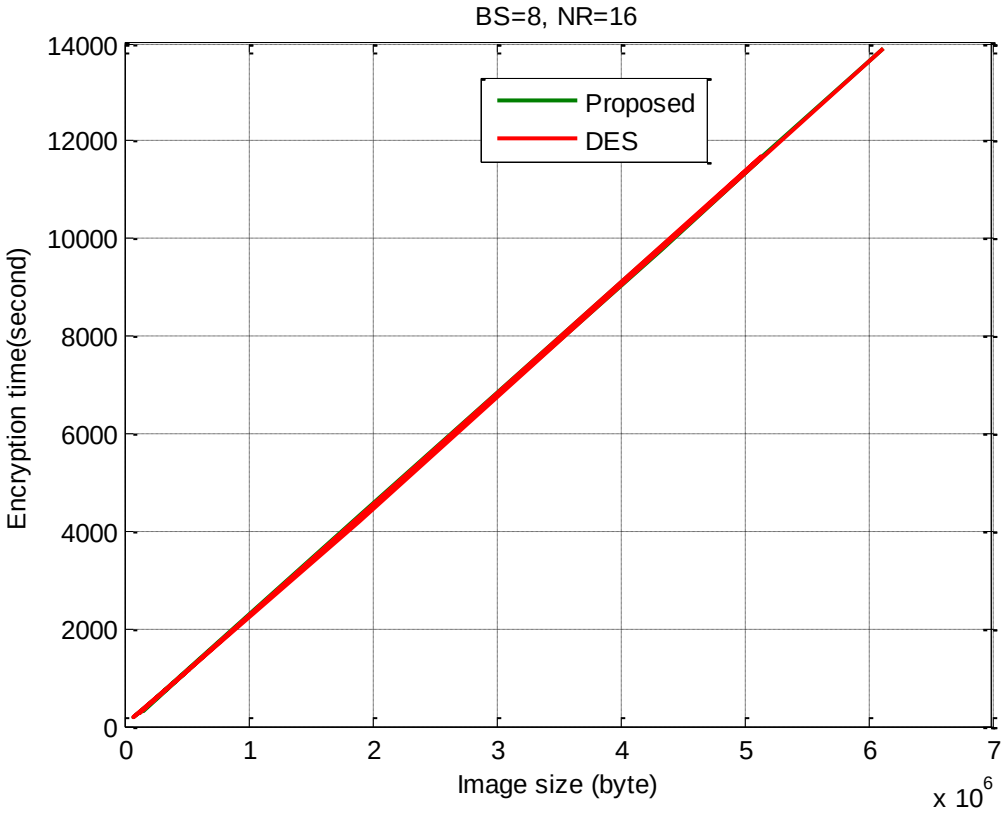

Figure 17: Image size VS encryption time(BS=8 byte, NR=16)

The image cryptography using the proposed method can be accomplished using only one round (more than one round is required to optimize MSE and PSNR values), table 4 shows the result of implementing the proposed method using RN=1, and BS=128 bytes

Table 4: Results using RN=1 and BS=128 bytes

Image number	Size (byte)	ET(second)	DT(second)	ETP(byte per second)	DTP(byte per second)
1	150849	17.9640	17.9640	8397.3	8397.3
2	77976	9.2760	9.2760	8406.2	8406.2
3	518400	61.5830	61.5830	8417.9	8417.9
4	5140800	620.7780	620.7780	8281.2	8281.2
5	4326210	518.3580	518.3580	8346.0	8346.0
6	122265	14.4790	14.4790	8444.3	8444.3
7	518400	62.0130	62.0130	8359.5	8359.5
8	150975	17.8390	17.8390	8463.2	8463.2
9	150975	17.8390	17.8390	8463.2	8463.2
10	151353	17.9180	17.9180	8447.0	8447.0
11	1890000	227.0670	227.0670	8323.5	8323.5
12	6119256	727.5990	727.5990	8410.2	8410.2
Average	1609800	192.7261	192.7261	8396.6	8396.6
Speed up of the proposed method			8396.6/448.1836= 18.7347		

From table 4 we can see that the proposed method added an enhancement to DES results, the ET was decreased and TP was increased, the proposed method has a significant speedup which is equal in average 18.7347 time, figure 18 shows the improvements achieved by the proposed method.

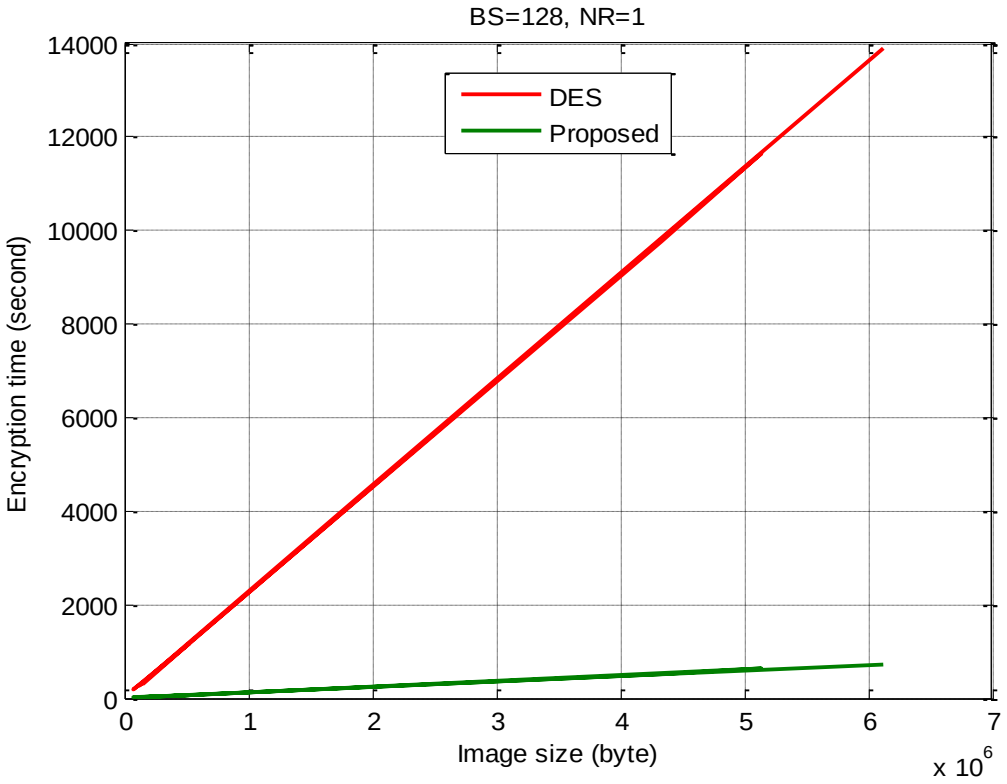

Figure 18: Proposed method improvements

Now we will discuss the effects of varying BS and NR.

An image with size = 518400 bytes was implemented using the proposed method by fixing NR to 4 and varying BS value, table

Table 5: Results when varying BS (Image size=518400, NR=4)

BS	Number of blocks	ET	DT	ETP	DTP
8	64800	294.9900	294.9900	1757.3	1757.3
16	32400	286.2810	286.2810	1810.8	1810.8
20	25920	246.9940	246.9940	2098.8	2098.8
50	10368	256.7410	256.7410	2019.2	2019.2
100	5184	251.5040	251.5040	2061.2	2061.2
128	4050	249.2110	249.2110	2080.2	2080.2
200	2592	243.9170	243.9170	2125.3	2125.3
256	2025	248.6570	248.6570	2084.8	2084.8
400	1296	240.6700	240.6700	2154.0	2154.0
500	1037	245.4910	245.4910	2111.7	2111.7
1000	518	246.0540	246.0540	2106.9	2106.9

Increasing BS will decrease ET and thus TP will be increased, using block size =400 bytes will give the best performance as shown in figures 19 and 20.

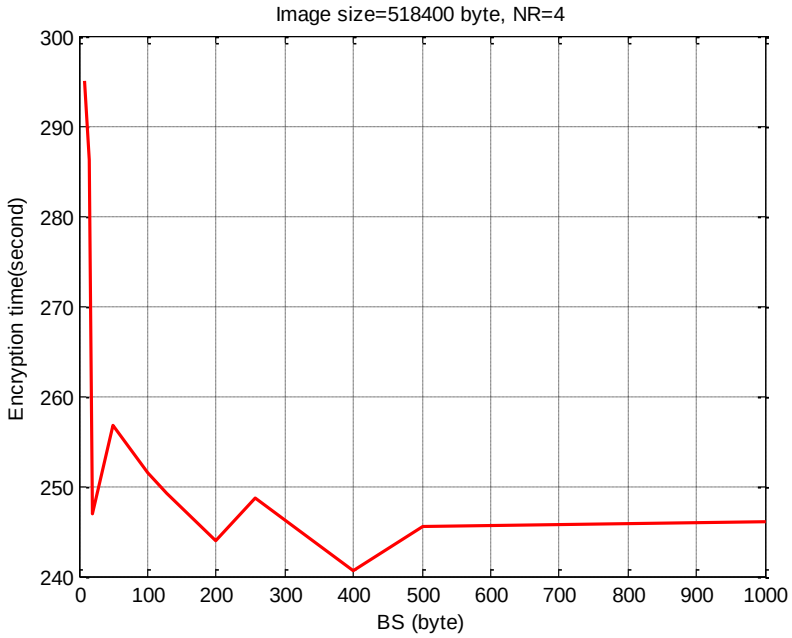

Figure 19: ET when increasing BS

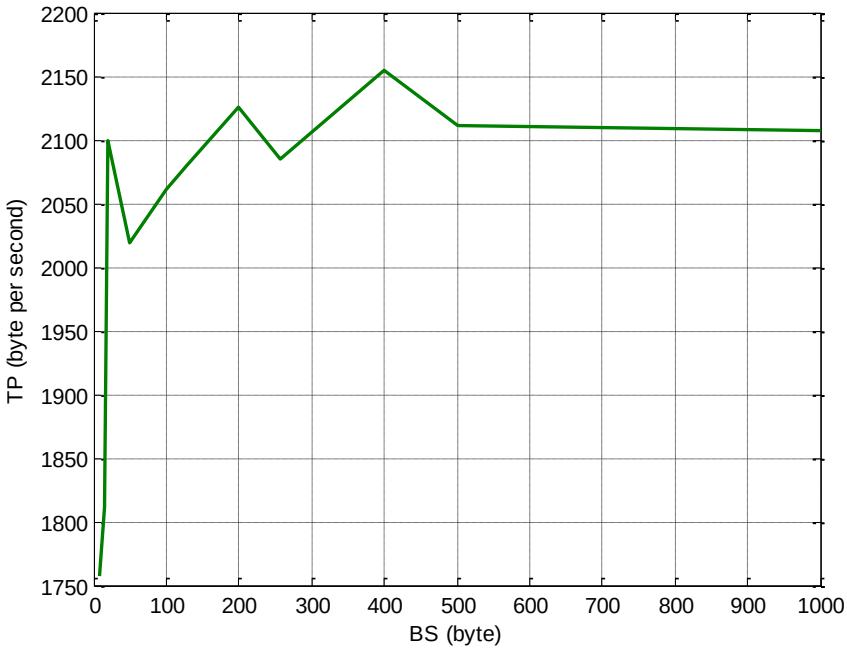

Figure 20: TP when increasing BS

The previous experiment was repeated, but her we fixed the BS and used varying values of NR, table 6 shows the obtained results.

Table 6: Varying NR (Image size=518400, BS=400)

Number of rounds	ET	DT	ETP	DTP
1	60.5550	60.5550	8560.8	8560.8
2	121.4670	121.4670	4267.8	4267.8
4	241.6610	241.6610	2145.2	2145.2
5	302.4450	302.4450	1714.0	1714.0
8	484.8240	484.8240	1069.3	1069.3
9	542.2940	542.2940	955.9390	955.9390
10	604.5570	604.5570	857.4874	857.4874
13	788.2640	788.2640	657.6477	657.6477
14	842.9500	842.9500	614.9831	614.9831
15	904.1250	904.1250	573.3720	573.3720
16	966.6130	966.6130	536.3056	536.3056

Here increasing NR will increase ET and thus will decrease TP, and for big number of rounds the efficiency of the proposed method will be rapidly drooped as shown in figures 21 and 22.

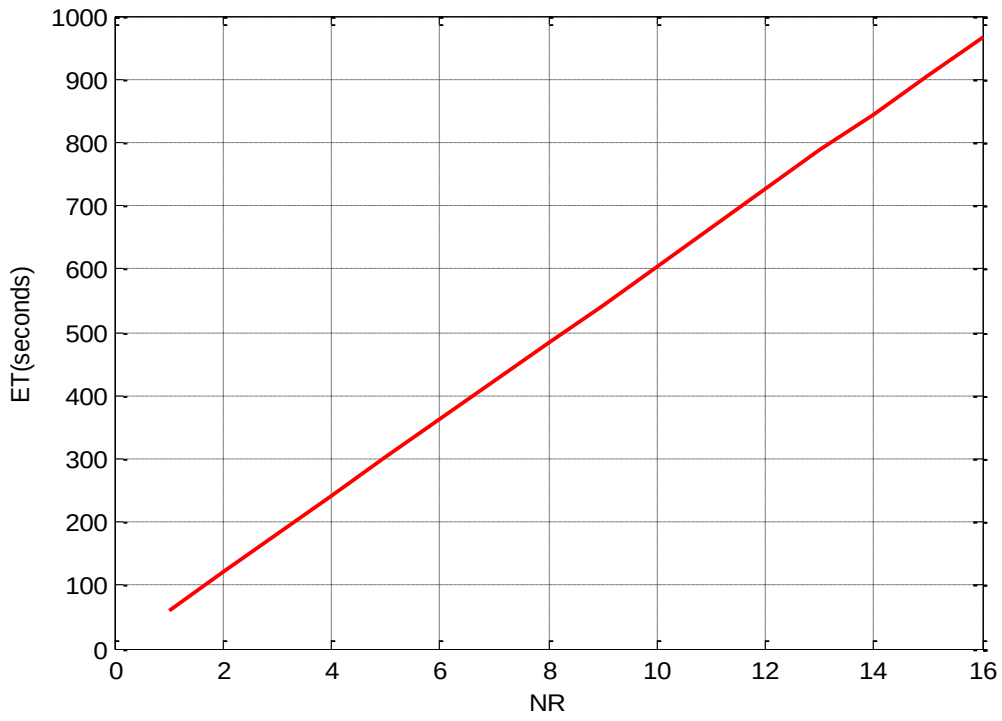

Figure 21: ET increasing when increasing NR

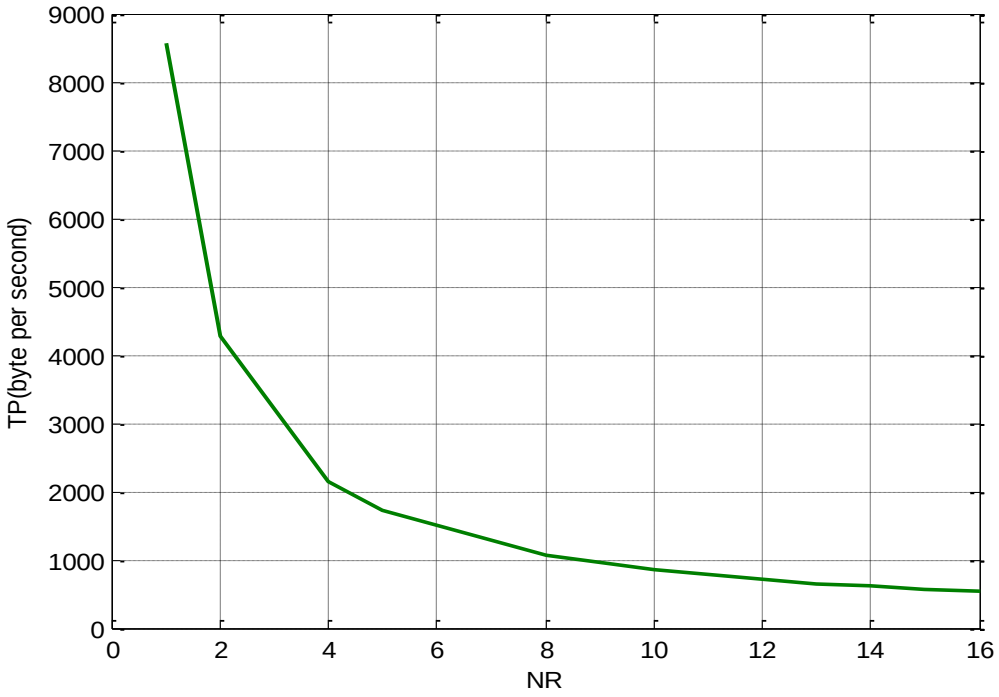

Figure 22: TP decreasing when increasing NR

Here we have to notice that using one round is sufficient to achieve the security level, extra rounds are needed to increase the encrypted image level of destruction as shown in figure 23

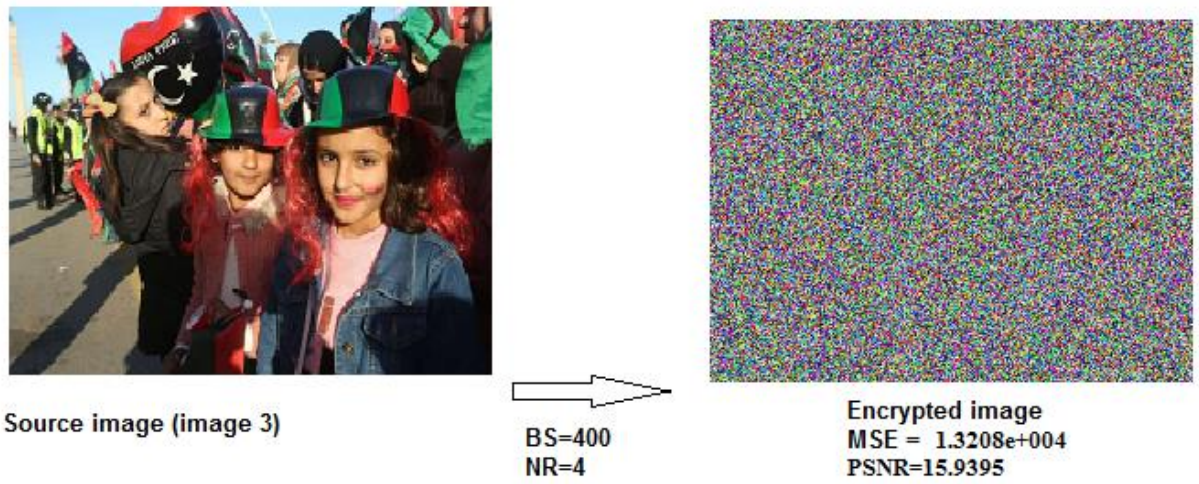

Figure 23: Sample output of the encrypted image

The proposed method provided excellent values for PSNR and MSE during the encryption and decryption phases, table 7 shows the calculated values of these parameters setting NR to 4 and BS to 400.

Table 7: Proposed method quality parameters values

Image number		Encryption			
	Size (byte)	MSE	PSNR	MSE	PSNR
1	150849	1.3199e+004	15.9466	0	Infinite
2	77976	1.3214e+004	15.9352	0	Infinite
3	518400	1.3208e+004	15.9395	0	Infinite
4	5140800	1.4907e+004	14.7297	0	Infinite
5	4326210	9.6399e+003	19.0886	0	Infinite
6	122265	1.4959e+004	14.6946	0	Infinite
7	518400	9.6372e+003	19.0914	0	Infinite
8	150975	9.5727e+003	19.1586	0	Infinite
9	150975	9.6204e+003	19.1089	0	Infinite
10	151353	9.5678e+003	19.1637	0	Infinite
11	1890000	1.3217e+004	15.9328	0	Infinite
12	6119256	1.3208e+004	15.9396	0	Infinite

Conclusion

A simple, secure, efficient and multipurpose method of data cryptography was introduces. This method can be used to encrypt-decrypt any type of image regardless the type and size, also it can be used for text data cryptography. It was shown that the proposed method can be easily implemented and updated by replacing the image_keys, BS an NR without changing the sequence of operations. It was shown that the proposed method provides a high level of data protection and security based on the complex city of the private key which is to be generated from two secret images using a determined BS and NR. The Obtained experimental results showed that the proposed method is very efficient, it decreased the encryption-decryption times, thus it increased the throughput of the data cryptography, it was shown that the proposed method has a significant speedup comparing with DES method. The proposed method gave excellent values for the quality parameters MSE and PSNR; these values can be controlled by NR to achieve an acceptable level of data destruction during the encryption phase.

References

[1] Majed O Al-Dwairi, Ziad A Alqadi, Amjad A Abujazar, Rushdi Abu Zneit, Optimized true-color image processing, World Applied Sciences Journal, vol. 8, issue 10, 2010, pp. 1175-1182.

[2] Jamil Al Azzeh, Hussein Alhatamleh, Ziad A Alqadi, Mohammad Khalil Abuzalata, Creating a Color Map be used to Convert a Gray Image to Color Image, International Journal of Computer Applications, vol. 153, issue 2, 2016, pp. 31-34.

[3] Qazem Jaber Ziad Alqadi, Jamil azza, Statistical analysis of methods used to enhance color image histogram, XX International scientific and technical conference, 2017.

[4] Bassam Subaih Ziad Alqadi, Hamdan Mazen, A Methodology to Analyze Objects in Digital Image using Matlab, International Journal of Computer Science & Mobile Computing, vol. 5, issue 11, 2016,pp. 21-28.

[5] Mazen A.Hamdan Bassam M.Subaih, Prof. Ziad A. Alqadi, Extracting Isolated Words from an Image of Text, International Journal of Computer Science & Mobile Computing, vol. 5, issue 11, 2016, pp. 29-36.

[6] Dr. Amjad Hindi, Dr. Majed Omar Dwairi, Prof. Ziad Alqadi, Analysis of Procedures used to build an Optimal Fingerprint Recognition `System, International Journal of Computer Science and Mobile Computing, vol. 9, issue 2, 2020, pp. 21 –37.

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

[8] Ahmad Sharadqh Naseem Asad, Ismail Shayeb, Qazem Jaber, Belal Ayyoub, Ziad Alqadi, Creating a Stable and Fixed Features Array for Digital Color Image, IJCSMC, vol. 8, issue 8, 2019, pp. 50-56.

[9] Ziad Alqadi, Dr. Mohammad S. Khrisat, Dr. Amjad Hindi,Dr.Majed Omar Dwairi, VALUABLE WAVELET PACKET INFORMATION TO ANALYZE COLOR IMAGES FEATURES, International Journal of Current Advanced Research, vol. 9, issue 2, 2020, pp. 2319.

[10] Ziad AlQadi, M Elsayyed Hussein, Window Averaging Method to Create a Feature Victor for RGB Color Image, International Journal of Computer Science and Mobile Computing, vol. 6, issue 2, 2017,pp. 60-66.

[11] Bilal Zahran Belal Ayyoub, Jihad Nader, Ziad Al-Qadi, Suggested Method to Create Color Image Features Victor, Journal of Engineering and Applied Sciences, vol. 14, issue 1, 2019, pp. 2203-2207.

[12] Ahmad Sharadqh Naseem Asad, Ismail Shayeb, Qazem Jaber, Belal Ayyoub, Ziad Alqadi, Creating a Stable and Fixed Features Array for Digital Color Image, IJCSMC, vol. 8, issue 8, 2019, pp. 50-56.

[13] Yousf Eltous Ziad A.Al Qadi,Ghazi M. Qaryouti, Mohammad Abuzalata,ANALYSIS OF DIGITAL SIGNAL FEATURES EXTRACTION BASED ON KMEANS CLUSTERING, International Journal of Engineering Technology Research & Management, vol. 4, issue 1, 2020, pp. 66-75.

[14] 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, 2020, pp. 48-55.

[15] 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, 2019, pp. 4092-4098.

[16] Ziad Alqadi, Majid Oraiqat, Hisham Almujafet, Salah Al-Saleh, Hind Al Husban, Soubhi Al-Rimawi, A New Approach for Data Cryptography, International Journal of Computer Science and Mobile Computing, vol. 8, issue 8, 2019, pp. 30-48.

[17] Ayman Al-Rawashdeh, Ziad Al-Qadi, Using wave equation to extract digital signal features, Engineering, Technology & Applied Science Research, vol. 8, issue 4, 2018, pp. 1356-1359.

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

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

[20] 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, 2019, pp. 76-90.

[21] Ziad Alqadi, Ahmad Sharadqh, Naseem Asad, Ismail Shayeb, Jamil Al-Azzeh, Belal Ayyoub, A highly secure method of secret message encoding, International Journal of Research in Advanced Engineering and Technology, vol. 5, issue 3, 2019, pp. 82-87.

[22] Musbah Aqel Ziad A. Alqadi, Performance analysis of parallel matrix multiplication algorithms used in image processing, World Applied Sciences, vol. 6, issue 1, 2009, pp. 45-52.

[23] Jihad Nadir, Ashraf Abu Ein, Ziad Alqadi, A Technique to Encrypt-decrypt Stereo Wave File, International Journal of Computer and Information Technology, vol. 5, issue 5, 2026, pp. 465-470.

[24] Musbah J Aqel, Ziad ALQadi, Ammar Ahmed Abdullah, RGB Color Image Encryption-Decryption Using Image Segmentation and Matrix Multiplication, International Journal of Engineering and Technology, vol. 7, issue 3, 2018, pp. 104-107.

[25] Belal Zahran Rashad J Rasras, Ziad Alqadi, Mutaz Rasmi Abu Sara, B Zahran, Developing new Multilevel security algorithm for data encryption-decryption (MLS_ED), International Journal of Advanced Trends in Computer Science and Engineering, vol. 8, issue 6, 2019, pp. 3228-3235.

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

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

[28] Ziad A AlQadi, Accurate Method for RGB Image Encryption, International Journal of Computer Science and Mobile Computing, vol. 9, issue 1, 2020, pp. 12-21.

[29] Ziad Alqadi, Majid Oraiqat, Hisham Almujafet, Salah Al-Saleh, Hind Al Husban, Soubhi Al-Rimawi, A New Approach for Data Cryptography, International Journal of Computer Science and Mobile Computing, vol. 8, issue 9, 2019, pp. 30-48.

[30] Jamil Al-Azzeh, Ziad Alqadi, Qazem Jaber, A Simple, Accurate and Highly Secure Method to Encrypt-Decrypt Digital Images, JOIV: International Journal on Informatics Visualization, vol. 3, issue 3, 2019, pp. 262-265.

[31] Dr Saleh A Khawatreh Dr Majed, Omar Dwairi, Prof. Ziad Alqadi, Dr. Mohammad S. Khrisat, Dr. Amjad Hindi, Digital color image encryption-decryption using segmentation and reordering, International Journal of Latest Research in Engineering and Technology (IJLRET), vol. 6, issue 5, 2020, pp. 6-12.

[32] Mutaz Rasmi Abu Sara Rashad J. Rasras, Ziad A. AlQadi, A Methodology Based on Steganography and Cryptography to Protect Highly Secure Messages, Engineering, Technology & Applied Science Research, vol. 9, issue 1, 2019, pp. 3681-3684.

[33] 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, issue 5, 2016, pp. 125-131.

[34] PROF. ZIAD A. ALQADI, A SIMPLE METHOD TO ENCRYPT-DECRYPT SPEECH SIGNAL, International Journal of Engineering Technology Research & Management, vol. 5, issue 2, pp. 44-52, 2021.

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

[36] 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, 2019, pp. 14-26.

[37] Musbah Aqel, Ziad A. Alqadi, Performance analysis of parallel matrix multiplication algorithms used in image processing, World Applied Sciences Journal, vol. 6, issue 1, 2009. pp. 45-52.

[38] Amjad Y Hindi, Majed O Dwairi, Ziad A AlQadi, A Novel Technique for Data Steganography, Engineering, Technology & Applied Science Research, vol. 9, issue 6, 2019,pp. 4942-4945.

[39] 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, 2019, pp. 4092-4098.

[40] Bilal Zahran Belal Ayyoub, Jihad Nader, Ziad Al-Qadi, Suggested Method to Create Color Image Features Victor, Journal of Engineering and Applied Sciences, vol. 14, issue 1, 2019,pp. 2203-2207 .

[41] Akram A Moustafa, 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, vol. 5, issue 5, 2009. pp. 355-362.

[42] Rushdi Abu Zneit, Jamil Al-Azzeh, Ziad Alqadi, Belal Ayyoub, Ahmad Sharadqh, Using Color Image as a Stego-Media to Hide Short Secret Messages, International Journal of Computer Science and Mobile Computing, vol. 8, issue 6, 2019, pp. 106-123.

[43] Bilal Zahran Belal Ayyoub, Jihad Nader, Ziad Al-Qadi, Suggested Method to Create Color Image Features Victor, Journal of Engineering and Applied Sciences, vol. 14, issue 1, 2019,pp. 2203-2207.

[44] Mohammed Ashraf Al Zudool, Saleh Khawatreh, Ziad A. Alqadi, Efficient Methods used to Extract Color Image Features, IJCSMC, vol, 6, issue 12, 2017,pp. 7-14.

[45] 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, 2008,pp. 211-214.

[46] 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, 2019,pp. 4092-4098.

[47] Ziad Alqadi, A practical approach of selecting the edge detector parameters to achieve a good edge map of the gray image, Journal of Computer Science, vol. 5, issue 5, 2009,pp. 355-362.

[48] M. Abu-Faraj, and Z. Alqadi, "Image Encryption using Variable Length Blocks and Variable Length Private Key," International Journal of Computer Science and Mobile Computing (IJCSMC), vol. 11, Iss. 3, pp. 138-151, 2022.

[49] M. Abu-Faraj, A. Al-Hyari, and Z. Alqadi, "A Dual Approach for Audio Cryptography," Journal of Southwest Jiaotong University, vol. 57, no. 1, pp. 24-33, 2022.

[50] 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.

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

[52] M. Abu-Faraj, Khaled Aldebe, and Z. Alqadi, "Deep Machine Learning to Enhance ANN Performance: Fingerprint Classifier Case Study," Journal of Southwest Jiaotong University, vol. 56, no. 6, pp. 685-694, 2021.

[53] M. Abu-Faraj, Z. Alqadi, and K. Aldebei, "Comparative Analysis of Fingerprint Features Ex- traction Methods," Journal of Hunan University Natural Sciences, vol. 48, iss. 12, pp. 177-182, 2021.

[54] 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.

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

[56] 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.

